Reconocimiento Facial en Azure para Reforzar la Seguridad y Prevenir Delitos

Samuel Pastrana Bedoya

Jairo Junior Cetre Agualimpia

Trabajo de Grado presentado como requisito para optar al título de:

Especialista en Big Data e Inteligencia de Negocios

Asesor: Ingrid Durley Torres Pardo
Título de Posgrado

Universidad Católica Luis Amigó
Facultad de Ingenierías y
Arquitectura
Especialización en Big Data e Inteligencia de Negocios
Medellín, Colombia
2024

Dedicatorias

Samuel Pastrana Bedoya
A mis padres

La preocupación por el hombre y su destino siempre debe ser el interés primordial de todo esfuerzo técnico. Nunca olvides esto entre tus diagramas y ecuaciones.

Albert Einstein

Jairo Junior Cetre Agualimpia

En primer lugar, elevo mi gratitud a Dios, cuya guía y misericordia han sido mi fuerza y mi luz en cada paso de esta travesía. Sin Su infinita bondad, este logro no habría sido posible.

A mis padres, Jairo Cetre y Arlen Agualimpia, les debo todo mi reconocimiento. Su inquebrantable apoyo y amor incondicional han sido mi mayor fortaleza. Mamá, tu resiliencia ante las adversidades ha sido mi inspiración constante. Papá, tu pujanza y ejemplo de trabajo duro me han guiado en todo momento.

Mi novia, Carolina, ha sido mi compañera inquebrantable en este viaje. Su apoyo incondicional y su amor han sido mi roca en los momentos de desafío. Agradezco profundamente su presencia constante a mi lado.

Aunque ya no está físicamente entre nosotros, quiero rendir un especial tributo a mi abuelo, Ángel Marino Agualimpia. Su legado de lucha y determinación han dejado una marca indeleble en mi vida. Su recuerdo vive en mí como un faro de inspiración y perseverancia.

A mi querida tía Denis Agualimpia, mi eterna gratitud por su amor y por abrirme las puertas de su hogar en estos casi 10 años de mi estadía en la ciudad.al recibirme cuando era apenas un niño. Su generosidad, cariño y protección han sido un regalo invaluable en mi vida, y su presencia ha marcado un capítulo significativo en mi camino hacia el éxito académico.

A todos los demás familiares, amigos, profesores y compañeros de estudio que han contribuido a mi formación y crecimiento, les doy las gracias de todo corazón. Cada palabra de aliento y cada gesto de apoyo han sido combustible para mi determinación.

Este logro lo dedico a todos ustedes, mis seres queridos, cuyo amor y apoyo han sido la fuerza motriz detrás de cada paso que he dado. Su presencia ha hecho de este camino un viaje memorable, y prometo honrar el legado con cada logro que alcance en el futuro.

Agradecimientos

Expreso mi profundo agradecimiento al profesor Víctor Gil y a la profesora Ingrid Durley Torres Pardo por su guía y dedicación en mis trabajos de grado 1 y 2, respectivamente. Agradezco a la Universidad Católica Luis Amigó y a la Facultad de Ingenierías y Arquitectura por brindarme un entorno propicio para mi formación. Reconozco especialmente a Oney Vanegas Godin, Linas Restrepo, Cardona y al Grupo Record de Colombia por su invaluable apoyo y orientación en mi crecimiento personal y profesional, especialmente en la comprensión y apreciación de la inteligencia de negocios como una disciplina esencial en mi desarrollo profesional.

Resumen

Proyecto enfocado en el reconocimiento facial automático y el aprendizaje profundo impulsado por inteligencia artificial para Segurtronic, una empresa que brinda servicios de vigilancia y vende cámaras de seguridad,monitoreo, y control de pánico, . Este trabajo presenta el proceso de detección de personas dentro de una instalación donde se utilizan cámaras. Se enviará una alerta si la persona detectada no resulta ser reconocida; en este caso, se le pedirá que se registre o proporcione sus huellas digitales en un lugar designado por la empresa.

Este desarrollo consta de dos fases. La primera fase consiste en la clasificación y análisis de imágenes utilizando la plataforma Azure (Azure Vision) para el entrenamiento necesario. La segunda fase implica el reconocimiento facial utilizando una biblioteca de Python. Este desarrollo nos permite identificar a una persona, incluso si lleva la cara cubierta; el modelo también considera el rango de edad de la persona detectada. Todas estas características son claves para lograr la detección definida como objetivo de este trabajo, desarrollando un sistema que no solo detecta, sino que también puede predecir delitos relacionados con la suplantación del reconocimiento facial de personas, en un futuro cercano.

Es importante enfatizar que el reconocimiento facial debe realizarse en puntos específicos, en lugar de en todos los lugares donde la cámara esté enfocada, ya que estas son las áreas más sensibles para observar personas con acceso restringido. Este desarrollo nos permite almacenar un historial de cuándo se analizó un rostro y el tiempo transcurrido entre la primera detección (ingreso al edificio) y la última detección (salida del edificio) y/o las instalaciones.

Palabras clave: (Detección, Azure, Python, Delitos, Rostro).

