SISTEMA DE SEGURIDAD VEHICULAR BASADO EN EL RECONOCIMIENTO DEL PROPIETARIO

VEHICLE SAFETY SYSTEM BASED ON OWNER RECOGNITION

ARTÍCULO DE INVESTIGACIÓN

García, Adriel [1]
UVP Universidad del Valle de Puebla
im42659@uvp.edu.mx
ORCID: 0009-0002-8603-6778

López, Sergio [2]
UVP Universidad del Valle de Puebla
sergio.lopez@uvp.edu.mx
ORCID: 0000-0001-9762-8109

Recibido el 29 de mayo de 2024. Aceptado el 1 de julio de 2024. Publicado el 31 de agosto de 2024.

Reseña de Autor [1]

Estudiante de la Licenciatura en Ingeniería Mecatrónica. Durante mi formación académica, he tenido la oportunidad de participar en diversas actividades y proyectos que han enriquecido mi conocimiento y experiencia en el campo.

- Experiencia Académica y Proyectos
  - Expo ciencias en la UPAEP:
    - Tema: Telemetría.
    - Descripción: Participé en este evento, presentando un proyecto que se centraba en la recopilación y transmisión de datos a distancia.
  - Servicio Social con CONCYTEP:
    - Proyecto: Elaboración de una CNC.
    - Descripción: Durante mi estancia en el servicio social, colaboré en la construcción de una máquina CNC (Control Numérico por Computadora), lo que me permitió adquirir conocimiento en el funcionamiento del equipo.
  - Prácticas Profesionales con Grupo ACCIONA:
    - Área: Mantenimiento Operacional.
    - Descripción: Realicé mis prácticas profesionales en la Torre Inxignia del banco BBVA, trabajando con el Grupo Acciona, un servicio externo especializado en el mantenimiento y limpieza. Aquí, desarrollé conocimientos en equipos HVAC (calefacción, ventilación y aire acondicionado), participando en el mantenimiento y optimización de estos sistemas críticos para el confort y la eficiencia energética.

Mi experiencia en estas áreas ha sido fundamental para mi desarrollo como ingeniero mecatrónico, proporcionándome una visión integral de cómo aplicar la teoría en proyectos prácticos y reales. Estoy comprometido con la mejora continua.

Reseña de Autor [2]

Ingeniero Industrial por el Tecnológico Nacional de México Campus Puebla, Maestro en Ingeniería Administrativa y Calidad por la Universidad La Salle Benavente, Doctor en Alta Dirección por la Universidad del Valle de Puebla.

Posdoctor en Administración de Negocios por el Centro de Estudios e Investigaciones para el Desarrollo Docente. TSU en Gestión y Administración de PyME por la Universidad Abierta y a Distancia de México.

Ha colaborado con organizaciones privadas de los sectores manufacturero, comercial y de servicios implementando Sistemas de Gestión de Calidad, desarrollado y mejorando procesos, gestionando información de sistemas y aplicándola en la toma de decisiones.

Ha trabajado en publicaciones e impartido conferencias en diversas instituciones como BUAP, UPAEP, CEUNI, IEU, UVP, etc., relacionadas con temas de liderazgo, productividad, motivación, marketing, ingeniería y uso de la información en procesos de investigación.

Resumen

Se comienza con una revisión exhaustiva de las técnicas actuales de reconocimiento facial y la adquisición de imágenes, utilizando el lenguaje de programación Python para el procesamiento y reconocimiento de rostros.

Se implementó un sistema de captura de imágenes con la cámara del dispositivo electrónico, que tomó y almacenó 300 fotografías del rostro del propietario. Estas imágenes fueron utilizadas para entrenar un modelo de reconocimiento facial basado en el método EigenFaces, con la biblioteca OpenCV de Python. El modelo fue evaluado para garantizar su precisión y efectividad en la identificación del propietario y la detección de rostros desconocidos.

Este proyecto no solo contribuye a la tecnología de seguridad vehicular, sino que también ofrece una base sólida para futuras investigaciones y mejoras en el campo del reconocimiento facial y la prevención del robo de automóviles.

Palabras clave: Eigenface, reconocimiento facial, seguridad vehicular, OpenCV, Python.

Abstract

The present research began with a comprehensive review of current facial recognition techniques and image acquisition, using the Python programming language for face processing and recognition.

An image capture system was implemented using a camera connected to the software, which took and stored 300 photographs of the owner's face. These images were used to train a facial recognition model based on the EigenFaces method, using the OpenCV Python library. The model was evaluated to ensure its accuracy and effectiveness in identifying the owner and detecting unknown faces.

This project not only contributes to vehicle security technology, but also provides a solid foundation for future research and improvements in the field of facial recognition and car theft prevention.

Keywords: Eigenface, facial recognition, vehicle security, OpenCV, Python

Introducción

Actualmente la creciente búsqueda de proteger de manera eficiente un vehículo se ha vuelto esencial. El robo de automóviles es una realidad que año tras año crece, y el estado de Puebla no escapa a esta problemática. Los crecientes métodos utilizados por los ladrones exigen respuestas igualmente avanzadas para salvaguardar el robo de vehículos de cada uno de los usuarios, por lo que dicha investigación explora el panorama sobre el robo de vehículos en el estado de Puebla durante el período 2023-2024.

