








Analysis of the use of Convolutional Neural Networks for facial recognition in the district of San Juan de Lurigancho

Guadalupe Mori Víctor Hugo¹, Benites Gómez Rafael Eduardo Sebastián¹, Rayme Serrano Rubén Alejandro¹, Coaquira Torres Edgar¹, Huerta Rojas Miguel Angel¹, Rivera Echegaray Luis Alberto¹, and Ogosi Auqui José Antonio²

¹Universidad Privada San Juan Bautista, Perú, victor.guadalupe@upsjb.edu.pe, rafael.benites@upsjb.edu.pe, ruben.rayme@upsjb.edu.pe, edgar.coaquira@upsjb.edu.pe, miguel.huertar@upsjb.edu.pe, luis.riverae@upsjb.edu.pe

²Universidad Nacional Federico Villarreal, Perú, jogosi@unfv.edu.pe

Abstract– *In recent years the use of artificial intelligence has become popular due to its effectiveness to learn automatically as it emulates the behavior of a human brain processing data and information that manages to perceive creating patterns to make decisions, this is achieved thanks to neural networks, there are several types of neural networks, which differ in their structure, how they process information and how they learn from it, which is why each one has different applications and can be used in different contexts depending on the type of problem it addresses. In this project we will analyze convolutional neural networks and their relevance in image analysis to later use it in facial recognition, training it in the detection of faces through images from different angles considering the triangular pattern of the face in order to identify people to provide better public safety through video surveillance.*

Keywords– *Convolutional neural networks (CNNs), facial recognition, video surveillance*

I. INTRODUCTION

Facial recognition is a biometric technique used to identify a person from his or her face.

used to identify a person from his or her face.

Convolutional neural networks are a type of machine learning that has been successfully used in face recognition in many countries around the world.

Face recognition technology (FRT) is a tool that is increasingly being used in both the private and public sector. This technology has the potential to improve security, efficiency and user experience. However, it also raises many controversies as some say it is affecting privacy and data protection.

II. BACKGROUND OF THE RESEARCH

In Peru and in many other countries, TRF is being used in a variety of sectors such as product and service recognition, mobile payments, identity authentication and automatic photo tagging. The Peruvian regulatory framework relating to data protection is relatively straightforward and there is already a law in Peru that protects the privacy and data protection of individuals. This is Law No. 29733, the Personal Data Protection Law, which was enacted in 2011. This law establishes the principles and rules for the protection of

personal data of natural persons, whether sensitive or non-sensitive data. Personal data is any information about a natural person that identifies him/her or makes him/her identifiable, such as his/her name, surname, address, telephone, email, among others.

The law establishes the following rights of the holders of personal data:

1. Right to information: The holder has the right to be informed about the purpose and use of his/her personal data.
2. Right to rectification: The holder has the right to have his/her personal data rectified if it is inaccurate or incomplete.
3. Right to cancellation: The holder has the right to have his/her personal data cancelled if it is no longer necessary for the purpose for which it was collected.
4. Right to oppose: The holder has the right to object to the processing of his personal data.

The law also establishes the obligations of data controllers, which are data controllers, who are the natural or legal persons who collect, store, store, process and persons or legal entities that collect, store, use or transfer personal data, use or transfer personal data.

Those responsible for the processing of personal data must comply with the following requirements:

1. Obligation to obtain the consent of the owner: The data controller must obtain the consent of the data subject must obtain the consent of the data subject before collecting, storing, using or transferring personal data. personal data.
2. Obligation to inform the holder: The controller must inform the holder of the personal data controller must inform the data subject about the the holder about the purpose and use of his personal data. personal data.
3. Obligation to protect personal data: The data controller must data controller must adopt the necessary security measures to protect the necessary

security measures to protect the personal data of the personal data of the owners.

In the article Facial Recognition Technologies in

Colombia [1], presents a summary of facial recognition technologies in Colombia technologies in Colombia, it includes a description of the technologies, a discussion of the description of the technologies, a discussion of the legal and ethical and ethical implications, and a review of relevant literature. Facial recognition technologies are a powerful tool that can be used to powerful tool that can be used for a variety of purposes, including security purposes, including security, identification, and marketing. In Colombia, facial recognition technologies are increasingly used in a variety of applications, including police surveillance, facility access including police surveillance, access to facilities and identity verification. This article of relevant literature, including academic articles, government reports, and policy academic articles, government reports, and policy papers, and also includes discussion with experts in the field of facial recognition technology.

The results show that facial recognition technologies have the potential to improve security and efficiency in a variety of applications. However, there are also risks associated with the use of these technologies, including discrimination, privacy and security. This article discusses the legal and ethical implications of the use of facial recognition technologies in Colombia. but also discusses measures that can be taken to mitigate the risks associated with the use of these technologies, and reaches the following conclusions:

- Facial recognition technologies have the potential to potential to improve security and efficiency in a variety of a variety of applications.
- There are also risks associated with the use of these technologies, including discrimination, privacy and security. privacy and security.
- Measures are needed to mitigate the risks associated with the use of facial recognition technologies. facial recognition technologies.