Tabla de Contenido

Lista de figuras

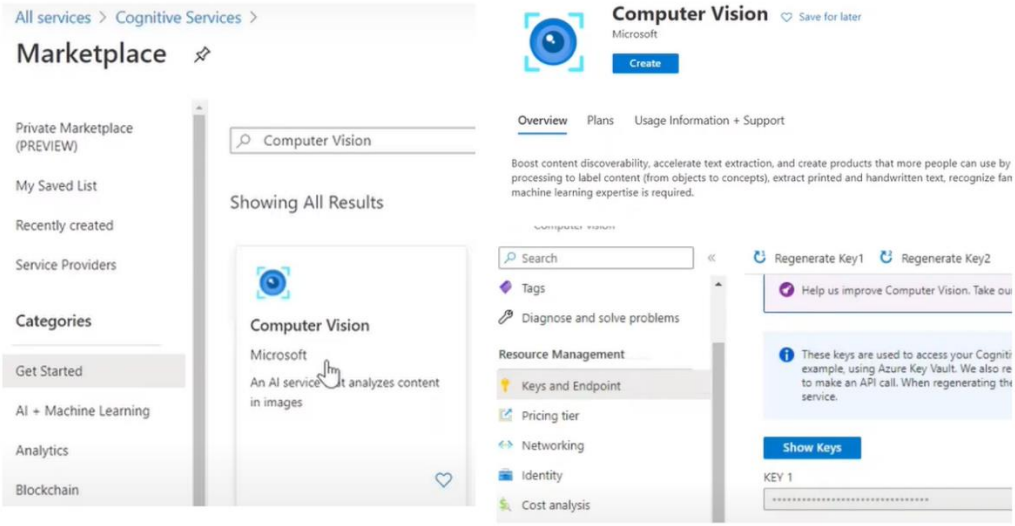

Ilustración 1: Configuración Servicio Análisis de Imágenes en Azure

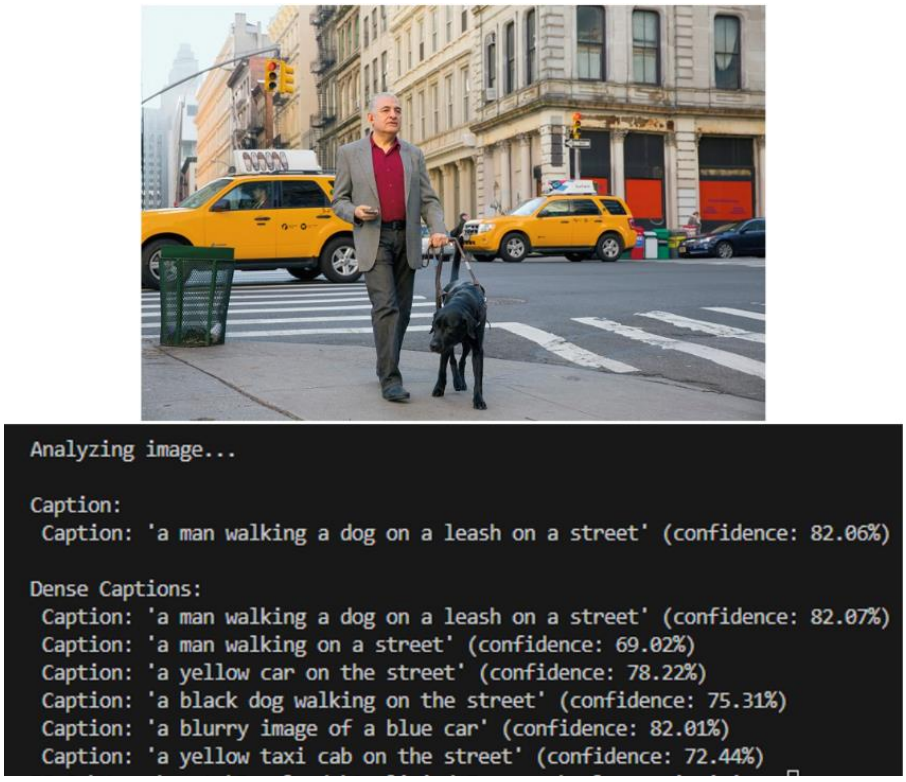

Ilustración 2 Primera Prueba Análisis de Imágenes Con Azure

Ilustración 3 Segunda Prueba Análisis de Imágenes, Reconocimiento de Rostros

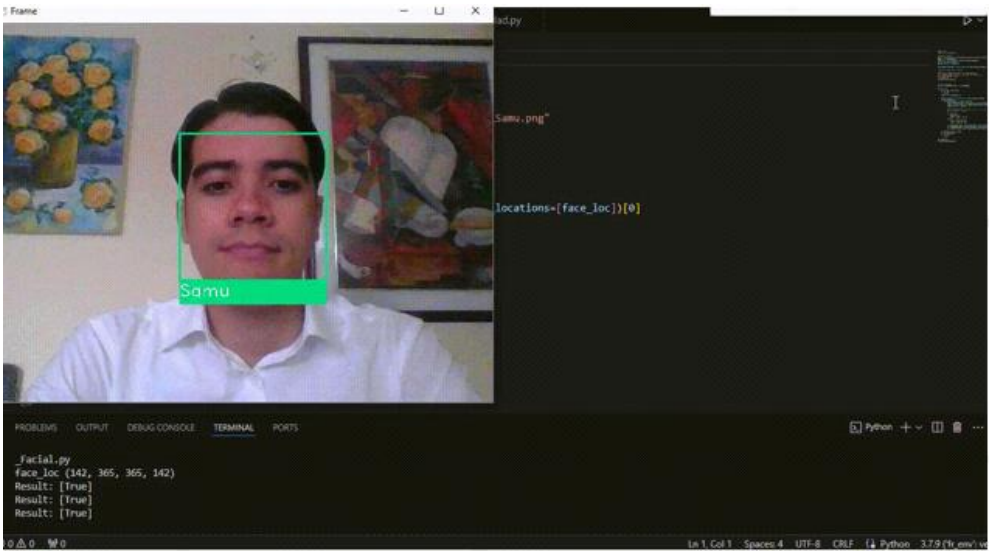

Ilustración 4 Primer Desarrollo: Reconocimiento Facial

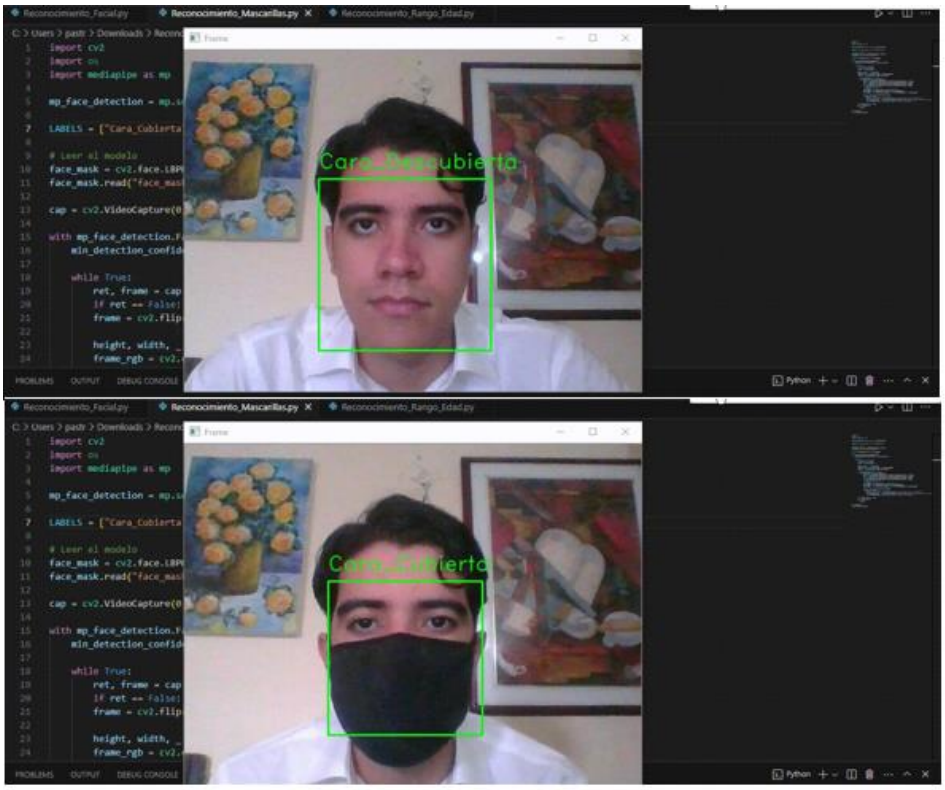

Ilustración 5 Segundo Desarrollo: Rostros Cubierto o Descubiertos

Ilustración 6 Tercer Desarrollo: Reconocimiento Rango de Edad y Género

Lista de tablas

Tabla 1 Código Análisis de Imágenes

```python
from dotenv import load_dotenv
import os
from PIL import Image, ImageDraw
import sys
from matplotlib import pyplot as plt
from azure.core.exceptions import HttpResponseError
import requests

 # import namespaces
from azure.ai.vision.imageanalysis import ImageAnalysisClient
from azure.ai.vision.imageanalysis.models import VisualFeatures
from azure.core.credentials import AzureKeyCredential


def main():
    global cv_client

    try:
        # Get Configuration Settings
        load_dotenv()
        ai_endpoint = os.getenv('AI_SERVICE_ENDPOINT')
        ai_key = os.getenv('AI_SERVICE_KEY')

        # Get image
        image_file = 'Labfiles/01-analyze-images/Python/image-analysis/images/shakira.jpg'
        if len(sys.argv) > 1:
            image_file = sys.argv[1]
def AnalyzeImage(image_filename, image_data, cv_client):
    print('\nAnalyzing image...')

    try:
        # Get result with specified features to be retrieved
        result = cv_client.analyze(
            image_data=image_data,
            visual_features=[
                VisualFeatures.CAPTION,
                VisualFeatures.DENSE_CAPTIONS,
                VisualFeatures.TAGS,
                VisualFeatures.OBJECTS,
                VisualFeatures.PEOPLE],
                )


    except HttpResponseError as e:
        print("Status code: {}".format(e.status_code))
        print("Reason: {}".format(e.reason))
        print("Message: {}".format(e.error.message))

    # Display analysis results
    # Get image captions
    if result.caption is not None:
        print("\nCaption:")
        print(" Caption: '{}' (confidence: {:.2f}%)".format(result.caption.text, result.caption.confidence * 100))
```

Tabla 2 Código Reconocimiento Facial

```python
import cv2
import face_recognition
import winsound

# Imagen a Comparar
path = "C:\\Users\\pastr\\Downloads\\ReconocimientoFacialPython\\Images\\Samu.png"
image = cv2.imread(path)
face_loc = face_recognition.face_locations(image)[0]
x1, y1, x2, y2 = face_loc
print("face_loc", face_loc)

face_image_encodings = face_recognition.face_encodings(image, known_face_locations=[face_loc])[0]

# Mostrar imagen con el recuadro
'''
print("face_image_encodings:",face_image_encoding)
cv2.rectangle(image, (x1, y1), (x2, y2), (0, 255, 0), 2)
cv2.imshow("Image", image)
cv2.waitKey(0)
cv2.destroyAllWindows()
'''
while True:
    ret, frame = cap.read()
    if not ret:
        break
    frame = cv2.flip(frame, 1)

