PROTOTIPO DE AUTENTICACIÓN DE DOBLE FACTOR BASADO EN RECONOCIMIENTO FACIAL PARA EMAIL

FACE RECOGNITION-BASED TWO-FACTOR AUTHENTICATION PROTOTYPE FOR EMAIL

Cristal Karina Galindo Durán
Escuela Militar de Ingeniería, México
cdgalindod@gmail.com

Roberto Alfonso Ortíz Rivera
Escuela Militar de Ingeniería, México
ortizriveraalfonso@gmail.com

Juan Villegas Cortez
Universidad Autónoma Metropolitana, Unidad Azcapotzalco, México
juanvc@azc.uam.mx

Recepción: 7/marzo/2025 **Aceptación:** 24/abril/2025

Resumen

Con la evolución de la tecnología y el constante incremento de los ciberataques es importante para las instituciones incorporar sistemas de autenticación reforzados que permitan salvaguardar su información. Este trabajo presenta el diseño y desarrollo de un prototipo de autenticación de doble factor que considera el reconocimiento facial como la segunda etapa de validación como refuerzo. Dicho prototipo está enfocado en subsanar el sistema de autenticación tradicional, usuario y contraseña, del eMail institucional tradicional.

El prototipo fue desarrollado utilizando tecnologías Java y Python, siguiendo una arquitectura cliente-servidor, implementando la librería DeepFace. Los resultados obtenidos se analizaron desde dos vertientes, con pruebas realizadas al prototipo y la validación del algoritmo de reconocimiento facial. El prototipo desarrollado que aquí se presenta, mejora y refuerza la seguridad contra ciberataques de suplantación de identidad.

Palabras Clave: Biometría, Inteligencia Artificial, Reconocimiento facial, Seguridad.

Abstract

With the evolution of technology and the constant increase of cyber-attacks, it is important for institutions to incorporate reinforced authentication systems to safeguard their information. This paper presents the design and development of a two-factor authentication prototype that considers facial recognition as the second stage of validation as reinforcement.

This prototype is focused on replacing the traditional authentication system, username and password, of the traditional institutional eMail. The prototype was developed using Java and Python technologies, following a client-server architecture, implementing the DeepFace library. The results obtained were analyzed from two perspectives, with tests carried out on the prototype and the validation of the facial recognition algorithm. The developed prototype presented here improves and reinforces security against identity theft cyber-attacks.

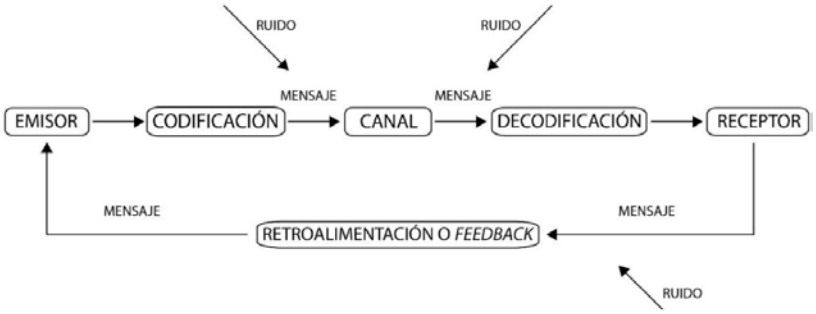
Keywords**:** *Artificial Intelligence, Biometrics, Facial recognition, Security.*

1. Introducción

En los últimos años los sistemas de identificación biométrica han adquirido una importancia creciente en sectores como el comercio, el gobierno y la seguridad debido a su capacidad para utilizar características físicas o conductuales únicas de las personas, tales como: huellas dactilares, geometría de la mano, rostro, iris del ojo, retina y voz. Entre estos sistemas, el reconocimiento facial ha ganado considerable interés en el ámbito de la biometría a nivel global, ya que ofrece una forma discreta y no invasiva de detectar, identificar y verificar la identidad de una persona [Alwahaishi, 2020]. Por otra parte, el correo electrónico (e-Mail) sigue siendo uno de los servicios más utilizados dentro de las organizaciones de todo tipo. Debido a que en el ámbito jurídico, los correos electrónicos tienen validez legal y pueden usarse como pruebas en casos judiciales, certificando y validando el proceso de la comunicación [Feliu, 2024], con las partes del procedimiento general de la comunicación acorde al modelo de comunicación de Shannon, Figura 1.