This article, Facial recognition technology and its risks to human rights [2], presents an overview of facial recognition technology, its risks to human rights, and measures that can be taken to mitigate these risks on human rights and measures that can be taken to mitigate these risks. Facial recognition technology is a powerful tool that can be used for a variety of purposes, including security identification and marketing. However, there are also risks associated with the use of this technology, including discrimination, privacy and security.

This article is based on a review of relevant literature, including academic articles, government reports and policy documents. The results obtained show that facial recognition technology has the potential to improve security and efficiency in a variety of applications. However, there are also risks associated with the use of these technologies, including discrimination, privacy, and security.

This article discusses the legal and ethical implications of using facial recognition technology. Measures that can be taken to mitigate the risks associated with the use of these technologies,

including regulation, technology, transparency and data protection. Among the main conclusions are:

- Facial recognition technology has the potential to improve security and efficiency in a variety of applications.
- However, there are also risks associated with the use of these technologies, including discrimination, privacy discrimination, privacy and security.

Measures are needed to mitigate the risks associated with the use of facial recognition technology.

III. CONCEPTUAL FRAMEWORK

A. Convolutional Neural Networks:

"Neural networks, also known as artificial neural networks (ANNs) or simulated neural networks (ANNs) or simulated neural networks (SNNs), are a subset of machine learning and form the backbone of deep learning algorithms." [5] The structure of these neural networks is inspired by the human brain as they emulate biological neurons interact with each other through the interact with each other through synapses.

Artificial neural networks (ANNs) are composed of layers of nodes, encompassing an input layer, one or more hidden layers, and an output layer.

Every node, also known as an artificial neuron, is linked to others, featuring an assigned weight and threshold. When the output of a particular node surpasses the predetermined threshold, the node activates and transmits data to the subsequent layer of the network; otherwise, no data is forwarded to the next layer.

Artificial neurons are also based on the structure of the biological neuron, which make up neural networks. The synapse that exists between biological neurons is achieved by the so-called synaptic buttons (which are equivalent to the data inputs in artificial neurons) these capture the input signals, then these signals pass through the body of the neuron and through an area called Axon, the electrical signal that travels through the Axon is called action potential and ends up going out through the output buttons.

In an artificial neuron the process is similar, capturing the data through the multiple connections that it may have, these pass to the body where the activation function is produced where the weighted result of the input data plus a bias by a function is passed, and then the result will pass to the next layer. the next layer.

All of this can be seen in Fig. 1

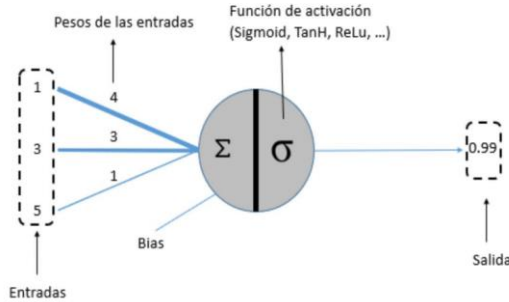


Fig. 1 Structure of an artificial neuron

"Neural networks can be classified into different types, which are used for different types, which are used for different purposes... Convolutional neural networks (CNNs) are similar to forward-propagation forward networks, but they are typically used for image for image recognition, pattern recognition and/or computer vision. pattern recognition and/or computer vision."[5].

Neural networks are based on improving their accuracy over time and training data to learn. As the algorithms of a machine are adjusted, increasingly more precisely with training, they increase their capacity and power, becoming an important tool in computing and artificial intelligence, since it allows classifying and grouping an enormous amount of information and at high speed. Speech recognition or image recognition tasks that expert humans perform manually can take hours, however, it could take just a few minutes for an artificial intelligence to process all the information and analyze it. One of the best-known neural networks is the Google search algorithm.

A convolution neural network stands out among other types of neural networks for its superior performance with image inputs, which is why it is mainly applied in image and motion detection. A convolutional network uses the principles of linear algebra, and specifically matrix multiplication, to identify patterns in an image; In mathematics, convolution is an operator that takes the values of two functions "A" and "B" and transforms them into a third function "C" whose value represents the magnitude by which "A" and an inverted version of "A" overlap. B.". This can be observed in Fig. 2.

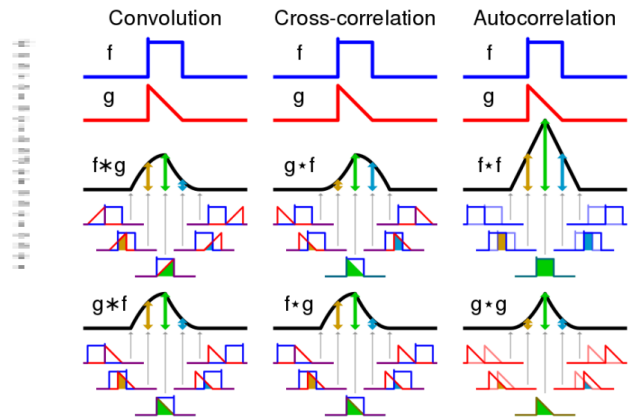


Fig. 2 Convolution of functions.

