ISSN: 0798-1015 DOI: 10.48082/espacios-a20v41n44p26

REVISTA ESPACIOS

Educación • Education • Educação • Vol. 41 (44) 2020 • Art. 26

Recibido/Received: 12/10/2020 • **Aprobado**/Approved: 12/11/2020 • **Publicado**/Published: 19/11/2020

Diseño e implementación de un sistema de biometría facial para el control de acceso en instituciones de educación superior

Design and implementation of a facial biometric system for access control in higher education institutions

TOVAR, Luis C.[1]
ECHAVEZ, Martín E.[2]
MARTELO, Raúl J.[3]

Resumen
En esta investigación se planteó una solución que busca contribuir con la seguridad en instituciones de educación superior. Como caso de estudio se seleccionó la Universidad de Cartagena con el fin de mejorar los controles de acceso que existen actualmente en esta institución. La investigación calificó como una investigación aplicada y se realizó bajo el Proceso Unificado de *Rational*. Como resultado, se obtuvo un sistema que puede reconocer a un usuario a una distancia de 5 metros máximo.
Palabras clave: seguridad, biometría, vigilancia, inteligencia artificial, identificación

Abstract
In this research, a solution that seeks to contribute to security in higher education institutions was proposed. As a case study, the University of Cartagena was selected to improve the access controls that exist in this institution. The research qualified as applied research and was conducted under the Rational Unified Process. As a result, a system that can recognize a user at a maximum distance of 5 meters was obtained.
key words: security, biometrics, surveillance, artificial intelligence, identification

1. Introducción

El reconocimiento facial es un área de gran interés por su impacto y aplicaciones en temas de carácter laboral, control de acceso, seguridad ciudadana, entre otros (Serratosa, 2012). Con la aplicación de sistemas basados en este tipo de tecnología se pueden reconocer criminales conocidos o sospechosos y las organizaciones pueden evaluar las caras de sus clientes con el fin de elaborar estrategias de marketing (Cadena, Montaluisa, Flores, Chancúsig, & Guaypatín, 2017). En este sentido, los sistemas biométricos permiten identificar a una persona mediante distintas partes del cuerpo humano, lo cual implica emular el proceso cognitivo que realiza un ser

[1] Profesor. Facultad de Ingeniería. Universidad de Cartagena. ltovarg@unicartagena.edu.co
[2] Ingeniero de Sistemas. Facultad de Ingeniería. Universidad de Cartagena. martinechavez1994@gmail.com
[3] PhD (e) – Magister en Informática. Líder del grupo de investigación INGESINFO. Profesor de planta del Programa Ingeniería de Sistemas de la Universidad de Cartagena. e-mail: rmartelog1@unicartagena.edu.co

humano al reconocer a sus semejantes (Scarel & Müller, 2010). Es en este aspecto, donde el estudio de la biometría, y los avances de la tecnología, dan como resultado la toma de medidas y el análisis de datos biológicos

como la huella de la mano, el iris y la voz (Nelson, 2018). De este modo, surgen los sistemas de reconocimiento facial, que toman decisiones de identificación de acuerdo a las características de las personas (Anscombe, 2017).

El sistema de reconocimiento facial es una tecnología asociada con promesas para fortalecer la seguridad pública, la comprobación de la identidad de los usuarios de entidades financieras, creación de vallas publicitarias inteligentes que muestran anuncios en respuesta a los estados de ánimo de los transeúntes (Andrejevic & Selwyn, 2020). En cuanto a la seguridad, estos sistemas son considerados como uno de los sistemas más confiables, debido a que sistemas con las claves de acceso o tarjeta, son vulnerables a ultrajes o clonaciones respectivamente, a diferencia de los sistemas que se basan en biometría (Motato & Loaiza , 2009). Por lo anterior, estas tecnologías son cada vez más aplicadas en diferentes sectores. En el trabajo de Morosan y colaboradores (Morosan, 2020) se presenta un sistema de reconocimiento facial dirigido a hoteles, que se describe como sistemas computarizados automatizados que permiten a los huéspedes del hotel el check-in / out, acceder a sus habitaciones y a otras áreas solo para huéspedes con identificación y verificación basada en imágenes faciales.