Por lo anterior, las diversas organizaciones gubernamentales, a través de sus dependencias y unidades utilizan el e-Mail. El cual se encarga del envío y recepción

de mensajes que contienen disposiciones, directivas y órdenes, las cuales son cruciales para cada organización.



Fuente: elaboración propia

Figura 1 Procedimiento general de la comunicación.

En el contexto de la certificación y autenticidad de los eMails: empresas operadoras certifican el contenido, momento exacto de envío y cuentas del emisor y receptor; utilizando códigos alfanuméricos para garantizar la veracidad de la información certificada. El término “autenticación” se refiere a un proceso electrónico que permite identificar electrónicamente a una persona natural o jurídica [Buchanan, 2017].

Por otra parte, la Inteligencia Artificial (IA) permite una mayor precisión y rapidez en el reconocimiento de patrones; entendiendo un patrón como una estructura o secuencia de datos que se repite de manera consistente, éstos pueden ser simples o complejos, y pueden encontrarse en una variedad de contextos y para nuestro caso de estudio, nos interesa tarbajar con los patrones asociados características del rostro humano. Por su parte, DeepFace [Viola, 2001] es un sistema de reconocimiento facial que hace uso de las técnicas de IA y Deep Learning creado por Facebook en el año 2014, permitiendo identificar de una forma confiable la identidad de una persona, proporcionando mayor seguridad de acceso al correo electrónico institucional, dando una mayor eficiencia y confiabilidad en los trámites y órdenes que se envíen por medio de este servicio.

De forma precisa, el prototipo de doble factor, permite la implementación, en materia de seguridad, utilizando diversas técnicas de autenticación para satisfacer las necesidades que se requieran en áreas específicas. Inclusive, el tener un proyecto

de este tipo, podría permitir complementar sistemas de seguridad mediante el reconocimiento facial para aumentar la seguridad y fiabilidad; por ejemplo, en accesos controlados o restringidos. Esto permite adaptarse a diversas necesidades y usos. Por su parte, en los trabajos relacionados encontramos la investigación titulada ‘’Redes neuronales artificiales de aprendizaje profundo para el reconocimiento facial y control de acceso de estudiantes a un laboratorio’’ [Cayllahua, 2019], se tuvo como objetivo la implementación de una red neuronal convolucional (Convolutional Neural Network, CNN) de Aprendizaje Profundo (Deep Learning, DL), para el reconocimiento facial y el control de acceso de estudiantes de la carrera de Ingeniería Mecatrónica.

En el trabajo presentado por [Félix, 2020] se propone la implementación de un sistema prototipo para el registro de asistencia de estudiantes de la Escuela Politécnica Nacional, la aplicación se desarrolló en Python y sigue una arquitectura móvil para dispositivos Android.

[Muñoz, 2021] implementó el sistema control de acceso de personal por medio de reconocimiento facial, en el cual se consideró algoritmos de DL aplicado en tiempo real, a través de la visión por computadora. Para detectar y alinear el rostro se utilizaron algoritmos de DL; así como una red neuronal convolucional en cascada multitarea (MTCNN), y el modelo pre-entrenado Facenet.

El autor J. A. Zarate[Zarate, 2023] desarrolló un prototipo de reconocimiento facial como segundo factor de autenticación, en donde algún empleado podía inicializar sesión a través de reconocimiento facial; sin embargo si un usuario sin autorización intentaba acceder al sistema, este guardará su imagen con fecha y hora en la que el usuario no autorizado intento acceder.