El objetivo principal es desarrollar un sistema de seguridad vehicular basado en el reconocimiento del propietario, una innovadora propuesta que busca no solo prevenir el robo de automóviles, sino también elevar los estándares de seguridad para los propietarios de vehículos Nissan Versa.

El primer paso de esta indagación implica un análisis exhaustivo de las estrategias de robo de automóviles más utilizadas en el Estado de Puebla. Comprender las tácticas empleadas por los delincuentes es esencial para diseñar un sistema de seguridad que aborde estas vulnerabilidades de manera efectiva.

La clasificación de estrategias de prevención de robo se presenta como la segunda fase de esta investigación. Identificar y evaluar las medidas existentes permite destacar las mejores prácticas y determinar áreas de mejora. Este análisis crítico sienta las bases para la propuesta de un sistema de seguridad innovador y específico para los vehículos Nissan Versa.

El componente central de esta investigación consiste en la evaluación de la viabilidad técnica de implementar un sistema de seguridad vehicular basado en el reconocimiento del propietario. Esta evaluación asegura que la solución propuesta no solo sea efectiva desde el punto de vista técnico, sino también práctica.

Al abordar esta problemática desde múltiples perspectivas, esta investigación no solo busca desarrollar un sistema de seguridad avanzado, sino también contribuir al bienestar de la sociedad poblana al proporcionar soluciones efectivas y asequibles.

Planteamiento del problema

Actualmente la creciente preocupación por la seguridad de los automóviles y la necesidad de combatir el robo, además que ha llegado a afectar a dichos propietarios en momentos como estacionarse en lugares públicos que en algunos casos este hecho sucede para cometer otros actos delictivos.

Por lo que, la seguridad de un automóvil es de gran importancia y que han impulsado por soluciones innovadoras y de este modo buscar la manera de eficientizar cada uno de los sistemas. Dado que "un sistema de alerta consiste en la instalación de equipos electrónicos que están ubicados en lugares estratégicos desde el punto de vista de la seguridad" (García et al., 2020), brindando así una mayor tranquilidad a los propietarios.

De acuerdo con el estudio de la INTERPOL y con apoyo de la base de datos sobre Vehículos de Motor Robados (SMV) señaló que, a nivel mundial, "en 2020, se registraron más de 7,533,193 vehículos de motor fueron identificados como robados" (INTERPOL, 2023). Aunque dicho dato puede ser erróneo debido a que aproximadamente 135 países registraron sus datos sobre vehículos robados a nivel nacional por lo que dicha cifra puede elevarse aún más.

Como respuesta a esta problemática, la dependencia propuso una solución concreta: la implementación del curso denominado FORMATRAIN. Este curso está diseñado para proporcionar a los participantes las habilidades necesarias en la identificación de vehículos, el uso efectivo de herramientas de investigación, así como la explotación de bases de datos y su conexión a la red mundial.

Lo mencionado conduce a que obtenga el apoyo de 11 naciones miembros y se compone de oficiales de policía e investigadores privados, todos ellos expertos en la investigación de delitos vinculados a vehículos, sin embargo, el poco apoyo brindado conduce a que no se solucione de una forma más eficiente la recuperación de un vehículo.

Por lo que, a nivel nacional, de acuerdo con el estudio realizado por Lundy (2021), durante el periodo 2020 - 2021, se registraron alrededor de 62, 563 vehículos robados siendo "ese año, al igual que el año pasado, la zona centro de México domina el robo de autos" (Lundy, 2021), al igual que el presente estudio nos menciona que Baja California Sur tiene el menor número de robos de vehículos. De igual importancia Lundy (2021), resaltan que los automóviles con seguro, las mismas aseguradoras han logrado recuperar alrededor del 40% de los automóviles robados.

Por consiguiente, en el estado de Puebla el estudio que se tiene por parte de Fiscalía General del Estado de Puebla (2023), en ese periodo se cometieron 5,623 casos de robos de vehículos. Estos incidentes ocurrieron de diversas formas, tanto con violencia como sin ella, y afectaron a una variedad de tipos de vehículos.

Por tanto, la falta de seguridad en los vehículos no solo pone en riesgo la seguridad de las personas, sino que también acarrea pérdidas económicas significativas. A pesar de los avances en la localización de vehículos mediante tecnologías como RFID, GSM y GPS, se ha observado que la eficiencia de estas soluciones se manifiesta una vez que el automóvil ha sido robado. Además, las estadísticas recientes muestran un aumento preocupante en el robo de vehículos.

Esto subraya la necesidad apremiante de la automatización de los sistemas de seguridad vehicular, ya que incluso con sistemas de localización implementados, los vehículos siguen siendo vulnerables en muchas ocasiones. Por todo lo anterior, la pregunta de investigación resultante es la siguiente:

¿Cómo mejora la prevención del robo de vehículos Nissan Versa el desarrollo de un sistema de seguridad vehicular basado en el reconocimiento del propietario en el estado de Puebla en el periodo 2023-2024?