    face_locations = face_recognition.face_locations(frame)
    if face_locations:
        for face_location in face_locations:
            face_frame_encodings = face_recognition.face_encodings(frame, known_face_locations=[face_location])[0]
            result = face_recognition.compare_faces([face_frame_encodings], face_image_encodings)
            print("Result:", result)

            #cv2.rectangle(frame, (x1, y1), (x2, y2), (0, 255, 0), 2)
            #print("Result:", result)

            if result[0]:
                text = "Samu"
                color = (125, 220, 0)
            else:
                text = "Desconocido"
                color = (50, 50, 255)
                winsound.Beep(1000, 500)

            cv2.rectangle(frame, (face_location[3], face_location[2]), (face_location[1], face_location[2] + 30), color, -1)
            cv2.rectangle(frame, (face_location[3], face_location[0]), (face_location[1], face_location[2]), color, 2)
            cv2.putText(frame, text, (face_location[3], face_location[2] + 20), 2, 0.7, (255, 255, 255), 1)

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

cap.release()
cv2.destroyAllWindows()
```

Tabla 3 Código Rostros Cubiertos-Descubiertos

```python
import cv2
import os
import mediapipe as mp

mp_face_detection = mp.solutions.face_detection

LABELS = ["Cara_Cubierta", "Cara_Descubierta"]

# Leer el modelo
face_mask = cv2.face.LBPHFaceRecognizer_create()
face_mask.read("face_mask_model.xml")

cap = cv2.VideoCapture(0, cv2.CAP_DSHOW)

with mp_face_detection.FaceDetection(
    min_detection_confidence=0.5) as face_detection:

    while True:
        ret, frame = cap.read()
        if ret == False: break
        frame = cv2.flip(frame, 1)

        height, width, _ = frame.shape
        frame_rgb = cv2.cvtColor(frame, cv2.COLOR_BGR2RGB)
        results = face_detection.process(frame_rgb)

        if results.detections is not None:
            for detection in results.detections:
                xmin = int(detection.location_data.relative_bounding_box.xmin * width)
                ymin = int(detection.location_data.relative_bounding_box.ymin * height)
                w = int(detection.location_data.relative_bounding_box.width * width)
                h = int(detection.location_data.relative_bounding_box.height * height)
                if xmin < 0 and ymin < 0:
                    continue
                face_image = frame[ymin:ymin + h, xmin:xmin + w]
                face_image = cv2.cvtColor(face_image, cv2.COLOR_BGR2GRAY)
                face_image = cv2.resize(face_image, (72, 72), interpolation=cv2.INTER_CUBIC)

                result = face_mask.predict(face_image)
                if result[1] < 150:
                    color = (0, 0, 255) if LABELS[result[0]] == "Con_mascarilla" else (0, 255, 0)
                    cv2.putText(frame, "{}".format(LABELS[result[0]]), (xmin, ymin - 15), 2, 1, color, 1, cv2.LINE_AA)
                    cv2.rectangle(frame, (xmin, ymin), (xmin + w, ymin + h), color, 2)

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

cap.release()
cv2.destroyAllWindows()
```