En el trabajo titulado “Implementación de un sistema de autenticación mediante validación biométrica para procesos bancarios” [La Madrid, 2023], se presenta un sistema de autenticación mediante validación biométrica, para procesos bancarios haciendo uso de una entrada de una imagen que el usuario brinda, para el reconocimiento facial se implemento mediante la técnica de Haar cascade que utiliza el lenguaje de programación Python y la librería de procesamiento de imágenes OpenCv2.

El resto de este artículo está organizado como sigue: en la sección 2 se describen el tipo de investigación y metodología utilizada; así como el desarrollo. En la sección 3 se explica de forma general los resultados obtenidos del caso de estudio. En la sección 4, se muestra la discusión. Finalmente, en la sección 5 se presentan las conclusiones y los posibles trabajos que pudieran dar continuidad a la investigación.

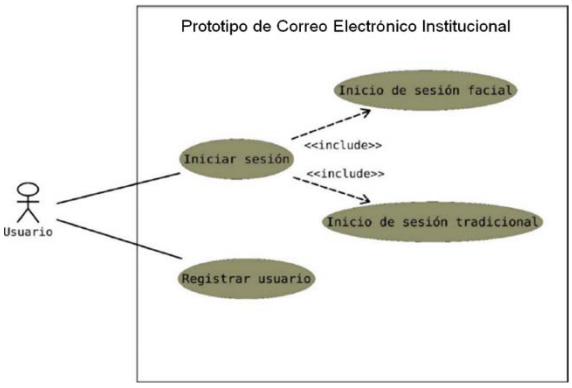
2. Métodos

El presente trabajo es una investigación de tipo aplicada. En donde para el desarrollo del prototipo se consideró el ciclo de desarrollo de software [Pressman, 2020], el cual consiste en 5 etapas, siendo estas:

- Análisis de requerimientos,
- Diseño del prototipo,
- Implementación,
- Pruebas y
- Mantenimiento.

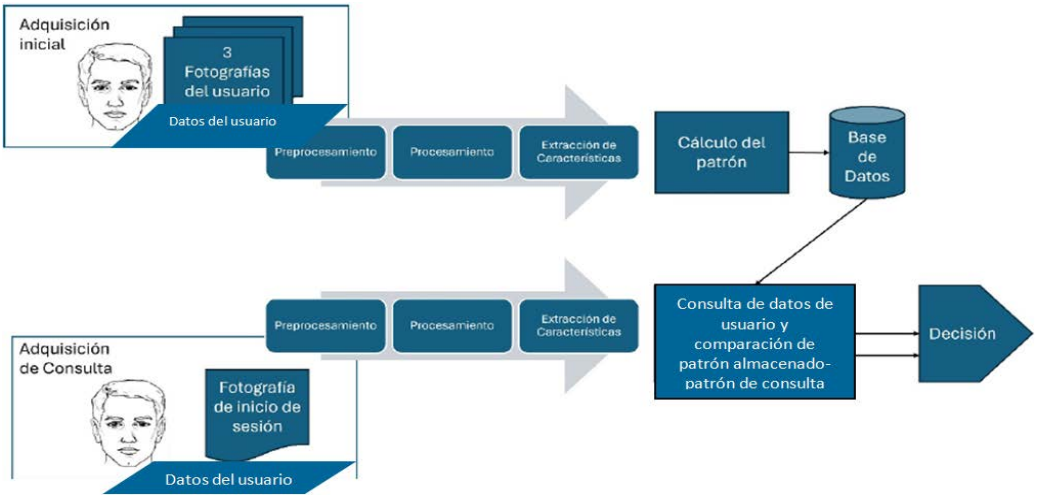
Las fases del desarrollo del prototipo y de forma generalizada sus actividades, son:

- **Análisis de requerimientos**. Se identificaron y documentaron los requisitos funcionales y no funcionales del prototipo, a través de entrevistas con el área encargada de administrar el correo electrónico institucional, y la revisión de documentos relevantes como las directivas vigentes para el desarrollo de sistemas. En la Figura 2 se presenta el diagrama de casos de uso, que permite visualizar los requerimientos funcionales del prototipo.
- **Diseño del prototipo**. Esta fase implicó el diseño de la arquitectura del prototipo y la especificación detallada de sus componentes. Se desarrollaron diversos diagramas como: diagrama de bloques del prototipo, diseño de pantallas conforme a los flujos ideales de cada uno de los casos de uso, modelo relacional de la base de datos, diagrama de arquitectura y diagrama de tecnologías propuestas para implementar el prototipo. En la Figura 3 se muestra el diagrama de bloques del prototipo, y en la Figura 4 se presenta el diseño de pantalla para acceder al prototipo.