Para abordar esta cuestión, se han establecido los siguientes objetivos:

Objetivo general

Desarrollar una propuesta sobre un sistema de seguridad vehicular basado en el reconocimiento del propietario para la prevención del robo de vehículos Nissan Versa en el estado de Puebla en el periodo 2023-2024.

Objetivo específico

- Nombrar las estrategias usualmente utilizadas para el robo de automóviles en el estado de Puebla en el periodo 2023-2024.
- Clasificar las diversas estrategias utilizadas para prevenir el robo de vehículos en el estado de Puebla durante el período 2023-2024.
- Demostrar la viabilidad técnica de implementar un sistema de seguridad vehicular basado en el reconocimiento del propietario en el estado de Puebla durante el período 2023-2024.

Revisión bibliográfica

De acuerdo con lo mencionado por Alanís et al. (2018), se aborda un sistema de reconocimiento de placas vehiculares que incluye el reconocimiento automático

de matrículas (LPR) y se analiza la funcionalidad de este sistema en términos de monitoreo y localización de vehículos.

Por otro lado, para Guerra Martínez (2018), los sistemas en las redes automotrices abordan la simulación de la comunicación en el protocolo CAN mediante la utilización de un microcontrolador, específicamente Arduino. El propósito central radica en la evaluación y análisis de las posibles fallas y errores inherentes a esta comunicación.

Dentro del contexto de las redes automotrices, el objetivo de dicho estudio es la prevención de ataques y el robo de información, problemáticas actuales y de gran relevancia. En adición, el autor introduce un modelo de ataque de tipo “Negación de Servicio” (DoS) dirigido al protocolo CAN. De igual forma menciona que este protocolo es ampliamente reconocido por sus múltiples ventajas, incluida su alta inmunidad a interferencias, lo que optimiza la comunicación entre diversos subsistemas en una red compartida.

De este modo, para la obtención del reconocimiento fácil Esparza et al. (2024), en el estudio que realizo en donde se pretende el reconocimiento facial mediante el procesamiento de imágenes, al aplicar patrones como Eigenfaces, histogramas de patrones locales binarios y los discriminantes Fischer faciales los cuales se sometieron a varias pruebas y de esta forma evaluar cuál método es el más eficiente en donde los resultados son mostrados mediante la tabla 1 y la tabla 2.

Tabla 1.

Resultados de las pruebas de error en el portátil.

Eigenfaces		LBPH		Fisherfaces	
Efic.(%)	Tiempo (ms)	Efic. (%)	Tiempo (ms)	Efic. (%)	Tiempo (ms)
97	4.67	96	28.95	94	3.42

Nota. Esparza et al., 2024, Revista Colombiana de Tecnologías de Avanzada: https://www.academia.edu/download/78513215/1183.pdf

Tabla 2.

Resultados de las pruebas de falsos positivos en el portátil.

Eigenfaces		LBPH		Fisherfaces	
Efic. (%)	Tiempo (ms)	Efic. (%)	Tiempo (ms)	Efic. (%)	Tiempo (ms)
0	5.6	0	26.9	6	3.4

Nota. Esparza et al., 2024, Revista Colombiana de Tecnologías de Avanzada: https://www.academia.edu/download/78513215/1183.pdf

Por otra parte, se presenta el uso de tecnología como es el identificador por radiofrecuencia (RFID) es una opción donde V. J. Acevedo Duran, A. García Sandoval y J. S. Sandino Ariza (2016) como se citó Aguilar et al. (2019) "se puede usar donde se requiera un continuo almacenamiento de datos y se tiene un difícil acceso a datos en algunos procesos como lo son el control de inventarios, movimiento de mercancías, control de acceso a vehículos, sistemas de librerías".

Por ello, Aguilar et al. (2019) abordan en su artículo el papel de la tecnología de microchips en la obtención de información vehicular mediante la exploración de como el sistema es capaz de contribuir a la identificación precisa de vehículos. Asimismo, se analiza la incorporación de tecnologías de la información y las telecomunicaciones

(TIC) en la implementación de herramientas como cámaras y radares de velocidad, que desempeñan un papel crucial en la validación de la información.

Sin embargo, para la prevención de robo de vehículos Bedolla y Bedolla (2023), en dicho estudio el autor presenta la creación de una aplicación que, mediante la autorización para las autoridades competentes, tiene como objetivo informar sobre aspectos clave como el color y la matrícula del vehículo.

Esta aplicación busca eficientizar la recuperación de vehículos en casos de robo, lo que minimizaría las pérdidas económicas para los propietarios. Para lograr este propósito, se implementan herramientas tecnológicas como el sistema de posicionamiento global (GPS) y el sistema global para las comunicaciones móviles (GSM), las cuales permiten un seguimiento y localización efectiva del automóvil. Además, el estudio ofrece una visión panorámica de la problemática de los actos delictivos de robo de vehículos.

Método y Metodología

La presente investigación corresponde al diseño no experimental derivado de que las variables no se manipularán en ningún momento. A partir de lo anterior se pueden tener estudios con carácter transversal o transeccional y longitudinal. En el estudio transversal, el investigador realiza estudios con la misma variable y se realiza una sola vez. Derivado de ello, esta investigación tiene un carácter transversal o transeccional.

Por lo tanto, dicha investigación es de nivel descriptivo debido a se pretende conocer, identificar, describir las características de fenómeno, por lo que se considera una circunstancia temporal-espacial.