En el trabajo de Hoang y colaboradores (Hoang, Dang, Nguyen, & Tran, 2018) se despliega una solución basada en la combinación de etiquetas RFID y reconocimiento facial para monitorear la asistencia de los empleados cuando entran o salen de la oficina. Mientras que en el trabajo de Trivikram y colaboradores (Trivikram, Samarpitha, Madhavi, & Mose, 2017) se evalúa un sistema híbrido de reconocimiento facial y de voz para identificación biométrica en áreas que requieren alta seguridad, utilizan las dos tecnologías, porque afirman que el reconocimiento facial no es efectivo para identificar a personas cuando usan anteojos, sombreros o tienen barba. En cuanto a las instituciones educativas, la implementación de sistemas de reconocimiento facial se ha acelerado, debido a su ya extensa infraestructura de videovigilancia y vigilancia de circuito cerrado (Andrejevic & Selwyn, 2020). Un caso que pudo ser resuelto por este tipo de tecnología fue el caso del robo del bolso de la esposa del embajador de Corea del Sur Kim Doo-Sik quienes asistían a un evento de cultura en la Universidad de Cartagena al interior del Campus San Agustín (El Tiempo, 2019). Por lo anterior, se han realizado algunos proyectos donde se presenta un proyecto de investigación dirigido a la identificación, análisis y prueba sistemáticas de sistemas de reconocimiento facial de código abierto y comerciales disponibles, para universidades inteligentes altamente tecnológicas (Bakken, Varidireddy, & Uskov, 2020).

Por los beneficios de la tecnología de reconocimiento facial y debido a los eventos de inseguridad que se pueden presentar al interior de las instituciones educativas, se plantea este proyecto, que busca controlar el acceso a las instalaciones de las instituciones apoyando la seguridad de directivos, trabajadores y estudiantes dentro de los planteles, con el fin de disminuir el número de hurtos y otros hechos delictivos.

2. Metodología

La presente investigación se tipificó como aplicada, debido a que busca resolver un problema (Hernández, Fernández, & Baptista, 2014). La investigación aplicada se caracteriza por utilizar o aplicar conocimientos adquiridos a la vez que se adquieren otros, luego de implementar y sistematizar la práctica fundamentada en investigación (Murillo, 2008). Por otro lado, se obtuvo información disponible en libros, artículos y diferentes publicaciones científicas asociadas a la Inteligencia Artificial (IA) y al reconocimiento facial. Como técnicas de recolección de información se aplicó la encuesta. Se realizaron dos encuestas, una dirigida a personas con conocimiento en tecnologías de desarrollo software y otras a personas del común sin conocimientos expresos sobre tecnologias. Con la primera el objetivo fue facilitar la elección de la metodología de desarrollo y la segunda conocer la percepción de seguridad que tienen las personas.

2.1. Metodología de desarrollo del software

Este proyecto se realizó bajo los criterios y principios de la metodología de desarrollo de software RUP (Rational Unified Process), la cual es una metodología iterativa e incremental que se caracteriza por su enfoque en casos de uso y la arquitectura de la solución a desarrollar (Kruchten, 2004). Estas características permiten tener siempre en cuenta los requerimientos, la creación de modelos y vistas para comprender cada parte del software y fomentar la reutilización de componentes (Martínez & Martínez, 2014). A continuación, se describen las fases correspondientes a la metodología RUP, que dieron solución a cada uno de los objetivos específicos del proyecto.

Fase inicial: se recolectó información relacionada con el reconocimiento facial en libros, revistas científicas y otros documentos, de igual manera, se obtuvo información a partir de una población de estudiantes, administrativos y docentes activos, a los cuales se les realizaron dos encuestas, lo cual facilitó determinar y especificar los requerimientos funcionales.

Fase de elaboración: en esta fase se diseñaron los artefactos UML (diagramas y modelos), que permitieron construir una arquitectura y un plan de desarrollo para el software.

Fase de construcción: se desarrolló un prototipo del software a partir de los artefactos UML, es decir, el desarrollo de los componentes y funcionalidades, implementación de estructuras de datos, elaboración de documentación técnica, la integración de la solución y las pruebas de verificación del prototipo desarrollado.

Fase de transición: se realizaron las pruebas de validación del software desarrollado en un entorno real, así como la elaboración de la documentación final del software.

