

PLATAFORMA DE SERVICIOS DE RECONOCIMIENTO FACIAL PARA DETECCIÓN DE PRÓFUGOS DE LA JUSTICIA EN ECUADOR

A FACIAL RECOGNITION SERVICES PLATFORM FOR THE SEARCH OF JUSTICE FUGITIVES IN ECUADOR

<https://doi.org/10.5281/zenodo.3926901>

AUTORES: José González Astudillo^{1*}

Martín Zhindón Mora²

DIRECCIÓN PARA CORRESPONDENCIA: jose.gonzalez.69@est.ucacu.edu.ec

Fecha de recepción: 19 / 02 / 2020

Fecha de aceptación: 22 / 05 / 2020

RESUMEN

El presente trabajo plantea la implementación de una plataforma de reconocimiento facial, diseñada para su uso por entidades de seguridad gubernamentales y por el público en general, mediante servicios web. El objetivo principal de la plataforma es apoyar a las entidades de seguridad del país en la búsqueda y captura de personas requeridas por la justicia, mediante el uso del reconocimiento a partir de imágenes provenientes de fuentes públicas y privadas. Para lograr mejores resultados se escogió el detector de rostros basado en aprendizaje profundo de OpenCV en combinación con un modelo pre entrenado de reconocimiento facial basado en *deep metric learning*. Las pruebas de la plataforma se realizaron utilizando diversas fuentes de imagen en distintos entornos. El resultado final de este trabajo es una plataforma reconocimiento facial, funcional y escalable, con una tasa de éxito de que bordea el 92% con tiempos de respuesta bajos.

Palabras clave: *Aprendizaje profundo, reconocimiento facial, detección de rostros, biometría.*

^{1*} Ingeniero de Sistemas, Universidad Católica de Cuenca.

² Magister en Geomatica con Mención en Ordenamiento Territorial, Universidad Católica de Cuenca.

ABSTRACT

This document presents the design and implementation of a facial recognition platform conceived for government security organizations and the general public through web services. The main objective of the platform is to support security organizations in the processes of searching and capturing people who are required by justice, using facial recognition techniques applied into images generated from public and private sources. The best results we obtained involved the use of the OpenCV deep learning based face detector, chosen in combination with a pre-trained facial recognition model based on deep metric learning. The testing was done using multiple video sources in different environments. The final result is a functional, scalable and reliable facial recognition platform, with a success rate of 92% and low response times.

Keywords: *Deep learning, facial recognition, face detection, biometry.*

INTRODUCCIÓN

En el Ecuador, los índices delincuenciales han incrementado de manera alarmante. Según el Ministerio de Gobierno (2019), en el año 2019 el robo a personas incrementó un 8% con respecto al 2018, de igual manera el robo a unidades económicas creció un 9% y el robo a vehículos un 20%. En cuanto a homicidios intencionales, estos se incrementaron un 15% a nivel nacional. Aunque los gobiernos de turno invierten recursos para mitigar las causas que provocan la inseguridad ciudadana, esta parece llevar un paso adelante en todos los aspectos.

Debido a la actual situación de violencia y delincuencia que atraviesa el país, es necesario proponer soluciones que permitan reducir los índices de inseguridad. El desarrollo del presente trabajo pretende impactar en el ámbito social, específicamente en el bienestar ciudadano, mediante el uso de las tecnologías de la información.

En esta propuesta se implementó una plataforma de reconocimiento facial, diseñada para ser expuesta al público mediante servicios web. La lógica desplegada se estructuró para satisfacer los requerimientos y contexto del país, buscando la integración con los entes encargados de la seguridad ciudadana. Al tener el control del desarrollo de la plataforma se combinaron diferentes técnicas y cambios a los algoritmos de detección de rostros y reconocimiento facial.

En el ámbito de los métodos tradicionales de reconocimiento facial, Kumar, Kumar, Malathi, Vengatesan & Ramakrishnan (2018) proponen un sistema de reconocimiento facial para identificación de sospechosos. Su propuesta plantea una arquitectura en la que, a partir de una fuente de video se extraen características del rostro utilizando el algoritmo de histogramas de patrones locales binarios, estas características se comparan con una base de datos para obtener el rostro más parecido.