Tabla 4 Código Reconocimiento Rango de Edad

```
import cv2

def faceBox(faceNet,frame):
    frameHeight = frame.shape[0]
    frameWidth = frame.shape[1]
    blob = cv2.dnn.blobFromImage(frame,1.0,(227,227), [104,117,123,], swapRB=False)
    faceNet.setInput(blob)
    detection = faceNet.forward()
    bboxs = []
    for i in range(detection.shape[2]):
        confidence = detection[0,0,i,2]
        if confidence > 0.7:
            x1 = int(detection[0,0,i,3]*frameWidth)
            y1 = int(detection[0,0,i,4]*frameHeight)
            x2 = int(detection[0,0,i,5]*frameWidth)
            y2 = int(detection[0,0,i,6]*frameHeight)
            bboxs.append([x1,y1,x2,y2])
            cv2.rectangle(frame, (x1,y1),(x2,y2),(0,255,0),1)
    return frame, bboxs



faceProto = "C:\\Users\pastr\\Downloads\\ReconocimientoFacialPython\\Age_Estimation\\opencv_face_detector.pbtxt"
faceModel = "C:\\Users\pastr\\Downloads\\ReconocimientoFacialPython\\Age_Estimation\\opencv_face_detector_uint8.pb"
ageProto = "C:\\Users\pastr\\Downloads\\ReconocimientoFacialPython\\Age_Estimation\\age_deploy.prototxt"
ageModel = "C:\\Users\pastr\\Downloads\\ReconocimientoFacialPython\\Age_Estimation\\age_net.caffemodel"

genderProto = "C:\\Users\pastr\\Downloads\\ReconocimientoFacialPython\\Age_Estimation\\gender_deploy.prototxt"
genderModel = "C:\\Users\pastr\\Downloads\\ReconocimientoFacialPython\\Age_Estimation\\gender_net.caffemodel"


faceNet = cv2.dnn.readNet(faceModel, faceProto)
ageNet = cv2.dnn.readNet(ageModel,ageProto)
genderNet = cv2.dnn.readNet(genderModel,genderProto)

MODEL_MEAN_VALUES = (78.4263377603, 87.7689143744, 114.895847746)
ageList = ['(0-2)', '(4-6)', '(8-12)', '(15-20)', '(25-32)', '(38-43)', '(48-53)', '(60-100)']
genderList = ['Male', 'Female']


video = cv2.VideoCapture(0)

padding = 20

while True:
    ret,frame = video.read()
    frame,bboxs = faceBox(faceNet,frame)
    for bbox in bboxs:
    #face = frame[bbox[1]:bbox[3], bbox[0]:bbox[2]]
    face = frame[max(0,bbox[1]-padding):min(bbox[3]+padding,frame.shape[0]-1),max(0,bbox[0]-padding):min(bbox[2]+padding, frame.shape[1]-1)]
    blob = cv2.dnn.blobFromImage(face, 1.0, (227,227),MODEL_MEAN_VALUES, swapRB=False)
    genderNet.setInput(blob)
    genderPred = genderNet.forward(blob)
    gender = genderList[genderPred[0].argmax()]


    ageNet.setInput(blob)
    agePred = ageNet.forward()
    age = ageList[agePred[0].argmax()]


    label= "{}.{}".format(gender,age)
    cv2.rectangle(frame,(bbox[0],bbox[1]-30), (bbox[2],bbox[1]), (0,255,0),-1)
    cv2.putText(frame, label, (bbox[0], bbox[1]-10), cv2.FONT_HERSHEY_SIMPLEX, 0.8, (255,255,255),2, cv2.LINE_AA)
cv2.imshow("Age-Gender",frame)
k=cv2.waitKey(1)
if k==ord('q'):
    break
ideo.release()
v2.destroyAllWindows()
```

1. Introducción

La seguridad y la identificación oportuna de los rostros captados por las cámaras que utilizan servicios de reconocimiento por medio de inteligencia artificial son fundamentales para cualquier empresa en esta era moderna y tecnológica. Esto es especialmente cierto para empresas como Grupo Record de Colombia, que necesitan proteger sus instalaciones y recursos de manera integral. En este contexto, el uso de la tecnología de reconocimiento facial basada en inteligencia artificial se presenta como una solución innovadora y altamente eficaz para fortalecer la seguridad y optimizar las operaciones.

El propósito principal de este proyecto es implementar un sistema de reconocimiento facial que satisfaga las necesidades específicas de Grupo Record de Colombia. Por esta razón, el trabajo se concentró en la implementación de un sistema completo de identificación de rostros que permita utilizar el reconocimiento facial en tiempo real a través de las cámaras de seguridad corporativas.

El valor agregado de este trabajo reside en su capacidad para mejorar de manera integral la seguridad y supervisión en la empresa. Un sistema de reconocimiento facial permitirá una identificación y verificación más precisa de los empleados y visitantes, disminuyendo los peligros de acceso no autorizado y asegurando un entorno más protegido en las instalaciones.

El enfoque metodológico de este proyecto se centrará en describir un sistema de vanguardia y los requisitos necesarios para el desarrollo del sistema de reconocimiento facial, así como en crear una función personalizada que se especialice en la identificación y análisis de rostros. Adicionalmente, se formuló la implementación de un sistema de reconocimiento facial en los sistemas de control de acceso de Segurtronic, con énfasis en la preparación continua para una verificación segura.

El uso de este modelo fortalecerá la posición del Grupo Record de Colombia en el mercado de seguridad y monitoreo, y ayudará a reforzar su imagen como una empresa innovadora y comprometida con la seguridad de sus clientes y usuarios.