This type of neural network is composed of three types of layers:

Convolutional layer: It is responsible for obtaining different new images from an initial image by applying filters known as kernels to extract certain important features or patterns. Each kernel runs through the image and will generate a new image that contains what that kernel detected; thus, different images are generated with each kernel applied to the image.

Pooling layer: Downsampling is what is used in this layer, the most used technique being max pooling, this layer is responsible for reducing the resolution of the images generated in the convolution layer, compressing it so that it is easier to detect new patterns in the next convolution layer since convolutional networks generally have several convolution and pooling layers to be able to generate increasingly more complex patterns that together feed a multilayer network that is a machine learning model. A visual example of this can be seen in Fig. 3.

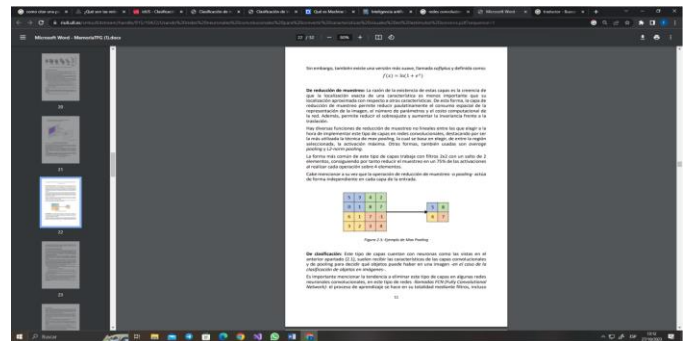


Fig. 3 Max Pooling Grouping.

Fully connected layer: This layer is the one that performs a final classification of the received image that is the result of the previous layers that are partially connected layers, that is, not all the nodes of a layer are connected to all the nodes of the layer. above, however, in this layer, each node

that owns it is directly connected to each node in the previous layer. As seen in Fig.4, there's a visual example of the structure of a convolutional network.

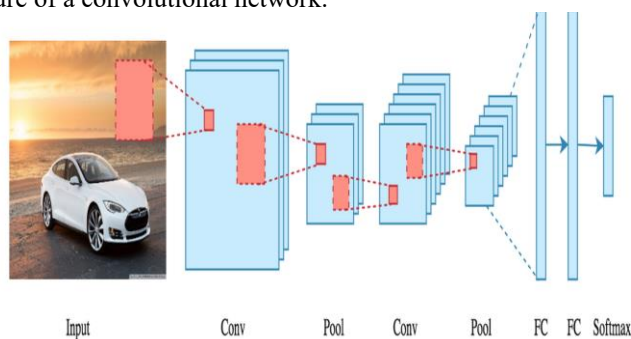


Fig. 4 Structure of a convolutional network

B. Facial Recognition

It is a system that allows the identity of a person to be automatically identified and verified based on the characteristics of their face by capturing, analyzing and comparing facial patterns in an image or video with a database in a matter of seconds, this is born and developed in computer vision research, which is a scientific discipline that aims to ensure that machines have the ability to capture images of the real world, process and analyze them so that they can perceive and understand their environment.

“Facial recognition algorithms make automatic and instantaneous comparisons between a previously archived and digitized image according to algorithmic calculations of distances between certain cardinal points of the face to be identified, and a digitization, according to the same calculations, of a photograph taken on the spot. This automatic verification claims to be more agile and accurate than any document verification and facial feature matching carried out manually.” [7] There are many factors that can negatively affect the technology of facial recognition increasing its margin of error such as the quality of the image, the position of the face, changes in expression, the aging of the person, the presence of certain objects such as glasses, caps or masks and the lighting but it is something in What is always being improved, this technology learns automatically by relying on machine learning algorithms and is automatically improved to achieve better efficiency. Due to this, they are used in sectors that demand a high level of security such as banks or customs, and also in other applications and services such as transportation, parcel deliveries and access to some cell phone apps.

C. Video surveillance

It is a visual surveillance technology through a system of video cameras which are strategically placed to supervise and monitor an area either in real time or by storing the images and videos captured by the cameras in a recording system. “Today, new information and communication technologies are making their way strongly and extending their use to more and

more areas of society. Public security is not unrelated to this expansion, since those are being implemented with the objective of guaranteeing it. Thus, facial recognition has been incorporated into video surveillance systems by law enforcement agencies in some countries. This is a technical method of identifying people through a photograph or image captured by a video camera that has said system incorporated.”[7] This surveillance technique added to facial recognition technology will facilitate the identification of people with requirements who travel in a certain area, in order for it to be carried out there must previously be a database with the person's information and images of their face, these images are compared with the images detected by the surveillance camera and it will be possible to identify the person by recognizing the characteristics and patterns of their face, which vary in each individual, making them identifiable.