Tradicionalmente, existen dos enfoques de investigación: el cualitativo y el cuantitativo, sin embargo, la investigación se centra en un enfoque de tipo mixta que consiste en recopilar, analizar e integrar tanto investigación cuantitativa como cualitativa. Este enfoque se utiliza cuando se requiere una mejor comprensión del problema de investigación, y que no te podría dar cada uno de estos métodos por separado.

De esta manera dicha investigación se basa mediante la siguiente metodología propuesta:

- Búsqueda de información de sistemas de reconocimiento facial:
  - Realizar una revisión exhaustiva de la literatura científica, artículos especializados, libros y recursos en línea relacionados con los sistemas de reconocimiento facial.
  - Identificar los principios básicos, algoritmos, tecnologías y aplicaciones más relevantes en el campo del reconocimiento facial.

- Investigación de múltiples programas para la adquisición de imágenes:
  - Explorar diferentes programas y herramientas que permitan la captura de imágenes de manera efectiva y eficiente.
  - Evaluar las características, funcionalidades y compatibilidad de cada programa con los requisitos del proyecto.

- Detección de rostros mediante el lenguaje de programación de Python con Visual Studio Code:
  - Utilizar Python y Visual Studio Code para programar algoritmos de detección de rostros utilizando bibliotecas como OpenCV.
  - Desarrollar scripts y programas que permitan la detección precisa de rostros en imágenes y vídeos.

- Almacenamiento de imágenes para el entrenamiento de la detección de rostro:

- Crear una base de datos de imágenes que contenga ejemplos de rostros tanto reconocidos como desconocidos.
- Organizar y etiquetar las imágenes de manera adecuada para su uso en el entrenamiento de algoritmos de detección facial.

- Realización del entrenamiento de detección del rostro mediante las imágenes almacenadas:
  - Utilizar las imágenes almacenadas para entrenar modelos de detección de rostros utilizando técnicas de aprendizaje automático y redes neuronales.
  - Ajustar y optimizar los parámetros del modelo para mejorar su precisión y rendimiento.

- Detección de rostro muestre desconocido a aquellas imágenes que no son reconocidas:
  - Implementar un sistema que, basado en los modelos entrenados, pueda distinguir entre rostros reconocidos y desconocidos.
  - Configurar el sistema para mostrar una etiqueta de "desconocido" cuando se detecte un rostro que no esté presente en la base de datos de rostros conocidos.

Población

En esta investigación, no se considera una población específica, ya que el enfoque se centra en un caso de estudio particular. El objetivo es beneficiar a través de este caso de estudio, sin identificar una población definida para el mismo.

Resultados

En el transcurso de esta investigación, se desarrolló un programa utilizando el lenguaje de programación Python a través del entorno de desarrollo integrado (IDE) Visual Studio Code. El primer paso consistió en el almacenamiento de múltiples

imágenes, para lo cual se implementó el siguiente código en Visual Studio Code como se muestra en la figura 1.

Figura 1.