Palabras claves (Seguridad, Identificación, Rostros, Cámaras, Reconocimiento facial, Inteligencia artificial, Empresa)

2. Planteamiento del Problema

Hemos desarrollado una solución de reconocimiento facial basada en inteligencia artificial adaptada a las necesidades específicas de Grupo Record de Colombia. Durante el proceso de desarrollo, encontramos una limitación en la que Azure denegaba el permiso para acceder a Azure Face API. Por lo tanto, aunque el reconocimiento facial se realiza en Python mediante una biblioteca de reconocimiento facial, tuvimos que buscar una alternativa y desarrollar el análisis de imágenes utilizando Azure.

Desafíos y Oportunidades:

Esta situación presenta una clara oportunidad de mejora. Una vez que se obtengan los permisos necesarios, se podría utilizar Azure Face API para migrar el código de reconocimiento facial a Azure. Además, el uso de Azure Face API puede mejorar la precisión y la eficiencia del reconocimiento facial, lo que simplificará la administración y la escalabilidad de la solución en el futuro. La utilización de Azure Face API conlleva una serie de beneficios adicionales. En primer lugar, la solución se beneficiará de la escalabilidad automática que ofrece la nube de Azure, permitiendo manejar un creciente volumen de datos y usuarios sin comprometer el rendimiento. En segundo lugar, la administración se simplifica gracias a las herramientas integradas de Azure para el monitoreo, la gestión y la seguridad, facilitando así el mantenimiento y la actualización del sistema.

Por último, la migración a Azure Face API no solo representa una mejora técnica, sino también una estratégica, al alinearse con las tendencias actuales de adopción de servicios en la nube, lo cual es vital para mantenerse competitivo y a la vanguardia en el campo de la tecnología de reconocimiento facial. De esta manera, se asegura que la solución no solo cumpla con los estándares actuales, sino que también esté preparada para futuras expansiones y actualizaciones tecnológicas.

Impacto Potencial:

Esta posible transición no sólo resolvería los desafíos encontrados durante el desarrollo inicial, sino que también abriría nuevas oportunidades para mejorar la funcionalidad y el rendimiento de las soluciones de reconocimiento facial. En última instancia, Grupo Record de Colombia podrá aprovechar todo el potencial de la tecnología de inteligencia artificial para mejorar la seguridad y eficiencia de sus operaciones.

Palabras clave (Solución, Azure, Permiso, Azure Face API, Python, Desafíos)

3. Justificación

Este proyecto utilizó las herramientas de Azure para crear una solución integral que permitió a las cámaras de seguridad empresariales implementar reconocimiento facial en tiempo real. Gracias a esta tecnología, se pudo detectar y analizar las características de las personas grabadas por las cámaras, mejorando significativamente las capacidades de seguridad y vigilancia de los servicios.

El enfoque del proyecto fue personalizado e innovador desde el punto de vista tecnológico, buscando optimizar la autenticación, la seguridad y la eficiencia en el acceso del personal y los visitantes. La implementación de sistemas de reconocimiento facial basados en inteligencia artificial en las empresas, especialmente en Segurcol, Segurtronic Technology Solutions y Segurtronic Ltda., parte del Grupo Récord de Colombia, fue un proyecto crucial para mejorar y potenciar tanto la seguridad como la eficiencia operativa.

Esta iniciativa se fundamentó en la importancia de la seguridad en la sociedad y en las empresas, especialmente en las áreas de vigilancia, seguridad y tecnología. La adopción de esta tecnología permitió una identificación y autenticación más precisas de empleados y visitantes, reduciendo el riesgo de acceso no autorizado y garantizando un entorno más seguro en las instalaciones de Segurco ltda,Segurtronic Technology Solutions y Segurtronic ltda.

Además, esta solución agilizó el proceso de incorporación y selección de empleados, reduciendo los

tiempos de espera y mejorando la productividad. Mantenerse a la vanguardia de la tecnología es esencial en un entorno empresarial competitivo, y esta solución demostró el compromiso de Segurcol y Segurtronic Technology Solutions con la innovación y las mejores prácticas tecnológicas. Esto no solo mejoró su posición en el mercado, sino que también fortaleció su imagen como líderes de la industria.

La adaptación de esta tecnología a las necesidades específicas de Segurcol y Segurtronic Technology Solutions aseguró su adecuada integración en los procesos operativos existentes, contribuyendo al cumplimiento normativo y la protección de la reputación de la empresa. Además, la capacidad de analizar y detectar características humanas en tiempo real aportó ventajas adicionales a las instalaciones de vigilancia, previniendo incidentes de seguridad y facilitando la toma de decisiones.

La implementación del reconocimiento facial fortaleció la posición del Grupo Récord de Colombia en el mercado de seguridad y vigilancia, diferenciándose de la competencia, aumentando la confianza de los clientes y atrayendo nuevas oportunidades de negocio.

Palabras claves (Vigilancia, Autenticación, Eficiencia, Integración, Productividad)

4. Marco de Referencias

Desde una perspectiva tecnológica, estaba claro lo importante que era aprovechar herramientas avanzadas como Azure Face API para el reconocimiento facial en tiempo real. La plataforma ofrecía varias funciones, como reconocimiento facial, atributos faciales, coincidencia facial y detección de similitudes faciales. Además, se destacó la viabilidad del proyecto al utilizar la versión de prueba de Azure, que permite a los usuarios probar sus características a un bajo costo inicial, aunque se deben considerar limitaciones de procesamiento y almacenamiento.

Esta revisión del estado actual descubrió trabajos anteriores que abordan cuestiones similares, incluidos los sistemas de reconocimiento de conductores basados en el reconocimiento facial y los sistemas de reconocimiento facial para la prevención del delito. Estos estudios destacan la relevancia y eficacia del reconocimiento facial en aplicaciones de seguridad y control de acceso. Sin embargo, nuestro proyecto destaca por su enfoque en integrar tecnologías avanzadas en plataformas en la nube como Azure, asegurando escalabilidad, flexibilidad y capacidad de adaptación a las diferentes

necesidades.