Es importante recalcar que los métodos tradicionales, tanto de detección de rostros y objetos (filtros de haar, histogramas de gradientes orientados) como también los algoritmos de reconocimiento facial (*Eigenfaces*, *FisherFaces*, *Local Binary Patterns*) han quedado rezagados frente a las nuevas tendencias que tienen como base el aprendizaje profundo. Deng y Yu (2014) definen al aprendizaje profundo como “*Un tipo de técnica de aprendizaje de máquina que utiliza varias capas de procesamiento de información no lineal, para obtener características, transformarlas, analizar sus patrones y clasificarlas*” (p.200).

Schroff, Ludwiczuk, y Satyanarayanan (2015) presentan FaceNET, un modelo de red neuronal convolucional para verificación y reconocimiento facial, entrenado utilizando la función *triplet loss*. El modelo logra un porcentaje de aciertos del 99.63% en el *dataset labeled faces in the wild* (Huang, Ramesh, Berg y Learned-Miller 2007).

King (2017) propone un modelo de reconocimiento facial basado en una red neuronal residual de 29 capas de convolución. El modelo planteado predice correctamente si dos imágenes corresponden a la misma persona, con una tasa de éxito del 99.38 %. Las pruebas se realizaron en el *dataset labeled faces in the wild* (Huang et al. 2007). El modelo y la librería son de libre acceso al público.

Hmani y Petrovska-Delacretaz (2018) realizan un análisis y estudio de *framework* OpenFace (Amos, Ludwiczuk y Satyanarayanan. 2016). En su investigación explican el proceso de experimentación y reentrenamiento del sistema, logrando superar el porcentaje de aciertos original. Además presentan una comparación de varios sistemas de reconocimiento facial como se puede apreciar en la tabla 1.

Tabla 1. Comparación de sistemas de reconocimiento facial.

Sistema	Desarrollador	Porcentaje de aciertos
FaceNet	Google	99.63 %
DeepID2	Departamento de ingeniería de la universidad de Hong Kong, China.	99.15%
VGG-DeepFace	Visual Geometry Group (VGG) de la universidad de Oxford	98.95%
CASIANet	Instituto de automatización de la academia de ciencias chinas	96.13%
DeepFace	Facebook	97.35%

Fuente: Hmani y Petrovska-Delacretaz (2018), State-of-the-art face recognition performance using publicly available software and datasets.

RESULTADOS

Santoso y Kusuma (2018), también realizan una modificación en el *framework* OpenFace, alterando la red neuronal de convolución para generar un modelo que les permite lograr un porcentaje de aciertos de 95%. En el mismo ámbito, Zheng y Zu (2018) plantean una red neuronal de convolución ligera para reconocimiento facial, la misma que según los autores “consume menos recursos de hardware mientras brinda un excelente desempeño”, los resultados de pruebas en la red propuesta alcanzan un porcentaje de aciertos de 98.46%.

En el presente trabajo se expone el diseño e implementación de una plataforma de reconocimiento facial, basada en redes neuronales profundas y herramientas *open source*, para la identificación de prófugos de la justicia en el Ecuador.

METODOLOGÍA

1. Análisis de técnicas de procesamiento de imágenes

Para la selección del método de detección de rostros a utilizar, se realizó una comparativa entre los detectores de las librerías *open source* Dlib y OpenCV. El detector por defecto de la librería Dlib está basado en el algoritmo de extracción de características por histogramas de gradientes orientados o hog (*Histogram of oriented gradients*). Por otro lado, el detector de rostros de la librería OpenCV se basa en redes neuronales profundas. Las pruebas se realizaron sobre un conjunto de 252 imágenes.

Tabla 2. Resultados de pruebas de detectores de rostros.