Con la arquitectura planteada se desarrolló el sistema de reconocimiento facial para el control de acceso en la Universidad de Cartagena, con los resultados obtenidos se pudo evidenciar la eficiencia del proyecto en términos de seguridad y rendimiento.

3. Resultados

3.1. Obtención de datos

Para esta investigación se tomó como caso de estudio la Universidad de Cartagena, el Campus de Piedra de Bolívar. Se empleó muestreo probabilístico, con el fin de brindar participación equitativa, lo cual implica el carácter aleatorio. La muestra calculada, con un nivel de confianza del 95%, fue de 150 personas encuestadas: entre estudiantes, administrativos y docentes, activos (en el periodo 2020-1), como se muestra en la Tabla 1.

Tabla 1

Características de la población y muestra

Universo	Estudiantes, docentes y administrativos de la Universidad de Cartagena.
Ámbito geográfico	El estudio se realizó en el campus de Piedra de Bolívar.
Metodología	Encuestas por medo virtual utilizando Formularios de Google.
Periodo de recogida de la información	Primer periodo del año 2020
Tipo de muestreo	Muestreo aleatorio
Tamaño de la muestra	150 personas
Error del muestreo	±4,9%
Nivel de confianza	±95%

Fuente: Autores

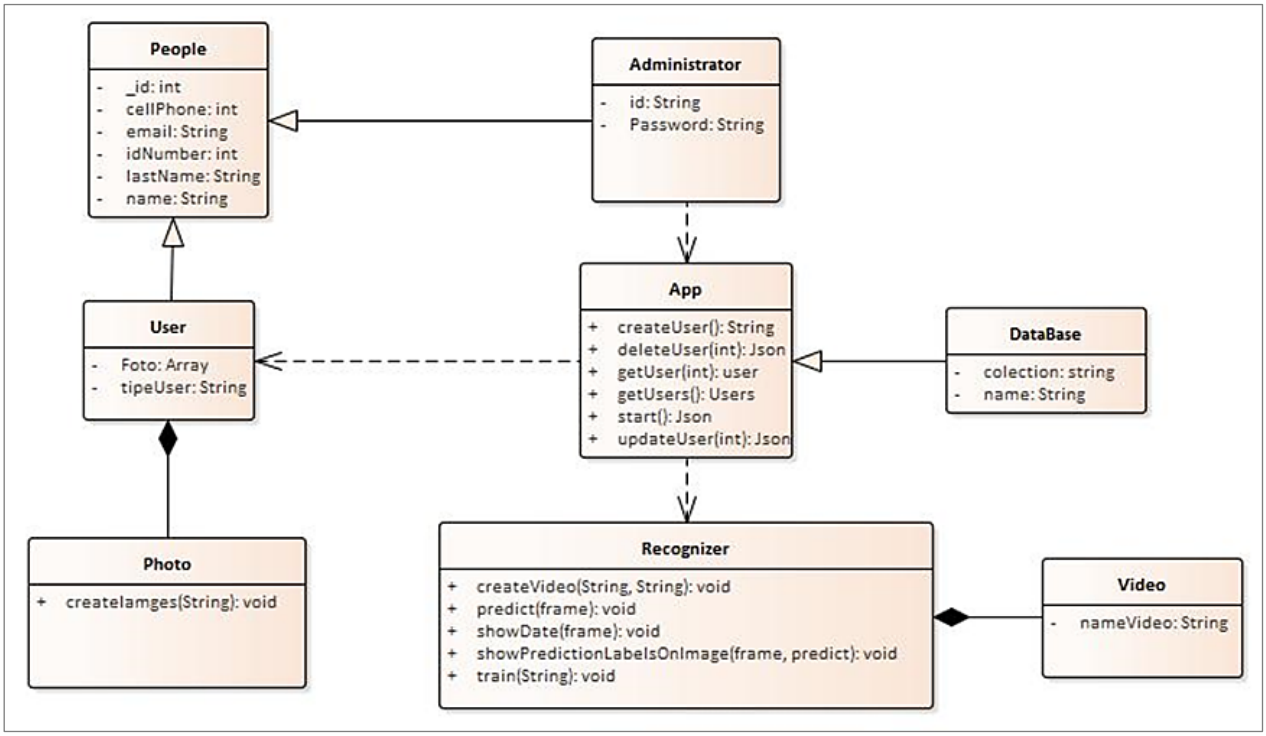
Para la obtención de la información se publicó la encuesta en grupos de redes sociales de la Universidad y también se envió directamente a algunos docentes y administrativos.