Código de almacenamiento de rostros

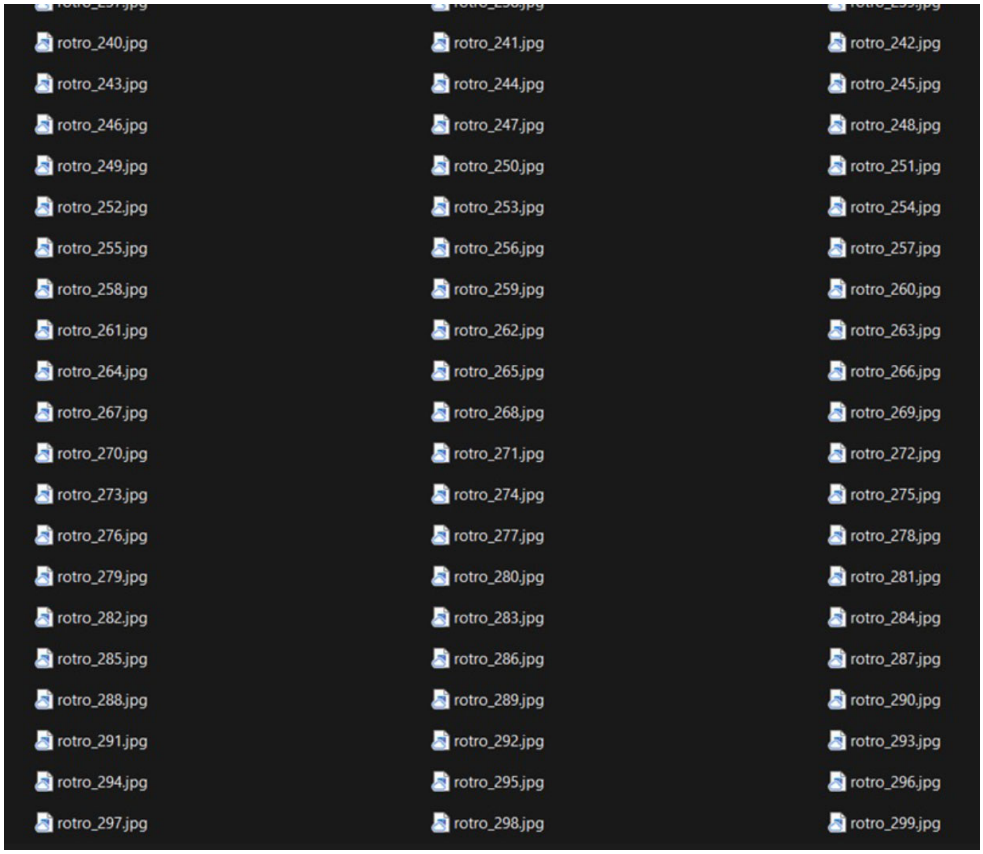
```python
import cv2
import os
import cv2.data
import imutils

nomarch = ''
dir = ''
crear = dir + '/' + nomarch

if not os.path.exists(crear):
    print('Carpeta creada: ', crear)
    os.makedirs(crear)

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

clasface = cv2.CascadeClassifier(
    cv2.data.haarcascades + 'haarcascade_frontalface_default.xml')
count = 350

while True:
    paus, vent = cap.read()
    if paus == False:
        break
    vent = imutils.resize(vent, width=700)
    gris = cv2.cvtColor(vent, cv2.COLOR_BGR2GRAY)
    auxvent = vent.copy()
    ros = clasface.detectMultiScale(gris, 1.3, 5)

    for (x, y, w, h) in ros:
        # Dibuja un rectángulo alrededor de cada rostro detectado.
        cv2.rectangle(vent, (x, y), (x+w, y+h), (0, 255, 0), 2)
        rostro = auxvent[y:y+h, x:x+w]  # Recorta el rostro de la imagen
        # Redimensiona el rostro a un tamaño específico.
        rostro = cv2.resize(rostro, (200, 200), interpolation=cv2.INTER_CUBIC)
        # Guarda el rostro recortado como una imagen.
        cv2.imwrite(crear + '/rotro_{}.jpg'.format(count), rostro)
        count += 1

    cv2.imshow('Ventana', vent)
    k = cv2.waitKey(1)
    if k == 27 or count >= 420:
        break

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