Librería	Rostros detectados	Falsos positivos	Tiempo promedio de detección (segundos)
OpenCV	1665	15	0.5304
Dlib	795	3	0.6172

Nota: Para las pruebas se realizó un escalamiento a una dimensión de 600 x 600 píxeles. Ambos detectores se ejecutaron bajo las mismas condiciones de entrada de datos y capacidades de procesamiento.

Fuente: Autor

Como se puede apreciar los resultados de la tabla 2, el detector de OpenCV logró identificar una mayor cantidad de rostros y en tiempos menores, en comparación con el detector de Dlib. Otro factor determinante se puede apreciar en la figura 1, el detector de OpenCV abarca un área mayor de detección del rostro, esto es importante ya que permite obtener características de mejor calidad sobre el rostro a identificar. Debido a esto se decidió utilizar el detector de OpenCV en esta investigación.

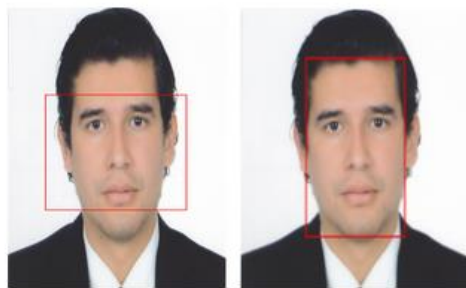


Figura 1. Comparación de áreas de detección de rostros para algoritmos, a la izquierda el resultado del detector de Dlib, a la derecha el resultado del detector de OpenCV.

Fuente: Autor

En cuanto a la selección del modelo de reconocimiento facial se puso a prueba el algoritmo de la librería Dlib, desarrollada por King (2017), contra el algoritmo del *framework* OpenFace. En ambos casos, los algoritmos procesan los rostros para obtener una

representación del mismo, en forma de un vector escalar de 128 variables discretas, conocido también como *image embedding*.

Para la comparación de los algoritmos, se seleccionó aleatoriamente 100 personas del *dataset labeled faces in the wild* (Huang et al. 2007). Por cada persona se utilizó una fotografía para simular la base de datos y otra fotografía como entrada del sistema.

El proceso de pruebas se realizó procesando las 100 imágenes de base, y por cada imagen de entrada, se obtuvo su *image embedding* y se realizó una iteración y comparación de distancia sobre los valores previamente recolectados, con la finalidad de obtener el rostro más similar. Se considera un caso exitoso si el proceso predice la identidad de la persona. Los resultados de la prueba se exponen en la tabla 3:

Tabla 3. Resultados de pruebas de reconocimiento facial.

Librería	Cantidad de sujetos	No reconocidos	Errores	Aciertos	Porcentaje de aciertos
OpenCV	100	1	4	94	94%
Dlib	100	2	28	70	70%

Nota: Para las pruebas de reconocimiento no se realizó pre procesamiento previo y se utilizó el detector de rostros de OpenCV.

Fuente: Autor

1. Diseño de la arquitectura de la plataforma

Para el desarrollo de la solución, se desplegó el servicio mediante la arquitectura cliente servidor con una base de datos centralizada. El diagrama de la arquitectura planteada se indica en la figura 2. El diseño de la plataforma permite su despliegue en múltiples servidores de aplicación independientes, lo cual plantea un escenario compatible con servicios en la nube.

Al desplegar la plataforma en la nube se puede realizar un balanceo de carga de las peticiones recibidas y también un escalamiento automático en función de las necesidades de procesamiento.