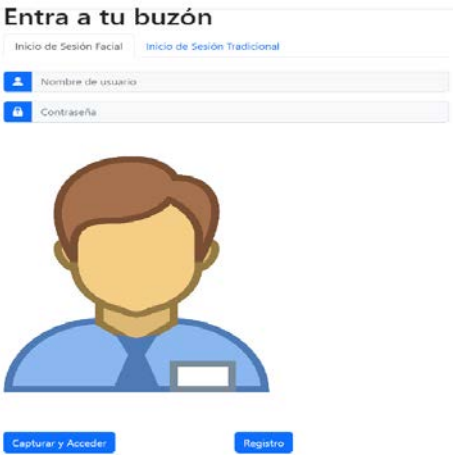
Fuente: elaboración propia

Figura 2 Diagrama de casos de uso del prototipo propuesto.



Fuente: elaboración propia

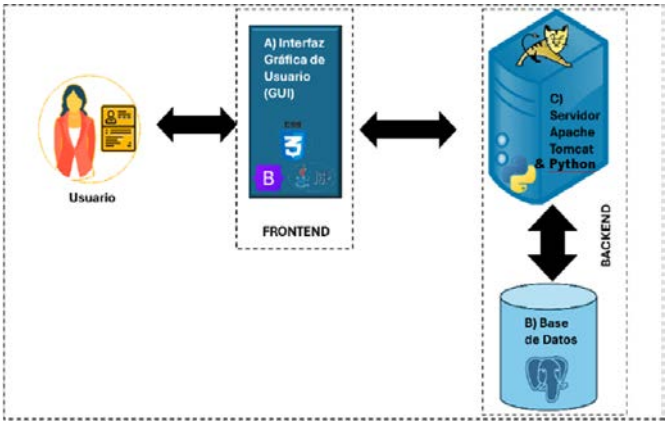
Figura 3 Diagrama de bloques del prototipo.



Fuente: elaboración propia

Figura 4 Propuesta de pantalla de inicio de sesión del prototipo.

- **Implementación**. En esta fase se desarrolló el prototipo basado en el diseño de la etapa anterior. El prototipo fue desarrollado bajo una arquitectura Cliente-Servidor, en donde la interfaz de usuario fue realizada con Java Server Page (JSP), Bootstrap y JavaScript; como servidor de aplicaciones Apache Tomcat y Python con el uso de bibliotecas de DeepFace para el reconocimiento facial; como servidor de bases de datos Postgresql. En la Figura 5 se muestra la arquitectura para el prototipo; así como, las tecnologías utilizadas en el *frontend* y *backend*.



Fuente: elaboración propia

Figura 5 Diagrama de tecnologías propuestas para el prototipo.

Además, esta fase consideró el proceso de reconocimiento facial propuesto por el autor Chun-Rong [Chun-Rong, 2020], el cual consiste en:

- Detección facial,
- Alineación facial,
- Extracción de características y
- Comparación.