Nextia, año 12, núm. 21
ISSN 2683-1988

De este modo se logró exitosamente almacenar las 300 imágenes dentro de la carpeta designada, tal como se muestra en la figura 2.

Figura 2.

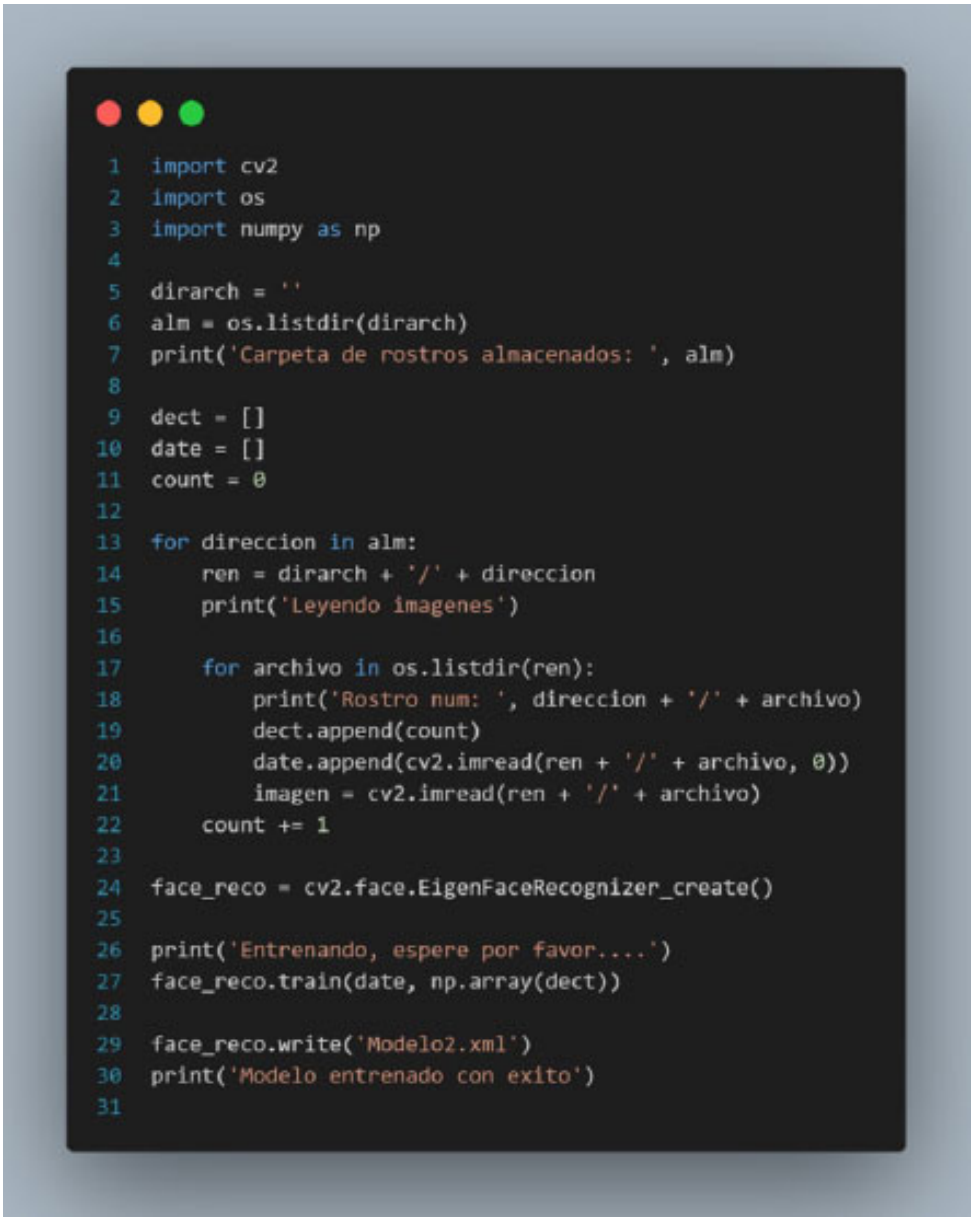
Almacenamiento de imágenes



De esta manera se procedió al entrenamiento utilizando el método Eigenfaces, el cual, según Esparza et al. (2024), ha demostrado ser altamente efectivo. A continuación, se presenta el código utilizado para iniciar el entrenamiento como se muestra en la figura 3.

Figura 3.

Código para la creación de los patrones numéricos de los rostros almacenados



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

dirarch = ''
alm = os.listdir(dirarch)
print('Carpeta de rostros almacenados: ', alm)

dect = []
date = []
count = 0

for direccion in alm:
    ren = dirarch + '/' + direccion
    print('Leyendo imagenes')

    for archivo in os.listdir(ren):
        print('Rostro num: ', direccion + '/' + archivo)
        dect.append(count)
        date.append(cv2.imread(ren + '/' + archivo, 0))
        imagen = cv2.imread(ren + '/' + archivo)
    count += 1

face_reco = cv2.face.EigenFaceRecognizer_create()

print('Entrenando, espere por favor....')
face_reco.train(date, np.array(dect))

face_reco.write('Modelo2.xml')
print('Modelo entrenado con exito')