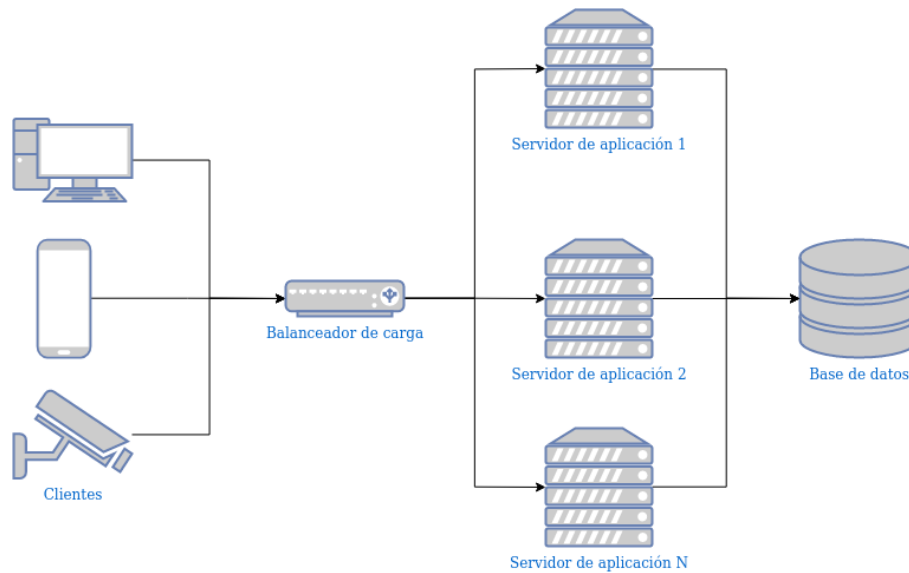


Figura 2. Diagrama de arquitectura para la plataforma de reconocimiento facial.

Fuente: Autor

1. Desarrollo de la plataforma de reconocimiento facial

La plataforma se compone de múltiples *frameworks* y librerías que interactúan entre sí. Para el desarrollo de la aplicación web se utilizó el *framework Java Enterprise Edition 2* en conjunto con otros componentes que se pueden apreciar en la figura 3.

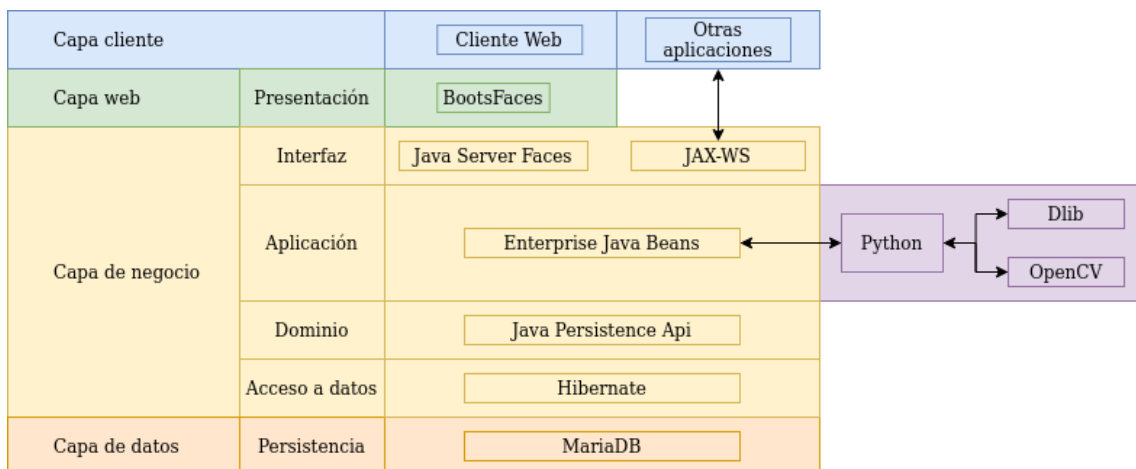


Figura 3. Diagrama de capas de la plataforma

Fuente: Autor

La capa de negocio interactúa con los componentes de detección de rostros y reconocimiento facial mediante llamadas a procedimientos remotos desplegados en *Python*. Estos últimos permiten un acoplamiento sencillo con las librerías OpenCV y Dlib.

El almacenamiento de información se realiza mediante el sistema gestor de base de datos MariaDB. El diagrama entidad relación de la figura 4, muestra las tablas creadas, las mismas permiten gestionar la información personal de los sujetos de interés judicial, sus *image embeddings* y también las consultas realizadas a la plataforma.