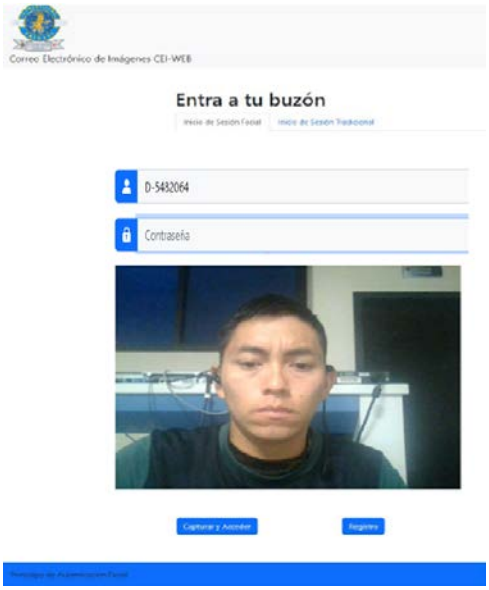
Por lo que se procedió a realizar una base de imágenes de 150 usuarios-personas con 3 muestras-fotografías cada uno, contando con un total de 450 imágenes digitales. Las imágenes fueron capturadas con una cámara web Microsoft® modelo LifeCam HD-3000, con resolución $720p$ HD en video y $1280x720\ píxeles$ en imagen, sensor de imagen CMOS, campo de visión de $68.5\ grados$, y capacidad de $30\ fps$.

Las imágenes obtenidas tienen las siguientes características: dimensiones $640\ x\ 480\ píxeles$, resolución de $96\ píxeles\ por\ pulgada$ y un tamaño en disco de $72\ KB$. Lo anterior para su procesamiento y validación del algoritmo de reconocimiento de patrones en rostros basado en el modelo DeepID. Dicho modelo es uno de los 12 modelos de DeepFace [Viola, 2001], desarrollado por el equipo de investigación de la Universidad de Ciencia y Tecnología de China; el cual utiliza múltiples capas convolucionales para mejorar la precisión del reconocimiento facial y es reportado como uno de los modelos más precisos con el 99.47% de precisión y una eficiencia de $0.15\ s$ por imagen [Taigman, 2014].

3. Resultados

Los resultados de esta investigación se muestran en dos vertientes:

- **Pruebas al prototipo**. Se realizaron pruebas unitarias a cada pantalla y componente del prototipo, probándolas de forma individual y mostrando el funcionamiento en cada funcionalidad del prototipo; así como, su integración de forma completa y sin errores de funcionamiento. En la Figura 6 se muestra la pantalla de inicio de sesión del prototipo de autenticación con el reconocimiento facial integrado.



Fuente: elaboración propia

Figura 6 Pruebas unitarias de inicio de sesión.

También se realizaron pruebas de integración donde se exploró el funcionamiento de forma integral en el componente y finalmente se realizaron pruebas de configuración en los principales navegadores web en los sistems operativos más comunes de las computadoras personales y dispositivos móviles: Microsoft Edge, Mozilla Firefox, Opera y Google Chrome. De las pruebas de configuración realizadas se encontraron ligeros problemas de renderizado en la interfaz, pero sin impacto significativo en la funcionalidad del prototipo. En general, las pruebas demostraron una funcionalidad correcta.

- **Pruebas de validación al algoritmo de reconocimiento facial**. Estas pruebas se realizaron para evaluar su precisión, exactitud, sensibilidad y robustez en condiciones reales, considerando un umbral de coincidencia del 80%. A continuación, se describen los criterios de evaluación y los resultados obtenidos. Para llevar a cabo las pruebas de validación, se utilizó el conjunto de 450 imágenes de 150 personas distintas, posteriormente se dividió en dos bases: entrenamiento y pruebas. Para la validación del algoritmo se utilizó el método de validación cross validation (validación cruzada), el cual consiste en dividir el total de las muestras en 50% base de entrenamiento y 50% base de prueba. Para llevar a cabo dicha validación se realizó lo siguiente:
  - ✓ **Selección de Imágenes**. Como se mencionó en la sección 2, se tomaron las imágenes de 150 usuarios con 3 tomas, dando un total de 450 imágenes. A partir de estas imágenes se generaron 225 números aleatorios sin repetición para repartir de forma equitativa las imágenes en la base de entrenamiento y base de prueba.
  - ✓ **Autenticación**. Se procedió a comparar las imágenes de la base de prueba con las imágenes de entrenamiento, y construir la matriz que permitiera contabilizar los diferentes datos: verdaderos negativos, falsos positivos, falsos negativos y verdaderos positivos, permitiendo obtener la matriz de confusión, Tabla 1.