El marco regulatorio y ético toma en cuenta regulaciones y estándares relacionados con la privacidad y protección de datos personales. Garantizar el cumplimiento de estas normativas era fundamental para asegurar la confianza y aceptación de la solución entre los usuarios y clientes. En resumen, este marco proporcionó una base sólida y diversa para el desarrollo de la solución de reconocimiento facial del Grupo Récord de Colombia. Al integrar aspectos técnicos, de investigación y regulatorios, buscamos brindar soluciones innovadoras, eficientes y éticas que fortalezcan la seguridad y prevengan delitos contra la seguridad personal.

Palabras Claves (Azure Face API, Coincidencia facial, Escalabilidad, Privacidad, Prevención del delito)

5. Antecedentes

Por medio de varias certificaciones Azure como lo son la AI-900 o DP-900, contamos con un conocimiento de la plataforma. Cada certificación tiene un enfoque específico:

- **Azure AI 900**: Esta certificación proporciona una comprensión fundamental de los servicios de inteligencia artificial (IA) de Azure. Esto incluye conceptos como aprendizaje automático, chatbots, servicios cognitivos y visión por computadora. Esta certificación le brinda las habilidades para comprender cómo implementar soluciones de inteligencia artificial utilizando servicios preconfigurados en Azure.
- **Azure DP 900**: DP 900 está enfocado a la computación en la nube usando Azure. Describir los conceptos básicos de almacenamiento, transformación y análisis de datos. Esta certificación le brinda las habilidades para trabajar con servicios de almacenamiento, bases de datos y herramientas de análisis de datos de Azure.

Además, nuestro trabajo se centra en el área de desarrollo y migración utilizando Azure como herramienta principal. Aprovechamos nuestras habilidades en Python para realizar transformaciones y análisis de datos dentro del entorno de Azure. Esto nos permite desarrollar soluciones innovadoras y migrar aplicaciones de manera eficiente en la plataforma.

Palabras Claves (Certificaciones, Azure AI-900, Azure DP-900, Inteligencia artificial, Migración)

6. Objetivos

1. Objetivo General

- Desarrollar una solución de reconocimiento facial basada en inteligencia artificial, adaptada a las necesidades específicas de Grupo Record de Colombia.

2. Objetivos Específicos

- Definir un plan de desarrollo y los requisitos necesarios para el avance de un sistema de reconocimiento facial, centrándonos en la extracción y transformación de datos no estructurada necesaria para entrenar el modelo.
- Desarrollar un servicio personalizado que se especialice en la identificación y análisis de rostros para Grupo Record De Colombia (Segurcol), y Segurtronic Technology Solutions, haciendo énfasis en la fase de Modelamiento de datos.
- Proponer un sistema de reconocimiento facial en las soluciones de control de acceso de **Segurtronic** y Segurtronic Technology Solutions, con un enfoque en el entrenamiento continúo de la autenticación segura y eficiente de empleados y visitantes, utilizando datos recopilados.

7. Viabilidad

Debido a problemas de permisos de Microsoft, no se pudo comprobar la viabilidad de un proyecto de reconocimiento facial de IA en Azure, en cambio, se decidió desarrollar un análisis de imágenes Azure y Python por medio de una librería para el reconocimiento facial. En concreto, necesitábamos un plan detallado que considerara tanto el mundo del big data como el de la inteligencia empresarial; al considerar las características del proyecto, era importante definir claramente las limitaciones y oportunidades que ofrece esta nueva plataforma en el contexto del procesamiento de big data. La implementación en Python y la biblioteca de reconocimiento facial fue una ventaja para las empresas que querían ingresar al mundo del big data y la inteligencia de negocios, ya que les permitió probar diferentes funcionalidades sin mucho esfuerzo inicial, sin embargo, era importante señalar que esta

nueva solución puede tener algunas limitaciones en términos de capacidad de procesamiento y almacenamiento, por lo tanto, tuvimos que diseñar el proyecto dentro de estos límites.

Estas son las funciones que proporciona la implementación en Python y la biblioteca de reconocimiento facial:

- Detección de rostros: Se logró detectar y ubicar rostros en imágenes. Esto es lo que estaba pasando en las aplicaciones donde se reconocen rostros. Lo que era necesario e importante era el reconocimiento, el recuento de personas y el seguimiento facial.
- Análisis de imágenes en Azure: El desarrollo del análisis de imágenes se realizó en Azure para complementar el reconocimiento facial y aprovechar sus capacidades de procesamiento y almacenamiento.
- Rango de edad: Puede estimar el rango de edad de las personas detectadas en una imagen. Esto fue relevante para aplicaciones que requieren análisis demográfico y personalización de contenido.

Palabras Claves (Permisos, Big data, Inteligencia empresarial, Procesamiento, Reconocimiento facial)

8. Metodología

En el desarrollo de un sistema de reconocimiento facial utilizando Python y la librería de análisis de imágenes de Azure Vision, se debe seguir una metodología estructurada que abarca diversas fases, desde la revisión de la literatura hasta la implementación y análisis de datos. A continuación, se describen las fases y los aspectos clave a considerar en cada una de ellas.

Fase 1: Revisión de la Literatura

La primera fase consiste en realizar una revisión de la literatura existente sobre el reconocimiento facial y el análisis de imágenes. Este paso es crucial para comprender el estado actual de la tecnología y las mejores prácticas, así como para identificar lagunas en el conocimiento que el proyecto podría abordar.

1. **Recolección de Datos:**

Qué datos recolectar: Información sobre técnicas y algoritmos de reconocimiento facial, estudios de caso, y avances recientes en el uso de Azure Vision.

Qué datos ignorar: Información obsoleta o no relevante para el uso específico de Azure y Python en el reconocimiento facial.

2. **Diseño de Muestreo:**

Acudir a bases de datos académicas, conferencias sobre inteligencia artificial y foros especializados donde se discuten las últimas investigaciones en el campo.

3. **Métodos de Recolección de Datos:**

Búsqueda en bibliotecas digitales, revisión de artículos científicos, y consultas con expertos en la materia.

4. **Métodos de Análisis de Datos:**

Emplear técnicas de aprendizaje automático para el preprocesamiento, modelado y evaluación de datos. Realizar validación cruzada y ajuste de hiperparámetros para optimizar el rendimiento del modelo.

Fase 2: Implementación en Python

La segunda fase se centra en la implementación práctica del reconocimiento facial utilizando Python con la librería face recognition y el análisis de imágenes con Azure Vision.