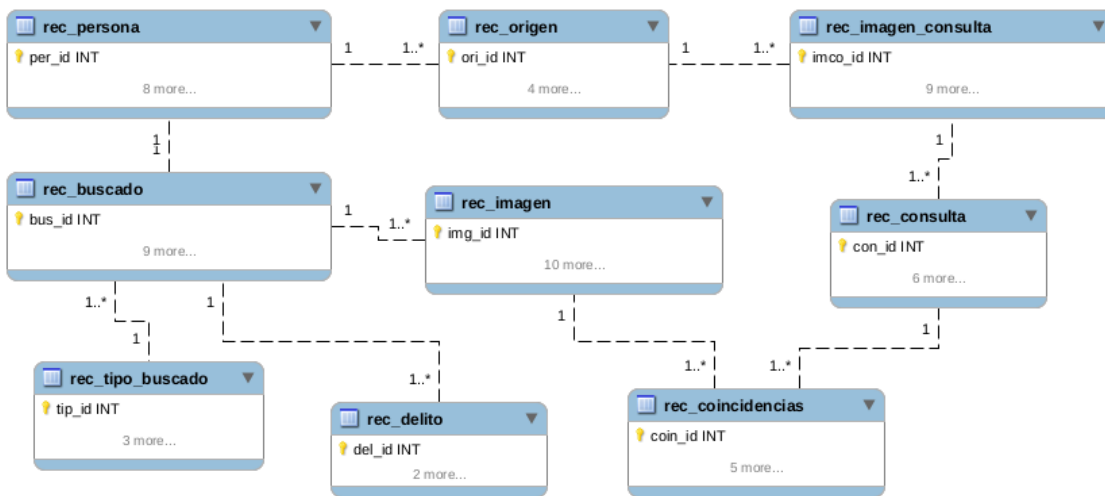


Figura 4. Diagrama entidad relación creado para la plataforma. Fuente: Autor

1. Pruebas de funcionamiento

En las pruebas de funcionamiento ejecutadas se simuló una base de datos de 300 personas requeridas por la justicia, para las cuales se almacenó información de identificación, nombre legal, sexo y una imagen frontal por persona. Una vez ingresada la información de base, se probó con 90 fotografías de 18 sujetos registrados en la base de datos. Cada una de las imágenes se procesó en la plataforma y se comparó contra las 300 previamente almacenadas. El proceso de obtención de similitud se realizó mediante el cálculo de la distancia entre los *image embeddings*.

El sistema devuelve como predicción de identidad, la información asociada a la persona con el valor de similitud más alto obtenido en el proceso de comparación, siempre y cuando supere un umbral de al menos 50% de similitud. El porcentaje de aciertos al predecir la identidad de las personas fue de 92%, los resultados de las pruebas se listan en la tabla 4.

Tabla 4. Resultados de pruebas de la plataforma

Sexo	Cantidad de imágenes	No reconocido	Errores	Aciertos
Hombre	60	5	0	55
Mujer	30	2	0	28

Nota: Para validar el funcionamiento de la plataforma se utilizó 5 imágenes por sujeto de pruebas, las mismas se recopilaron de diversas fuentes en ambientes no controlados.

Fuente: Autor

RESULTADOS

La plataforma desarrollada integra múltiples técnicas y herramientas, en el caso de la detección de rostros, es posible detectar rostros en múltiples escalas y orientaciones. El proceso de reconocimiento demostró ser eficiente en cuanto a recursos y apto para su consumo mediante servicios web. Los resultados del proceso de pruebas indican que la plataforma tiene un porcentaje de aciertos de 92,2%. La arquitectura propuesta y el diseño orientado a capas, muestran estabilidad y escalabilidad de la plataforma. De igual manera, el almacenamiento de los *image embeddings* en base de datos disminuye las necesidades de procesamiento.

DISCUSIÓN

Los resultados expuestos corroboran la validez y el correcto funcionamiento de la plataforma de reconocimiento facial y sus componentes. El desempeño general es aceptable en cuanto a precisión y tiempos de respuesta.