    La matriz de confusión se interpreta de la siguiente manera: Verdaderos Negativos ($TN = 53$), Falsos Positivos ($FP = 49$), Falsos

Negativos ($FN = 7$), y Verdaderos Positivos ($TP = 117$). A partir de la matriz de confusión [Skiena, 2017]:

- **Sensibilidad (*Recall*)**. La capacidad del modelo para identificar correctamente los casos positivos (Ecuación 1), obteniendo $Sensibilidad = 0.9435$.

$$Sensibilidad = \frac{TP}{TP + TF} \quad (1)$$

- **Especificidad**. La capacidad del modelo para identificar correctamente los casos negativos (Ecuación 2), obteniendo la $Especificidad = 0.5196$.

$$Especificidad = \frac{TN}{TN + FP} \quad (2)$$

- **Exactitud**. La proporción de predicciones correctas entre el total de casos evaluados (Ecuación 3) obteniendo una $Exactitud = 0.7522$.

$$Exactitud = \frac{TP + TN}{TP + TN + FP + FN} \quad (3)$$

- **Precisión**. La proporción de verdaderos positivos entre los casos predichos como positivos por el modelo, la cual se obtiene en la Ecuación 4, donde $Precisión = 0.7048$.

$$Precisión = \frac{TP}{TP + FP} \quad (4)$$

Tabla 1 Matriz de confusión modelo utilizado para la autenticación facial.

	Estimado por el modelo	
Real	**Negativo**	**Positivo**
Negativo	53	49
Positivo	7	117

Fuente: elaboración propia

Los resultados obtenidos indican que el modelo tiene una buena capacidad para identificar correctamente los casos positivos (alta sensibilidad) y una exactitud general del 75.22%. Sin embargo, la especificidad es relativamente baja, lo que sugiere

que el modelo tiene dificultades para identificar correctamente los casos negativos.

4. Discusión

Como se mencionó en la Sección 1, existen diversos trabajos que incorporan como factor adicional de autenticación el reconocimiento facial, a través de diversos algoritmos de la Inteligencia Artificial y Redes Neuronales, tal como [Cayllahua, 2019], [Muñoz, 2021], [Zarate, 2023], [La Madrid, 2023]; no obstante, el trabajo desarrollado implementa de forma particular, el inicio de sesión para el correo electrónico institucional y es desarrollado con tecnologías de lenguaje de programación Java, debido a normas de sistematización dictadas por la institución e integra en la parte de reconocimiento facial en Lenguaje de Python, de forma concreta usando Deep Face haciendo uso del modelo DeepID. También la investigación puede compararse con el trabajo de Cayllahua [Cayllahua, 2019], en cuanto a la cantidad similar de muestras utilizadas para validar el reconocimiento facial. Por otra parte, en el trabajo presentado por [Zarate, 2023] difiere de la propuesta presentada, pues en el trabajo desarrollado no se guarda las imágenes de las personas que desean ingresar al sistema; pero no se encuentran registradas.

5. Conclusiones

El presente trabajo describe de forma general el diseño y desarrollo de un prototipo que implementa un doble factor de autenticación considerando al correo electrónico institucional por un lado el primer factor consiste en las credenciales del usuario (usuario y contraseña) y como segundo factor el reconocimiento facial.

Los resultados obtenidos durante la validación del prototipo sugieren que la incorporación del reconocimiento facial como un factor adicional de autenticación mejora y aumenta la seguridad contra ciberataques de suplantación de identidad.

Por otra parte, es importante destacar que la precisión y exactitud del algoritmo de reconocimiento facial dependen en gran medida de la calidad y las características de las imágenes tomadas.