“A safeguard or surveillance stops being rewarding when it is perceived that personal information is being misused and becomes an intrusion on privacy; however, in the face of scenarios that put our lives at risk, the need for a safeguard becomes visible and can modify a negative thought of acceptance towards this type of technology. For this study, the situations in which privacy and security are compromised are contextualized to make a decision.” [3]. The authorities will have a very useful tool in their favor to achieve the capture of the wanted subjects, providing better security to the population of San Juan de Lurigancho specifically in the context of the state of emergency dictated for this district, which is the situation that supports the surveillance. in said area.

D. Artificial Intelligence

Artificial intelligence is generally defined as the ability of computers to imitate the human mind by performing activities that require human intelligence. "AI is the ability of machines to use algorithms, learn from data, and use what they learn to make decisions just as a human being would. However, to Unlike people, AI-based devices do not need to rest and can analyze large volumes of information at a time." [4].

Artificial intelligence is already used in multiple areas of science to help human activities and research, generating significant improvements and greater efficiency in the results. With the improvement of this technology, it can be applied in an increasingly wide range of fields, such as computer vision and language processing, in addition to being able to make complex decisions based on the information it receives, “AI-based technologies They are already being used to help humans benefit from significant improvements and enjoy greater efficiency in almost all areas of life. But the great growth of AI also forces us to be attentive to prevent and analyze the possible direct or indirect disadvantages that the proliferation of AI may generate.” [4], the rapid increase in the application of artificial intelligence in activities Humans can be a risk in the future since less and less human participation is needed in activities where machines with artificial

intelligence are used. Thanks to their ability to learn, analyze and make decisions, artificial intelligence is displacing humans from jobs. which is a problem since it would cause the unemployment of many people and this in turn would have a negative impact on the world economy.

"AI is poised to provide us with recommendations and forecasts regarding significant aspects of our lives, influencing domains such as health, well-being, education, employment, and interpersonal connections. Similarly, it will revolutionize business practices by conferring competitive advantages to companies' adept at swiftly and effectively incorporating these tools. Another advantage of AI lies in its capacity to enable machines and robots to undertake tasks deemed difficult, monotonous, or perilous by humans, thereby expanding the scope of what was once considered impossible [4]. While there are potential risks of adverse impacts on people's economic circumstances due to the integration of artificial intelligence, the overall benefits derived from utilizing machines in our activities outweigh these concerns. This utilization not only prevents a halt in activities and research but also accelerates development, yielding quicker and superior results. This, in turn, enhances the quality of life for the general population, who stand to gain from advancements and expedited progress."

E. Machine Learning

"Machine learning consists of a computing discipline in which, and through artificial intelligence algorithms, computer systems are capable of simulating the human learning process, solving situations and challenges for which they had not been previously programmed." [6]

Machines were always limited to doing only what they were programmed to do, however, the development in the power of hardware and software algorithms are achieving more every day, machines now have the ability to learn, and this It is achieved thanks to the analysis of a huge amount of data that the software analyzes allowing it to build models based on which to act, although this at the source code level does not represent a modification of it, we could say in a certain way that it is a modification of its base programming. "Machine learning is one of the main approaches to artificial intelligence. In short, it is an aspect of computing in which computers or machines have the ability to learn without being programmed to do so. A typical outcome would be suggestions or predictions in a particular situation." [4]

Unlike classic computers that were programmed to perform certain specific tasks, the learning capacity of new machines based on machine learning algorithms can offer a personalized experience to each user since they will gain experience and learn from the way they that are used, a clear example of this are search engines like Google for example, which relates the searches you perform with those you previously performed to get an idea of the user's interests;

Another example that we can see is with chat bots such as ChatGPT, which gives better responses to the user if they are provided with a prior context of the topic they wish to discuss, as well as social networks such as Facebook or Tiktok, which show publications or videos with a topic related to the subject. content that your user usually consumes. "The escalating volume and inherent intricacy of biological data have led to an increasing reliance on machine learning in biology for constructing informative and predictive models of the underlying biological processes." [8] Significant strides are being made in the realm of biology, thanks to machines serving as tools that aid researchers in processing and analyzing data and the biological phenomena under investigation. "Over the recent decades, machine learning has witnessed notable advancements in sophisticated learning, algorithms, and efficient preprocessing techniques. Among these developments, the progression of artificial neural networks (ANNs) towards more intricate architectures with enhanced learning capabilities has been encapsulated as deep learning (DL)" [9].

F. Deep Learning

"Deep neural networks typically encompass more than one Hidden Layer, arranged into deeply nested network architectures. Furthermore, they often feature advanced neurons distinct from those in simple ANNs. These advanced neurons can execute sophisticated operations (e.g., convolutions) or employ multiple activations on a neuron, departing from the use of a simple activation function." [9] Although the term Deep learning is usually confused with Machine learning, the difference is that Deep learning is an automatic learning algorithm that uses non-linear functions recursively to be able to learn different levels of complexity of the data that is being analyzed, an example of this is the detection of objects in images, where the edges are initially detected, which are the simplest shapes in the image, in the following layers more complex geometric shapes are detected, and as they are As you advance through the layers, a complete object is detected with better detail. This principle is what is used in convolutional neural networks.