3.2. Levantamiento de requisitos

Una vez obtenido los resultados de la encuesta se realizó el levantamiento de requisitos del sistema, con el fin de plantear la arquitectura base que sostiene el proyecto. Como parte de la arquitectura del proyecto se realizó el diagrama de clases de la aplicación web, el cual es fundamental en el desarrollo del proyecto, el diagrama obtenido se observa en la Figura 1.

Figura 1

Diagrama de clases



Fuente: autores

3.3. Desarrollo del proyecto

El proyecto se realizó teniendo en cuenta la arquitectura planteada, con tecnologías como Inteligencia Artificial, Machine Learning y almacenamiento en la nube, entre otros. El lenguaje de programación utilizado fue Python en el Backend y React.js en el Frontend, la base de datos utilizada fue MongoDB, la cual ofrece un despliegue gratuito en la nube de Mongo Atlas.

3.4. Elaboración del software

Para elaborar el software se utilizó el lenguaje de programación Python como lo sugirieron las personas expertas en tecnología en la encuesta realizada, este lenguaje de programación es muy popular en los campos de inteligencia artificial, Big Data e investigaciones científicas (Galeano & Peña, 2019). De igual manera se utilizó la librería OpenCv, la cual es open source y es utilizada en proyectos relacionados con el tratamiento de imágenes y videos (Arévalo, González, & Ambrosio, 2004). OpenCV (Open Source Computer Vision Library) es una biblioteca de software de aprendizaje por computadora y visión por computadora de código abierto, tiene interfaces C++ Python, java y MATLAB y es compatible con Windows, Linux, Android y Mac OS, esta librería es open source y totalmente gratuita (OpenCV, 2020).

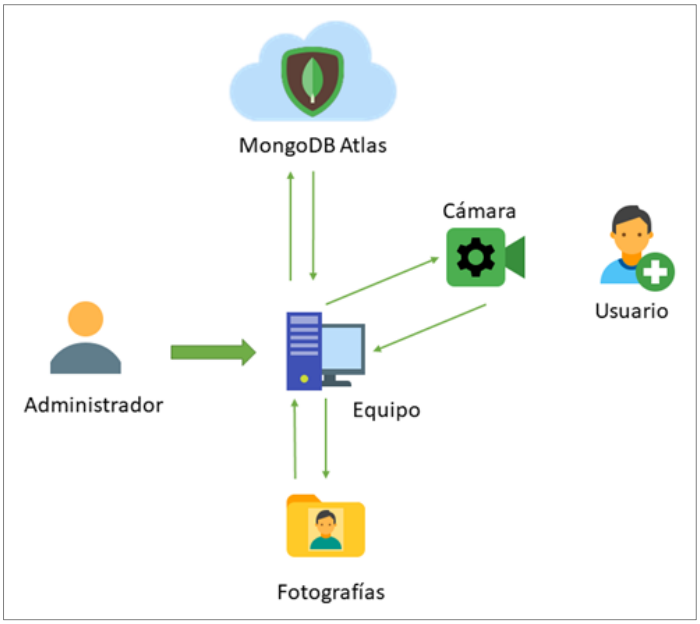
También se utilizaron paquetes de Python como NumPy, el cual es utilizado en computación científica, y también se puede utilizar como un contenedor eficiente multidimensional de datos genéricos (Numpy, 2020). Por otro lado, para mejorar el reconocimiento facial por parte de la librería OpenCv se utilizó la librería de Python Face-Recognition, la cual trabaja en conjunto con esta para optimizar el reconocimiento del rostro de las personas (Park & Jain, 2007). Esta biblioteca se especializa en encontrar y manipular rostros en imágenes, ubicando contornos de los ojos, nariz, boca y mentón de cada persona (Face-Recognition, 2020). Os, es otro de los paquetes utilizados, este proporciona una forma portátil de utilizar las funcionalidades del sistema operativo, en el proyecto se utiliza para la crear, eliminar y tener control sobre el sistema operativo.