```

Al mismo tiempo se generan los patrones numéricos correspondientes a las imágenes recopiladas como se muestra en la figura 4.

Figura 4.

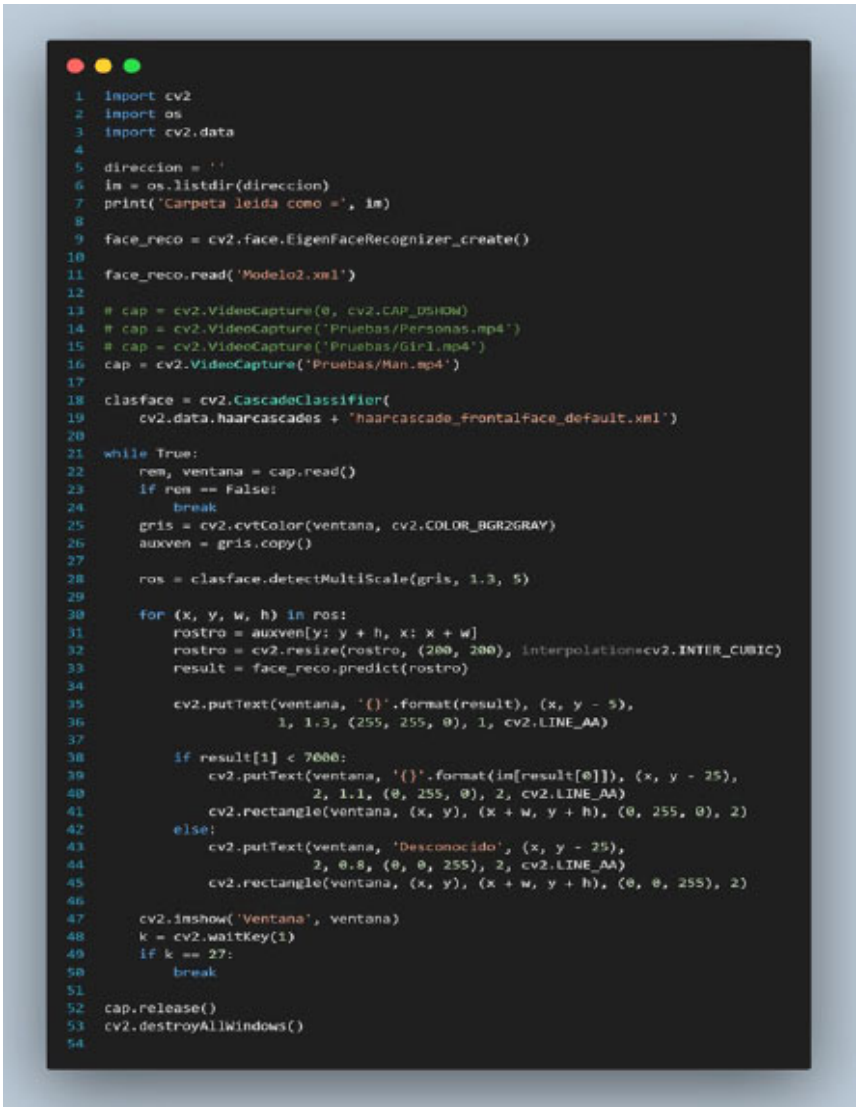
Creación de los patrones numéricos de los rostros almacenados.

```
<?xml version="1.0"?>
<opencv_storage>
<opencv_eigenfaces>
  <threshold>1.7976931348623157e+308</threshold>
  <num_components>300</num_components>
  <mean type_id="opencv-matrix">
    <rows>1</rows>
    <cols>40000</cols>
    <dt>d</dt>
    <data>
      1.3388666666666668e+02 1.3044333333333333e+02
      1.2679000000000001e+02 1.2194666666666667e+02
      1.1675000000000001e+02 1.1117000000000000e+02
      1.0462000000000000e+02 9.9420000000000002e+01
      9.4646666666666675e+01 8.8293333333333337e+01
      8.2109999999999999e+01 7.5620000000000005e+01
      7.0736666666666665e+01 6.5680000000000007e+01
      5.8520000000000003e+01 5.0483333333333334e+01
      4.3130000000000003e+01 3.8386666666666670e+01
      3.5123333333333335e+01 3.3023333333333333e+01
      3.1426666666666669e+01 3.0083333333333336e+01
      2.8856666666666669e+01 2.7873333333333335e+01
      2.6673333333333336e+01 2.5383333333333336e+01
      2.3920000000000002e+01 2.2053333333333335e+01
      2.0193333333333335e+01 1.8883333333333333e+01
      1.8183333333333334e+01 1.7313333333333336e+01
      1.6186666666666667e+01 1.5233333333333334e+01
      1.4593333333333334e+01 1.4036666666666667e+01
      1.3820000000000000e+01 1.3523333333333333e+01
      1.3386666666666667e+01 1.2823333333333334e+01
      1.2623333333333335e+01 1.2286666666666667e+01
      1.2056666666666667e+01 1.2063333333333334e+01
      1.1973333333333334e+01 1.1916666666666668e+01
      1.2076666666666668e+01 1.2313333333333334e+01
      1.2626666666666667e+01 1.2870000000000001e+01
      1.3303333333333335e+01 1.3876666666666667e+01
      1.4690000000000001e+01 1.5490000000000000e+01
```