1. **Recolección de Datos:**

Qué datos recolectar: Imágenes faciales para entrenamiento y prueba del modelo, parámetros de configuración de Azure Vision, y métricas de rendimiento del modelo.

Qué datos ignorar: Imágenes no relevantes o de baja calidad que no contribuyen al entrenamiento efectivo del modelo.

2. Diseño de Muestreo:

Seleccionar un conjunto diverso de imágenes faciales que incluya diferentes edades, géneros y etnias para asegurar un modelo robusto.

3. Métodos de Recolección de Datos:

Utilizar bases de datos públicas de imágenes faciales, capturar imágenes en entornos controlados y obtener imágenes de fuentes voluntarias con consentimiento informado.

4. Métodos de Análisis de Datos:

Emplear técnicas de aprendizaje automático para el análisis de datos recolectados y ajuste del modelo. Comparar los resultados con estudios previos para situar los hallazgos en un contexto más amplio.

Fase 3: Análisis y Conclusiones

La tercera fase implica analizar los datos recolectados y sacar conclusiones sobre la efectividad del sistema de reconocimiento facial implementado.

1. Recolección de Datos:

Qué datos recolectar: Resultados de precisión, recall, y F1-score del modelo, feedback de usuarios y expertos, y datos de rendimiento en diferentes escenarios.

Qué datos ignorar: Resultados preliminares no validados y datos que no aporten información significativa sobre el rendimiento del modelo.

2. Métodos de Análisis de Datos:

Análisis estadístico de las métricas de rendimiento del modelo y análisis cualitativo del feedback de usuarios y expertos. Comparar los resultados con estudios previos para situar los hallazgos en un contexto más amplio.

Conclusiones

En resumen, la implementación de un sistema de reconocimiento facial con Python y Azure Vision requiere una metodología bien estructurada que abarque desde la revisión de la literatura hasta la implementación práctica y el análisis de resultados. Al considerar cuidadosamente qué datos recolectar, cómo recolectarlos y analizarlos, y al utilizar metodologías de analítica de datos reconocidas, se puede desarrollar una solución robusta, eficiente y ética que fortalezca la seguridad y prevenir delitos.

9. Resultados

Durante el proyecto, hemos creado una solución utilizando tecnologías Azure y Python para análisis de imágenes y reconocimiento facial. Aquí algunos aspectos destacados:

- Implementación en Azure: Configuramos una infraestructura en Azure para gestionar datos, permitiendo un procesamiento y almacenamiento eficaz de imágenes con servicios como Azure Cognitive Services y Azure Storage.

- Desarrollo del Modelo de Reconocimiento Facial en Python: Creamos un modelo de reconocimiento facial usando herramientas de aprendizaje automático en Python, capaz de identificar y autenticar rostros en diversas condiciones.

- Integración en Aplicaciones: Integramos el servicio de reconocimiento facial en aplicaciones existentes de Grupo Record de Colombia y Segurtronic Technology Solutions, realizando pruebas en cámaras de clientes para verificar su desempeño en situaciones reales.

- Análisis Avanzado de Imágenes: Realizamos un análisis detallado de imágenes faciales para mejorar la precisión del reconocimiento, incluyendo extracción de características y comparación con patrones almacenados.

- Seguridad y Privacidad de Datos: Implementamos medidas de seguridad y privacidad para proteger la información facial de los usuarios, cumpliendo con regulaciones pertinentes.

En resumen, nuestro trabajo en Azure y Python para análisis de imágenes y reconocimiento facial ha

mejorado la seguridad y eficiencia en diversos contextos, incluyendo la integración exitosa de servicios de reconocimiento facial en cámaras de clientes para uso en situaciones reales.

Palabras Claves (Azure, Python, Reconocimiento facial, Integración, Seguridad y privacidad de datos)

10. Recomendaciones

En el marco del reconocimiento facial utilizando Azure, se presentan a continuación una serie de aspectos que podrían ser abordados en futuras investigaciones para fortalecer los estudios realizados hasta ahora.

Uno de los principales aspectos a mejorar es la posibilidad de utilizar los recursos de Azure no solo para analizar imágenes, sino también para desarrollar el reconocimiento facial directamente a través de Azure Face API. Esta mejora tendría como objetivo aprovechar las ventajas que ofrece Azure, como su robustez y seguridad, evitando el uso de un código tan abierto como el que se utiliza actualmente en Python.

Cabe destacar que la librería de “face_recognition” está quedando obsoleta con el tiempo. Esto sugiere que, en un futuro cercano, será necesario migrar a un desarrollo totalmente integrado en Azure. En nuestra investigación, nos vimos en la necesidad de instalar y configurar una librería específica de Python, así como descargar e instalar “dlib-for-FaceRecognition-main” para poder utilizar la biblioteca. Adicionalmente, tuvimos que instalar C# y NVIDIA para temas de compatibilidad con el desarrollo y las características del PC.

Estas experiencias subrayan la importancia de seguir avanzando hacia soluciones más integradas y optimizadas dentro del ecosistema de Azure, lo que permitirá simplificar el proceso y mejorar la eficiencia de los sistemas de reconocimiento facial.

El desarrollo en Python presenta varios desafíos que podrían mejorarse con la migración a Azure. Estos incluyen la gestión de dependencias, la necesidad de infraestructura local robusta y la dificultad de escalar las aplicaciones a medida que aumentan las demandas. Azure, por otro lado, ofrece un entorno

de desarrollo más controlado y estandarizado, con herramientas integradas para la gestión de dependencias, recursos de computación elásticos y servicios de seguridad avanzados.

Las empresas se pueden beneficiar enormemente al tener su código en Azure. Primero, se reduce la carga de gestionar infraestructura física, ya que Azure proporciona recursos en la nube que pueden ajustarse dinámicamente según las necesidades. Esto no solo optimiza los costos, sino que también mejora la eficiencia operativa. Segundo, Azure ofrece un alto nivel de seguridad y cumplimiento normativo, protegiendo los datos sensibles y garantizando la privacidad de los usuarios. Tercero, la integración con otros servicios de Azure, como análisis de datos y aprendizaje automático, permite a las empresas innovar y mejorar continuamente sus soluciones de reconocimiento facial.