3.5. Visión general del sistema

En la Figura 2 se observa un esquema que representa el sistema. Este sistema de reconocimiento facial está diseñado para trabajar en entornos web, una vez desplegado en un servidor, permitirá conectarse desde cualquier lugar donde se tenga acceso a internet. Para que el sistema pueda empezar a funcionar se debe contar con mínimo una cámara, la cual será la encargada de realizar el reconocimiento.

Figura 2

Esquema del sistema de reconociendo facial



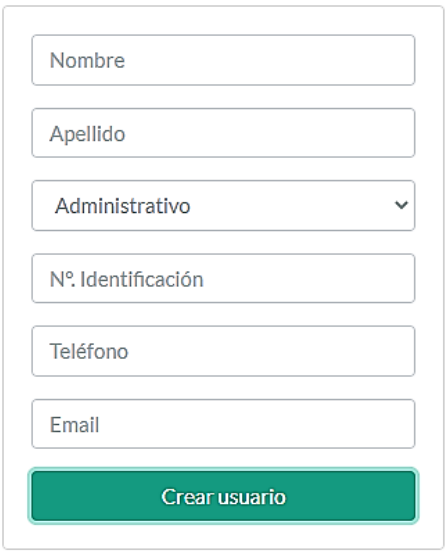
Fuente: autores

3.6. Registro de usuarios

Para registrar un usuario en el sistema se debe solicitar nombre, apellido, cargo que ocupa dentro del platel educativo (estudiante, docente o administrativo), número de identificación, teléfono y el correo electrónico, como se muestra en la Figura 3.

Figura 3

Formulario de registro



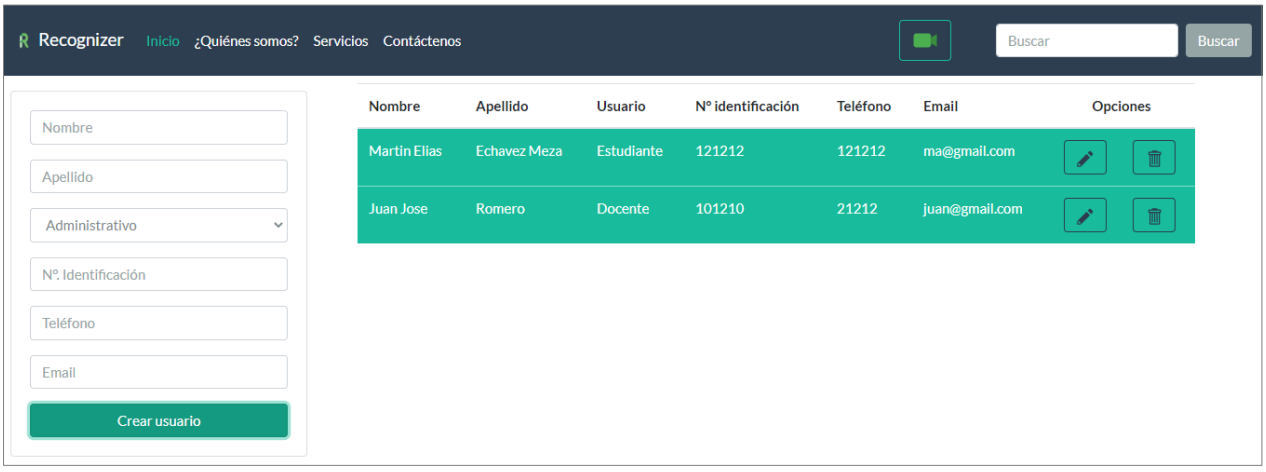
Fuente: autores

Al momento de registrar al usuario, se le pedirá que se ubique frente a la cámara con el fin de tomar 100 fotografías, las cuales serán almacenadas junto con los datos del usuario. Este proceso toma un tiempo aproximado a los 3 segundos. Los datos personales del usuario son almacenados en una base de datos alojada en MongoDB Atlas, el cual es un servicio gratuito en la nube que ofrece este administrador de base de datos, no obstante, las fotografías del usuario serán almacenadas de forma local en el equipo donde se encuentre desplegado el sistema.

Una vez creado el usuario, el sistema lista los usuarios creados, adicionalmente muestra dos botones para editar y eliminar usuarios de la plataforma. La vista completa del sistema se muestra a continuación en la Figura 4.