Posteriormente, a partir del código, se generó un archivo con extensión XML donde se almacenó el patrón numérico de los rostros capturados. Con este archivo, se creó un modelo que permitirá el reconocimiento de los rostros almacenados, asignando el nombre correspondiente o la leyenda 'Desconocido' a quienes no fueron entrenados. A continuación, se muestra el código resultante como se muestra en la figura 5.

Figura 5.

Código para el reconocimiento facial



```python
import cv2
import os
import cv2.data

direccion = ''
im = os.listdir(direccion)
print('Carpeta leida como =', im)

face_reco = cv2.face.EigenFaceRecognizer_create()

face_reco.read('Modelo2.xml')

# cap = cv2.VideoCapture(0, cv2.CAP_DSHOW)
# cap = cv2.VideoCapture('Pruebas/Personas.mp4')
# cap = cv2.VideoCapture('Pruebas/Girl.mp4')
cap = cv2.VideoCapture('Pruebas/Man.mp4')

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

while True:
    rem, ventana = cap.read()
    if rem == False:
        break
    gris = cv2.cvtColor(ventana, cv2.COLOR_BGR2GRAY)
    auxven = gris.copy()

    ros = clasface.detectMultiScale(gris, 1.3, 5)

    for (x, y, w, h) in ros:
        rostro = auxven[y: y + h, x: x + w]
        rostro = cv2.resize(rostro, (200, 200), interpolation=cv2.INTER_CUBIC)
        result = face_reco.predict(rostro)

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

        if result[1] < 7000:
            cv2.putText(ventana, '{}'.format(im[result[0]]), (x, y - 25),
                        2, 1.1, (0, 255, 0), 2, cv2.LINE_AA)
            cv2.rectangle(ventana, (x, y), (x + w, y + h), (0, 255, 0), 2)
        else:
            cv2.putText(ventana, 'Desconocido', (x, y - 25),
                        2, 0.8, (0, 0, 255), 2, cv2.LINE_AA)
            cv2.rectangle(ventana, (x, y), (x + w, y + h), (0, 0, 255), 2)

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

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

Al realizar las pruebas, se obtuvieron los siguientes resultados, los cuales fueron favorables y coinciden con los objetivos planteados, tal como se muestra en la tabla 3.

Tabla 3.

Resultados de la respuesta del sistema

Métricas	Valor (%)
Precisión	92.5
Tasa de verdaderos positivos	90.3
Tasa de falsos positivos	5.2
Número de imágenes de prueba	300

Análisis de Resultados

- Precisión: La precisión del 92.5% indica que el sistema puede identificar correctamente los rostros la mayoría del tiempo.
- Tasa de verdaderos positivos: Una tasa de verdaderos positivos del 90.3% sugiere que el sistema es bastante efectivo en reconocer los rostros que están en su base de datos.
- Tasa de falsos positivos: Una tasa de falsos positivos del 5.2% indica que el sistema ocasionalmente identifica incorrectamente a un rostro desconocido como conocido, lo cual es un área a mejorar.

Conclusiones y discusión

Los resultados obtenidos destacan la alta precisión y efectividad del sistema de reconocimiento facial desarrollado. La comparación realizada por Esparza et al. (2024), proporcionó un marco de referencia valioso para la implementación del modelo de reconocimiento facial utilizado en este proyecto. Sin embargo, la tasa de falsos positivos sugiere que existe margen para mejorar la discriminación entre rostros conocidos y desconocidos. Por lo tanto, futuros trabajos pueden enfocarse

en la optimización del modelo y la reducción de falsos positivos aumentando el número de rostros para fortalecer la robustez del sistema, de acuerdo a la tabla 4, muestra los resultados preliminares del sistema.

Tabla 4.

Resultados de la respuesta del sistema.

Partida	Distancia (metros)	Tiempo de respuesta	Consumo de energía al activar la seguridad	
			No	Si
1	1	Alto	Baja	Baja
2	2	Alto	Baja	Baja
3	3	Medio	Baja	Media
4	4	Medio	Media	Media
5	5	Bajo	Media	Alta
6	6	Bajo	Media	Alta
7	7	Bajo	Media	Alta

Estos resultados son fundamentales para respaldar la validez del sistema propuesto y su potencial aplicación en situaciones reales, como la seguridad vehicular, donde la identificación precisa y rápida de los usuarios es crucial. En conjunto, estos hallazgos subrayan la importancia del método utilizado y su impacto en el desarrollo de soluciones efectivas para mejorar la seguridad y prevenir el robo de vehículos.

Además del impacto en la seguridad, el desarrollo e implementación de este sistema de reconocimiento facial pueden tener implicaciones económicas significativas. Un sistema de seguridad más robusto y preciso puede reducir los

Nextia, año 12, núm. 21
ISSN 2683-1988

costos asociados con el robo de vehículos, aunque podría incrementar el costo inicial del automóvil para el usuario. Por lo tanto, esta investigación no solo contribuye a la mejora de la seguridad vehicular, sino que también tiene el potencial de generar beneficios económicos sustanciales.

Referencias

Alanís Carranza, L. E., Márquez Olivera, M. V., Hernández Herrera Olivera, V. G., & Sánchez García, O. (diciembre de 2018). Sistema de reconocimiento de placas vehiculares haciendo uso de modelos asociativos. *Research in Computing Science,* 147(12), 127-136. https://www.researchgate.net/publication/339203202_Sistema_de_reconocimiento_de_placas_vehiculares_haciendo_uso_de_modelos_asociativos

Aguilar Rodríguez, W. G., Aguilar Rodríguez, W. L., & Leguizamón Páez, M. A. (2 de junio de 2019). Tecnología Microchip Para Acceder a Información Vehicular Como Apoyo a Procesos de Control y Seguridad. *Scientia Et Technica*, 24(2), 263-274. https://doi.org/10.22517/23447214.20241

Bedolla, J., & Bedolla, J. (13 de Junio de 2023). Sistema de Reporte y Localización de Vehículos Robados. COCYTIEG, 7(1), 877-888. https://revistafesgro.cocytieg.gob.mx/index.php/revista/article/view/486

Esparza Franco, C. H., Tarazona Ospina, C., Sanabria Cuevas, E. E., & Velazco Capacho, D. A. (17 de abril de 2024). Reconocimiento facial basado en Eigenfaces, LBHP Y Fisherfaces en la Beagleboard-xm. *Revista Colombiana de Tecnologías de Avanzada*, X(XX), 145-152. https://www.academia.edu/download/78513215/1183.pdf

Fiscalía General del Estado de Puebla. (10 de Septiembre de 2023). Incidencia delictiva del fuero común enero - agosto 2023. *Fiscalía General del Estado de Puebla*. https://fiscalia.puebla.gob.mx/index.php/informacion-socialmente-util/incidencia-delictiva-por-municipio

García Torres, I. A., Castillo León, R. E., Dominguez De La Torre, L. J., & Parra López , R. A. (3 de Enero de 2020). Sistema de alerta usando Módulo de Reconocimiento de voz para detectar problemas de robo de vehículos. *Journal of business and entrepreneurial studies*, 4(1), 1-13. https://www.redalyc.org/articulo.oa?id=573667940024

Guerra Martínez, L. B. (14 de Mayo de 2018). *Seguridad en las redes automotrices* - Modelo de ataque en el protocolo CAN [Tesis de Licenciatura, Universidad de las Américas Puebla]. Reposito-

rio institucional de la Universidad de las Américas Puebla. http://catarina.udlap.mx/u_dl_a/tales/documentos/lir/guerra_martinez_lb/

INTERPOL. (14 de Octubre de 2023). La delincuencia relacionada con los vehículos afecta a todas las regiones del mundo y tiene claros vínculos con la delincuencia organizada y el terrorismo. INTERPOL. https://www.interpol.int/es/Delitos/Delincuencia-relacionada-con-los-vehiculos

Lundy, C. (14 de Marzo de 2021). Estadísticas de Robo de Vehículos México. Mexico Insurance Services INC. https://www.mexinsurance.com/es/estadisticas-de-robo-de-vehiculos/#