IV. DEVELOPMENT METHODOLOGY

The different methods with which we will work in the development of the facial recognition software will be:

- Data preprocessing: Facial images are preprocessed to eliminate noise, to have a clear and sharp image to improve the quality of the data, i.e.
- of the collected images. The data preprocessing included the following stages:
 1. Scaling: The images were scaled to a size of size of 224 x 224 pixels.
 2. Normalization: The images were normalized to have a range of values between 0 and 1.
- Software training: A convolutional neural network (CNN) model was used for the software to learn to

recognize the different faces shown to it. The model was trained over many trials with different faces, using a training dataset of 100 images

- Software evaluation: The software was evaluated using a test data set of 100 images. The accuracy of the software was calculated as the percentage of correctly classified images correctly identified.

Materials

- Data: A database containing the images with which the software will be trained will be used. The facial images will be gathered from the different security cameras in the San Juan de Lurigancho district.

Hardware: To develop the software, a computer with an Intel Core i7-12700 K processor and an NVIDIA GeForce RTX 3080 graphics card will be used and the Python programming language will be used in the Visual Studio environment.

To meet the objective of this project, the openCV library will be used as a tool for image processing.

“OpenCV is the image and video analysis and processing library par excellence, and its range of implemented algorithms and functions is enormously wide. Among this range we find functions as varied as image binarization, generation of SURF and HOG descriptors, background subtractors, etc.” [11]

Although from the beginning this library has been focused on being used with C++, which is the language in which it was written, due to Python having a great boom in the field of artificial intelligence, the OpenCV interface for Python was sought, which will be used to develop this project.

It will have 2 main phases, which are the image capture phases, where the program will capture images, it visualizes of a face to store them in a folder that will serve as our database for the next phase, which is recognition. In this phase, the program will analyze the patterns of the face it visualizes and will look for matches with the information in the database in order to identify the person. For this, we must first save the name of the person to whom the images in the database correspond. There will be lists of images corresponding to each person.

Image Capture: Below, the Python codes used for the capture phase will be presented, which are detailed step by step with comments from Fig. 5 and Fig.6:

```
#OpenCV module
import cv2
#Módulo para leer directorios y rutas de archivos
import os
#OpenCV trabaja con arreglos de numpy
import numpy
#Obtener el nombre de la persona que estamos capturando
import sys
nombre = sys.argv[1]

#Directorio donde se encuentra la carpeta con el nombre de la persona
dir_faces = 'C:\\Users\\Melany\\Downloads\\melanie\\FaceRecognition2-
master\\att_faces\\ori_faces'
path = os.path.join(dir_faces, nombre)

#Tamaño para reducir a miniaturas las fotografías
size = 4

#Si no hay una carpeta con el nombre ingresado entonces se crea
if not os.path.isdir(path):
    os.mkdir(path)

#cargamos la plantilla e inicializamos la webcam
face_cascade =
cv2.CascadeClassifier('haar_cascade_frontal_face_default.xml')
cap = cv2.VideoCapture(0)

img_width, img_height = 112, 92

#Ciclo para tomar fotografías
count = 0
while count < 100:
```

Fig. 5. Code of the image capture processing

```

#Codigo para tomar fotografias
count = 0
while count < 100:
    #leemos un frame y lo guardamos
    rval, img = cap.read()
    img = cv2.flip(img, 1, 0)

    #convertimos la imagen a blanco y negro
    gray = cv2.cvtColor(img, cv2.COLOR_BGR2GRAY)

    #redimensionar la imagen
    mni = cv2.resize(gray, (int(gray.shape[1] / size), int(gray.shape[0] / size)))

    """buscamos las coordenadas de los rostros (si los hay) y guardamos su posición"""
    faces = face_cascade.detectMultiScale(mni)
    faces = sorted(faces, key=lambda x: x[3])

    if faces:
        face_i = faces[0]
        (x, y, w, h) = [v * size for v in face_i]
        face = gray[y:y+h, x:x+w]
        face_resize = cv2.resize(face, (img_w_dth, img_height))

        #Dibujamos un rectangulo en las coordenadas del rostro
        cv2.rectangle(img, (x, y), (x+w, y+h), (0, 255, 0), 3)
        #Ponemos el nombre en el rectangulo
        cv2.putText(img, nombre, (x-10, y-10),
cv2.FONT_HERSHEY_PLAIN, 1, (0, 255, 0))

        #El nombre de cada foto es el numero del ciclo
        #Obtenemos el nombre de la foto
        #Despues de la ultima sumamos 1 para continuar con los demas
nombres
        pin=sorted([int(n:n.find('.'))] for n in os.listdir(path)
            if n[0]!='.' ]+[0])[-1] + 1

        #Metemos la foto en el directorio
        cv2.imwrite('%s/%s.png' % (path, pin), face_resize)

        #Contador del ciclo
        count += 1

    #Mostramos la imagen
    cv2.imshow('OpenCV Entrenamiento de '+nombre, img)

    #Si se presiona la tecla ESC se cierra el programa
    key = cv2.waitKey(10)