Para garantizar un rendimiento óptimo del prototipo, es fundamental establecer condiciones adecuadas para la captura de fotografías. Esto incluye asegurar una iluminación adecuada, minimizar el fondo y evitar obstrucciones faciales como gafas oscuras o sombreros; así como, definir la distancia requerida para cada foto. Al establecer todas estas condiciones, se puede aumentar la precisión y exactitud del algoritmo, mejorando la fiabilidad y efectividad del sistema de reconocimiento facial. A lo largo del desarrollo de este trabajo se han identificado un conjunto de trabajos futuros, con los cuales se podría dar continuidad a esta investigación, dichas propuestas son las siguientes:

- Incluir técnicas avanzadas como la verificación de liveness para distinguir entre un rostro humano real y una fotografía o video; además de incluir algoritmos que corrijan la rotación del rostro.
- Establecer una distancia óptima para la toma de fotografías, ya que las fotografías tomadas fueron recabadas a diferentes distancias, influenciando la precisión y exactitud del algoritmo.
- Paralelizar el algoritmo de DeepFace que permite la verificación de rostros, para reducir el tiempo de procesamiento cuando son cantidades considerables de imágenes.
- Incorporar la autenticación de doble factor a través de reconocimiento facial a otros sistemas y/o plataformas que maneje la institución para fortalecer su seguridad y minimizar riesgos.

6. Bibliografía y Referencias

[1] Alwahaishi, S., Zdrálek, J. Biometric Authentication Security: An Overview. 2020 IEEE International Conference on Cloud Computing in Emerging Markets (CCEM), Bengaluru, India, 87-91, November, 2020.

[2] Buchanan, W. J. 6 Authentication and Digital Certificates. Cryptography. River Publishers, Gistrup, Denmark, 183-216. 2017.

[3] Cayllahua, N. Y., Suárez, M. J. C. Redes neuronales de aprendizaje profundo para el reconocimiento facial y control de acceso de estudiantes a un laboratorio. Universidad Ricardo Palma, Lima, Perú. 2019.

[4] Chun-Rong, Z. Research on Face Recognition Technology Based on Deep Learning. In 2020 IEEE International Conference on Industrial Application of Artificial Intelligence (IAAI). 457-462, Harbin, China. 2020.

[5] Feliu, J, B. Los correos electrónicos y su valor probatorio ratificado por el Tribunal Supremo (Sentencia Sala 4ª de 23-07-20), España. 2024.

[6] Félix, M., L. L., Desarrollo de un sistema prototipo para el registro de asistencia de estudiantes de la Escuela Politécnica Nacional, basado en reconocimiento facial. [Trabajo de suficiencia profesional, Escuela Politécnica Nacional], Ecuador. 2020.

[7] La Madrid, C, G., Ruiz T, R. Implementación de un sistema de autenticación mediante validación biométrica para procesos bancarios. [Trabajo de suficiencia profesional, Universidad Peruana de Ciencias Aplicadas], Perú. 2023.

[8] Muñoz, E. Desarrollo de un sistema de control de acceso de personal empleando reconocimiento facial respaldado con técnicas de aprendizaje profundo. Universidad de las Fuerzas Armadas. Innovación para la Excelencia. Sangolquí, Ecuador. 2021.

[9] Pressman, Roger S., y Bruce R. Maxim. Software engineering: a practitioner's approach. Nineth edition. McGraw-Hill Education, New York, U.S.A. 2020.

[10] Skiena, S. S. The Data Science Design Manual, Text in Computer Science, Springer International Publishing, Cham. 212-221. New York, USA. 2017.

[11] Taigman, Y. Y., Yang, M., Ranzato, M., Wolf, L. DeepFace: Closing the Gap to Human-Level Performance in Face Verification. 2014 IEEE Conference on Computer Vision and Pattern Recognition. Ohio, USA., September, 2014.

[12] Viola, P., Jones, M. Rapid Object Detection using a Boosted Cascade of Simple Features. Proceedings of the 2001 IEEE Computer Society Conference on Computer Vision and Pattern Recognition. Hawaii, USA. December, 2001.

[13] Zarate, J. A. Desarrollo de software de reconocimiento facial, como segundo factor de autenticación que permite realizar inicio de sesión en un computador y generar un reporte de personas no autorizadas [Trabajo de grado, Universidad EAN]. Bogotá, Colombia. 2023.