En los casos en los que el sistema no logra reconocer a la persona se deben considerar las orientaciones extremas de los rostros, la calidad de imagen y el tamaño del rostro en las mismas. Para incrementar los porcentajes de similitud y aciertos es necesario realizar un proceso de mejora de la imagen, corrección de la orientación y agrandamiento del rostro detectado.

CONCLUSIONES

La combinación de múltiples sistemas y modelos open source, permitió desarrollar una plataforma robusta y escalable que permite realizar reconocimiento facial mediante servicios web.

Al utilizar modelos de detección y reconocimiento basados en redes neuronales profundas se obtuvo mejores resultados en comparación con los métodos tradicionales.

Los resultados de las pruebas demuestran que la implementación de la plataforma propuesta en este trabajo, podría contribuir a la búsqueda y captura de personas requeridas por la justicia.

REFERENCIAS BIBLIOGRÁFICAS

Ministerio de gobierno. (2019). *Indicadores de seguridad ciudadana*. [online] Available at: <http://cifras.ministeriodelinterior.gob.ec/comisioncifras/inicio.php#> [Accessed 19 Jan. 2020].

Kumar, V. D. A., Kumar, V. D. A., Malathi, S., Vengatesan, K., y Ramakrishnan, M. (2018, jul). Facial Recognition System for Suspect Identification Using a Surveillance Camera. *Pattern Recognition and Image Analysis*, 28(3), 410–420. Descargado de <http://link.springer.com/10.1134/S1054661818030136> doi: 10.1134/S1054661818030136

Deng, Li, y Yu, Dong. (2014). Deep Learning: Methods and Applications. *Foundations and Trends in Signal Processing*, Vol. 7, Nos. 3–4 (2013) 197–38. Descargado de <https://www.microsoft.com/en-us/research/wp-content/uploads/2016/02/DeepLearning-NowPublishing-Vol7-SIG-039.pdf>

doi: 0.1561/20000000039

Schroff, F., Kalenichenko, D., & Philbin, J. (2015). FaceNet: A Unified Embedding for Face Recognition and Clustering. Proceedings of the IEEE Computer Society Conference on Computer Vision and Pattern Recognition, 07-12-June-2015, 815–823. <https://doi.org/10.1109/CVPR.2015.7298682>

[Huang](#), Gary B., [Ramesh Manu](#), [Berg](#) Tamara y [Learned-Miller](#), Erik. (2007) Labeled Faces in the Wild: A Database for Studying Face Recognition in Unconstrained Environments. University of Massachusetts, Amherst, Technical Report 07-49, October, 2007.

King, D. E. (2017). *High Quality Face Recognition with Deep Metric Learning*. Recuperado a partir de <http://blog.dlib.net/2017/02/high-quality-face-recognition-with-deep.html>

Hmani, M. A., y Petrovska-Delacretaz, D. (2018, mar). State-of-the-art face recognition performance using publicly available software and datasets. En *2018 4th international*

conference on advanced technologies for signal and image processing (atsip) (pp. 1–6). IEEE. Descargado de [https://ieeexplore.ieee.org/document/8364450/](https://ieeexplore.ieee.org/document/8364450) doi: 10.1109/ATSIP.2018.8364450

Amos B., Ludwiczuk B. y Satyanarayanan M. (2016) Openface: A general-purpose face recognition library with mobile applications.

Santoso, K., y Kusuma, G. P. (2018). Face Recognition Using Modified OpenFace. *Procedia Computer Science*, 135, 510–517. Descargado de <https://linkinghub.elsevier.com/retrieve/pii/S1877050918314935> doi: 10.1016/j.procs.2018.08.203

Zheng, H. H., y Zu, Y. X. (2018). A Normalized Light CNN for Face Recognition. *Journal of Physics: Conference Series*, 1087, 062015. Descargado de <http://stacks.iop.org/1742-6596/1087/i=6/a=062015?key=crossref.24baf4cfe11a56fb226724dcbc99e1c1> doi: 10.1088/1742-6596/1087/6/06201513