```

Fig.6. Second part of the code

```

#Directorio donde se encuentran las carpetas con las caras de
entrenamiento
dir_faces = 'att_faces/orl_faces'

#Tamaño para reducir a miniaturas las fotografias
size = 4

# Crear una lista de imágenes y una lista de nombres correspondientes
(images, labels, names, id) = ([], [], (), 0)
for (subdirs, dirs, files) in os.walk(dir_faces):
    for subdir in dirs:
        names[id] = subdir
        subjectpath = os.path.join(dir_faces, subdir)
        for filename in os.listdir(subjectpath):
            path = subjectpath + '/' + filename
            label = id
            images.append(cv2.imread(path, 0))
            labels.append(int(label))
            id += 1
(img_w_dth, img_height) = (112, 92)

# Crear una matriz Numpy de las dos listas anteriores
(images, labels) = [numpy.array(lis) for lis in [images, labels]]
# OpenCV entrena un modelo a partir de las imágenes
model = cv2.face.LBPHFaceRecognizer_create()
model.train(images, labels)

# Parte 2: Utilizar el modelo entrenado en funcionamiento con la cámara
face_cascade = cv2.CascadeClassifier(
'haar_cascade_frontal_face_default.xml')
cap = cv2.VideoCapture(0)

while True:
    #leemos un frame y lo guardamos
    rval, frame = cap.read()
    frame=cv2.flip(frame, 1, 0)

    #convertimos la imagen a blanco y negro
    gray = cv2.cvtColor(frame, cv2.COLOR_BGR2GRAY)

    #redimensionar la imagen
    mni = cv2.resize(gray, (int(gray.shape[1] / size), int(gray.shape[0] / size)))

    """buscamos las coordenadas de los rostros (si los hay) y guardamos su posición"""
    faces = face_cascade.detectMultiScale(mni)

```

Fig. 8. Second part of the face recognition code

Face recognition: Below are screenshots of the Python code used in the recognition phase, which are detailed step by step with comments in Fig. 7, Fig. 8, Fig.9 and Fig.10.

```

#OpenCV module
import cv2
#Modulo para leer directorios y rutas de archivos
import os
#OpenCV trabaja con arreglos de numpy
import numpy
#Se importa la lista de personas con acceso al laboratorio
from listaPermitidos import flabianos
flabs=flabianos()

# Parte 1: Creando el entrenamiento del modelo
print('Formando...')

```

Fig. 7 First part of the face recognition code

```

for i in range(len(faces)):
    face_i = faces[i]
    (x, y, w, h) = [v * size for v in face_i]
    face = gray[y:y+h, x:x+w]
    face_resize = cv2.resize(face, (img_w_dth, img_height))

    # Intentado reconocer la cara
    prediction = model.predict(face_resize)

#Dibujamos un rectangulo en las coordenadas del rostro
cv2.rectangle(frame, (x, y), (x+w, y+h), (0, 255, 0), 3)

# Escribiendo el nombre de la cara reconocida
# La variable cara tendra el nombre de la persona reconocida
cara = '%s' % (names[prediction[0]])

```

Fig. 9. Third part of the face recognition

```

#Si la predicción tiene una exactitud menor a 100 se toma como predicción
#válida
if predicción[1] < 100 :
    #Poneremos el nombre de la persona que se reconoció
    cv2.putText(frame, '%s - %0f' % (cara, predicción[1]), (x-10, y-
10), cv2.FONT_HERSHEY_PLAIN, 1, (0, 255, 0))

    #En caso de que la cara sea de algún conocido se realizara
    #determinadas acciones
    #Busca si los nombres de las personas reconocidas están dentro
    #de los que tienen acceso
    #fabs. TuSi TuNo(cara)

    #Si la predicción es mayor a 100 no es un reconocimiento con la
    #exactitud suficiente
    elif predicción[1] > 101 and predicción[1] < 500:
        #Si la cara es desconocida, poner desconocido
        cv2.putText(frame, 'Desconocido', (x-10, y-10),
cv2.FONT_HERSHEY_PLAIN, 1, (0, 255, 0))

        #Mostramos la imagen
        cv2.imshow('OpenCV Reconocimiento facial', frame)

        #Si se presiona la tecla ESC se cierra el programa
        key = cv2.waitKey(10)
        if key == 27:
            cv2.destroyAllWindows()
            break

```

Fig. 10 Fourth part of the facial recognition code

The facial recognition program saves the images obtained and creates a list of images that serves as a database so that it can identify the same person later. The files and database can be seen in Fig.11.