Figura 4

Vista principal del administrador



Fuente: autores

3.7. Entrenamiento del sistema

El entrenamiento del sistema ocurre cada vez que se inicia el proceso de reconocimiento facial, es decir, cada vez que la cámara es encendida para empezar a reconocer a los usuarios que van a hacer su ingreso al plantel, se genera un archivo con extensión .yml el cual guarda las especificaciones de los rostros de las personas almacenadas en el sistema.

3.8. Identificación de personas por parte del sistema

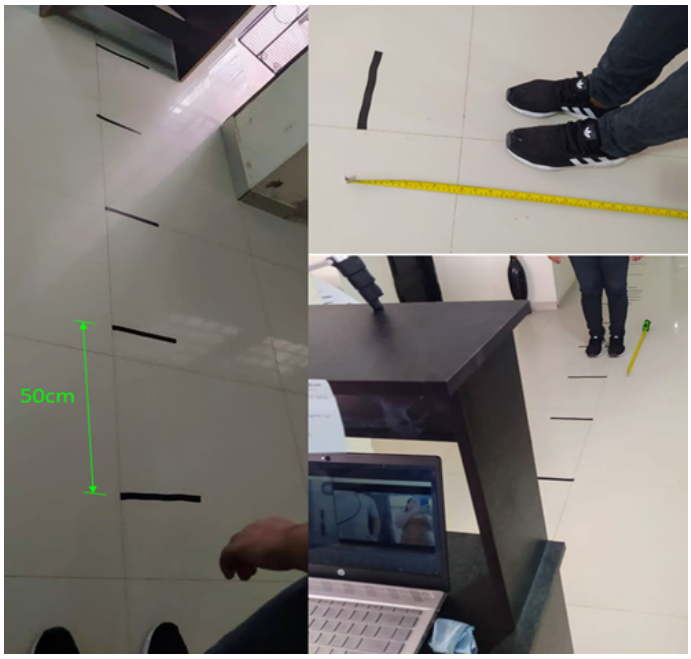
Para la identificación de los usuarios se debe encender el modo reconocimiento por parte del administrador del sistema, después los usuarios deben detenerse en frente de la cámara para que el sistema pueda reconocer sus rostros al momento de realizar el ingreso. El sistema compara el rostro con los ya entrenados previamente en el sistema, si el usuario se encuentra registrado mostrará el nombre completo de la persona en un recuadro debajo de su rostro en la pantalla, en caso contrario, se enviará un texto con la palabra desconocido en el mismo recuadro.

3.9. Pruebas de distancia

Se realizaron 5 tipos de pruebas al sistema, las cuales fueron: Pruebas de distancia, distancia vs personas, personas en movimiento, cantidad de personas vs número de cámaras y personas usando accesorios. Las pruebas de distancia fueron realizadas en ambientes controlados teniendo en cuenta una buena iluminación y el rostro totalmente descubierto por parte del usuario a reconocer, la cámara situada en un punto fijo. Para tener una medida exacta se colocaron marcas en el piso a una distancia de 50 centímetros cada una, también se utilizó un metro para corroborar la distancia entre cada una de las marcas colocadas, como se muestra en la Figura 5.

Figura 5

Prueba de distancia



Fuente: autores

Los resultados obtenidos se observan en la Tabla 2.

Tabla 2

Resultados obtenidos de la prueba de distancia

Distancia	Detección	Identificación
5 metros	No evidenciada	No evidenciada
4 metros	No evidenciada	No evidenciada
3 metros	Evidenciada	Evidenciada
2.45 metros	Evidenciada	Evidenciada
1 metro	Evidenciada	Evidenciada
50 centímetros	Evidenciada	Evidenciada