En conclusión, para futuras investigaciones y desarrollos en el ámbito del reconocimiento facial, sería altamente beneficioso explorar y adoptar las capacidades avanzadas de Azure. Esto no solo mejoraría la robustez y seguridad de las aplicaciones, sino que también optimizaría el proceso de desarrollo, mantenimiento y escalabilidad, proporcionando una solución integral y eficiente para el reconocimiento facial. Las empresas, al migrar a Azure, podrán enfocarse más en la innovación y el crecimiento, aprovechando una plataforma que les ofrece estabilidad, seguridad y escalabilidad.

Palabras Claves (Reconocimiento facial, Azure Face API, Python, Integración, Eficiencia)

11. Referencias

1. Amanullah MHabeeb RNasaruddin FGani AAhmed ENainar AAkim NImran M (2020). *Deep learning and big data technologies for IoT security.* Computer Communications.
2. Ande RAdebisi BHammoudeh MSaleem JS.(2020). *Internet of Things: Evolution and technologies from a security perspective.* Sustainable Cities and Society.
3. Ayub UAhsan SQureshi S (2022). *Scalable Big Data Pipeline for Video Stream Analytics Over Commodity Hardware.*
4. Bagchi TMahapatra AYadav DMishra DPandey AChandrasekhar PKumar A (2020). *Intelligent security system based on face recognition and IoT.* Materials Today: Proceedings.
5. Chang S, Duan Y (2022). *Application of Face Recognition in E-commerce Security Authentication in the Era of Big Data.* Security and Communication Networks.

6. Christakos PPetrellis NMousouliotis PKeramidas GAntonopoulos CVoros N (2023). *A High Performance and Robust FPGA Implementation of a Driver State Monitoring Application.* Sensors.
7. Cobbe JSingh J (2021). *Artificial intelligence as a service: Legal responsibilities, liabilities, and policy challenges.* Computer Law and Security Review.
8. Cuellar M (2023). *A virtue ethical approach to the use of artificial intelligence.* Data and Information Management.
9. Deng S (2023). *Face expression image detection and recognition based on big data technology.* International Journal of Intelligent Networks
10. Intan IPangerang F (2023). *Facial recognition using multi edge detection and distance measure.* IAES International Journal of Artificial Intelligence
11. Joshi RRigau MGarcía-Prieto CCastro de Moura MPiñeyro DMoran SDavalos VCarrión PFerrando-Bernal MOlalde ILalueza-Fox CNavarro AFernández-Tena CAspandi DSukno FBinefa XValencia AEsteller M (2022). *Look-alike humans identified by facial recognition algorithms show genetic similarities.* Cell Reports.
12. Kamil MZaini NMazalan LAhamad A (2023). *Online attendance system based on facial recognition with face mask detection.* Multimedia Tools and Applications.
13. Kim HChoi NKwon HKim H (2023). *Surveillance System for Real-Time High-Precision Recognition of Criminal Faces From Wild Videos.* IEEE Access.
14. Kumar KKasiviswanadham YIndira DPriyanka palesetti PBhargavi C (2023). *Criminal face identification system using deep learning algorithm multi-task cascade neural network (MTCNN).* Materials Today: Proceedings.
15. Naga PMarri SBorreo R (2023). *Facial emotion recognition methods, datasets and technologies: A literature survey.* Materials Today: Proceedings.
16. Naveen raj MR.Vadivel (2023). *Face recognition based attendance system using machine learning with location identification.* World Journal of Advanced Research and Reviews.
17. Nazira FUddin MRaju MHossain SRahman MMridha M (2021). *Face Recognition Based Driver Detection System.* 2021 International Conference on Data Analytics for Business and Industry.
18. Palmiotto FGonzález N (2023). *Facial recognition technology, democracy and human rights.* Computer Law and Security Review.
19. Pantano E (2020). *Non-verbal evaluation of retail service encounters through consumers' facial expressions.* Computers in Human Behavior.
20. Pham TSheta ADo DKing S (2020). *An integrated ambient intelligence system for a Smart Lab environment.* International Journal of Computational Science and Engineering.
21. Preethi SNiranjana Krupa B (2023). *Analyzing lower half facial gestures for lip reading applications: Survey on vision techniques.* Computer Vision and Image Understanding.

22. Principi FBerretti SFerrari COtberdout NDaoudi MDel Bimbo A (2022). *The Florence 4D Facial Expression Dataset.*

23. Rodelas NBallera M (2021). *Intruder detection and recognition using different image processing techniques for a proactive surveillance.* Indonesian Journal of Electrical Engineering and Computer Science.
24. Tighare PBhandekar PKannake R (2021). *International Journal of Scientific Research in Science and Technology.* Identification of Gender from Facial Features.
25. Yin XMa TBouferguene AAl-Hussein M (2021). *Automation for sewer pipe assessment: CCTV video interpretation algorithm and sewer pipe video assessment (SPVA) system development.* Automation in Construction.
26. Zennayi YBenaissa SDerrouz HGuennoun Z (2023). *Unauthorized access detection system to the equipments in a room based on the persons identification by face recognition.* Engineering Applications of Artificial Intelligence.
27. Zhang YWu MTian GZhang GLu J (2021). *Ethics and privacy of artificial intelligence: Understandings from bibliometrics.* Knowledge-Based Systems.
28. Zhang JZheng KMazhar SFu XKong J (2023). *Trusted emotion recognition based on multiple signals captured from video.* Expert Systems with Applications.
29. Sulthana MRaju C (2023). *Newton's Law of Gravitational Force (NLGF) based Machine Learning Technique for Uneven Illuminated Face Detection.* International Journal on Recent and Innovation Trends in Computing and Communication.
30. Chang SDuan Y (2022). *Application of Face Recognition in E-commerce Security Authentication in the Era of Big Data.* Security and Communication Networks.
31. https://learn.microsoft.com/en-us/credentials/certifications/azure-ai-fundamentals/?practice-assessment-type=certification#certification-prepare-for-the-exam
32. https://learn.microsoft.com/es-es/azure/ai-services/computer-vision/quickstarts-sdk/identity-client-library?tabs=windows%2Cvisual-studio&pivots=programming-language-python
33. https://learn.microsoft.com/es-es/azure/ai-services/computer-vision/how-to/specify-detection-model
34. https://learn.microsoft.com/es-es/azure/ai-services/computer-vision/overview-identity