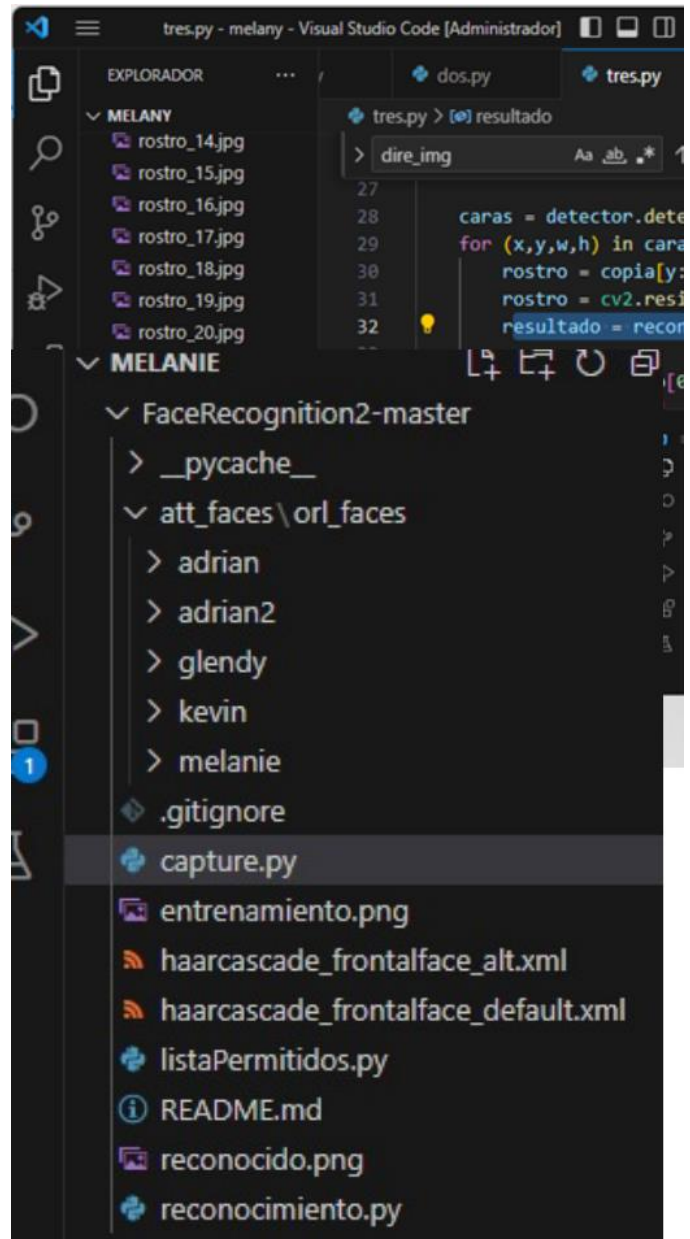


Fig. 11. File structure of the facial recognition system

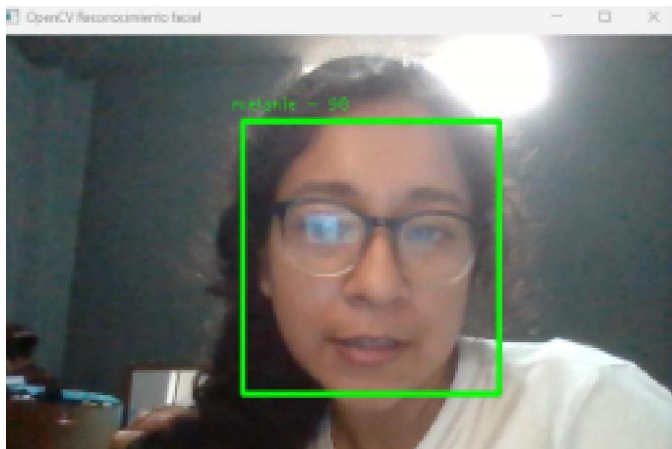


Fig. 12. Facial recognition real time visualizer

If there is no record of the person who can view, the face being viewed is identified as “unknown” just as we can see in Fig. 13 and Fig.14