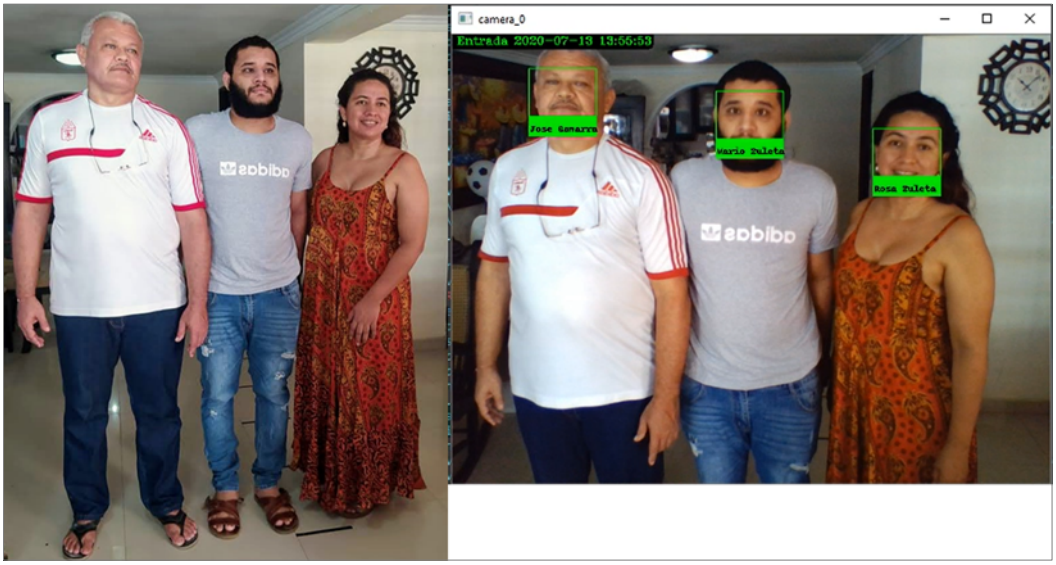
Fuente: Autores

3.10. Distancia vs personas

Esta prueba se realizó con 3 personas a una distancia de 2 metros como se observa en la Figura 6.

Figura 6

Prueba de distancia vs personas



Fuente: autores

En la Tabla 3 se muestran los resultados obtenidos de la prueba distancia vs personas.

Tabla 3

Resultados obtenidos de la prueba distancia vs personas

Distancia (metros)	Personas	Detección	Identificación
2	2	Evidenciada	Evidenciada
2	3	Evidenciada	Evidenciada
2	4	Evidenciada	Evidenciada
2	5	Evidenciada	Evidenciada
1	2	Evidenciada	Evidenciada
50 cm	2	Evidenciada	Evidenciada

Fuente: Autores

3.11. Personas usando accesorios

Esta prueba se realiza con el fin de prever al administrador del sistema sobre posibles accesorios que pueden impedir el correcto funcionamiento del sistema (ver Tabla 4).

Tabla 4

Prueba con personas usando accesorios

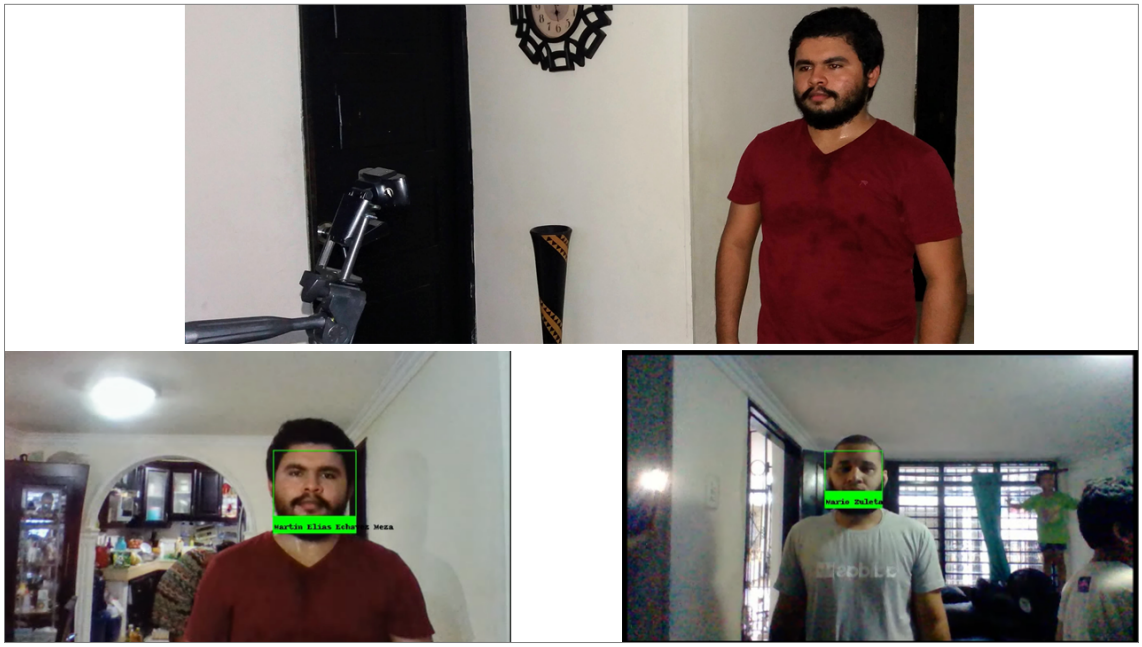
No de Pruebas realizadas	Accesorio	Detección	Identificación
1	Barba	Evidenciada	Evidenciada
1	Sombrero	Evidenciada	Evidenciada
1	Gorra	No Evidenciada	No Evidenciada
2	Gorra	Evidenciada	Evidenciada
1	Gafas de trabajo	Evidenciada	Evidenciada
1	Gafas de sol	Evidenciada	Evidenciada
1	Tapabocas	No Evidenciada	No Evidenciada
2	Tapabocas	Evidenciada	No Evidenciada