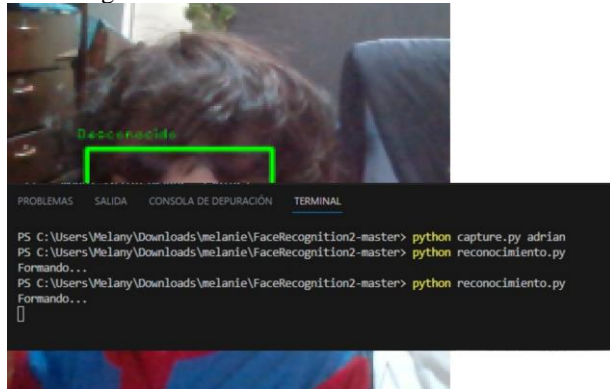


Fig. 13. Terminal output and facial recognition

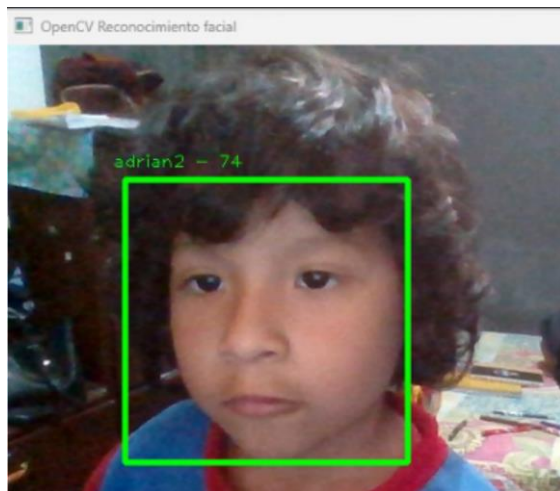


Fig. 14. Second face recognition image

ACKNOWLEDGMENT

We thank the whole team for their mutual effort.

REFERENCES

- [1] Arjona, J., Pérez, M., & García, J. (2022). Aplicación de redes neuronales artificiales para la clasificación de imágenes médicas. *Revista de Ingeniería y Ciencia*, 18(2), 137-152. doi: 10.22201/fca.24488923e.2022.2.1138
- [2] ARTOLA MORENO, Álvaro. Clasificación de imágenes usando redes neuronales convolucionales en Python. 2019.
- [3] Bautista, A., & Fernández, J. (2023). Redes neuronales artificiales para la predicción de la calidad de la fruta. *Revista Iberoamericana de Inteligencia Artificial*, 2(2), 23-36. doi: 10.1109/IAIA.2023.00023
- [4] BRAVO, Cristián J.; RAMIREZ, Patricio E. y ARENAS, Jorge. Acceptance of Face Recognition as a Surveillance and Safety Measure: An Empirical Study in Chile. *Inf. tecnol.* [online]. 2018, vol.29, n.2 [citado 2023-10-22], pp.115-122. ISSN 0718-0764. doi: 10.4067/S0718-07642018000200115. http://www.scielo.cl/scielo.php?script=sci_arttext&pid=0718-07642018000200115&lng=es&nrm=iso.
- [5] Caballero, M., & Rodríguez, J. (2022). Redes neuronales artificiales para la detección de fraudes en tarjetas de crédito. *Revista de Sistemas Computacionales*, 22(1), 57-72. doi: 10.22201/fca.24488923e.2022.1.1137
- [6] Córdoba, M., & Pérez, J. (2021). Redes neuronales artificiales para la generación de texto creativo. *Revista de Ciencias de la Información*, 26(2), 125-142. doi: 10.22201/fca.24488923e.2021.2.1136
- [7] Deng, W., Hu, J., & Guo, J. (2021). "ArcFace: Additive Angular Margin Loss for Deep Face Recognition." *IEEE Conference on Computer Vision and Pattern Recognition (CVPR)*.
- [8] Domingo Jaramillo, C. (2021). Utilización del sistema de reconocimiento facial para preservar la seguridad ciudadana, *El Criminalista Digital*, 9, 20-37. <http://revistaseug.ugr.es/index.php/cridi/article/view/20899>
- [9] GREENER, Joe G., et al. A guide to machine learning for biologists. *Nature Reviews Molecular Cell Biology*, 2022, vol. 23, no 1, p. 40-55.
- [10] JANIESCH, Christian; ZSCHECH, Patrick; HEINRICH, Kai. Machine learning and deep learning. *Electronic Markets*, 2021, vol. 31, no 3, p. 685-695.
- [11] Jin, Y., Zhang, C., & Liu, C. (2021). "Face Recognition Using Cross-Pose Deep Learning." *Sensors*, 21(4), 1412.
- [12] Liu, W., Wen, Y., Yu, Z., Li, M., Raj, B., & Song, L. (2020). "SphereFace: Deep Hypersphere Embedding for Face Recognition." *IEEE Transactions on Pattern Analysis and Machine Intelligence*, 43(4), 1075-1088.
- [13] Martínez-Molina, A. F., Martínez-Arango, E. M., & Sánchez-Agudelo, J. S. (2023). Facial recognition technologies in Colombia: Comparative analysis in relation to data protection. *Ius et Praxis*, 29(1), 3-26. doi:10.4067/S0718-00122023000100003. <https://www.scielo.cl/pdf/iusetp/v29n1/0718-0012-ius-29-01-3.pdf>
- [14] ROUHIAINEN, Lasse. *Inteligencia artificial*. Madrid: Alienta Editorial, 2018.
- [15] Sanabria Moyano, J. E., Roa Avella, M. d. P., & Lee Pérez, O. I. (2022). Tecnología de reconocimiento facial y sus riesgos en los derechos humanos. *Revista Criminalidad*, 64(3), 61-78. doi:10.47741/17943108.366. <https://revistacriminalidad.policia.gov.co:8000/index.php/revcriminalidad/article/view/366/614>