Fuente: Autores

La barba es un distintivo que algunos hombres les gusta portar, por estas razones el sistema debe estar preparado para esta situación. Con el fin de realizar las pruebas, se registraron 2 usuarios con barba y distintos cortes de cabello, en la Figura 7 se evidencia la correcta detección e identificación de cada uno de estos casos.

Figura 7

Prueba con barbas



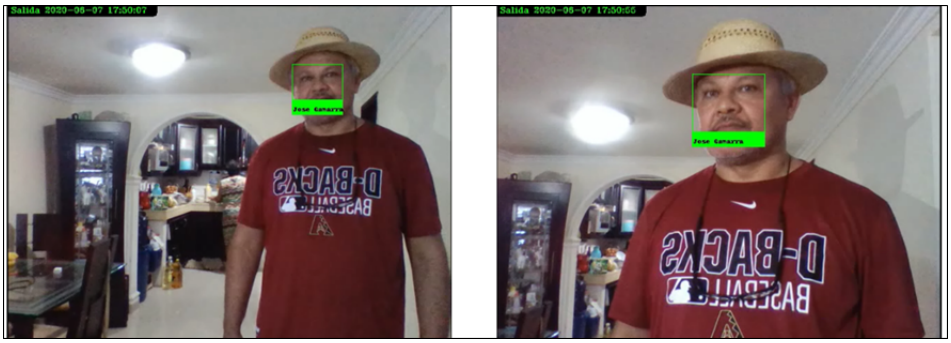
Fuente: autores

Adicionalmente a las pruebas con barba se realizó un experimento donde se registró en el sistema a un usuario con barba, posteriormente este usuario se quitó la barba y el sistema lo reconoció de igual forma.

En cuanto a la prueba con sombrero, no se presentó inconvenientes en la detección ni en reconociendo facial, tal como se muestra en la Figura 8, donde se aprecia que el sistema identifica al usuario.

Figura 8

Prueba con sombrero

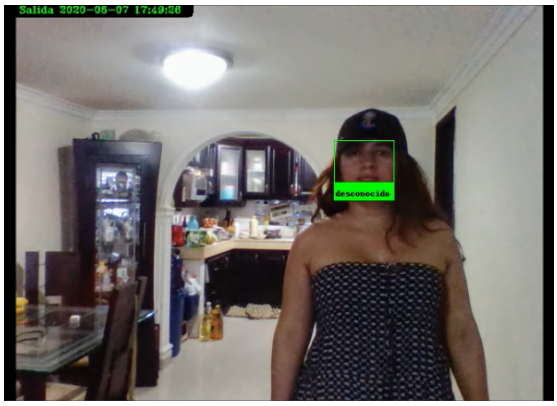


Fuente: autores

Por su parte en la prueba con gorra, se realizaron dos. En la primera prueba se evidenció que este accesorio puede interferir en el reconocimiento de la persona por parte del sistema, detectando el rostro, pero arrojando como resultado, que es un desconocido, tal como se observa en la Figura 9.

Figura 9

Prueba 1 con gorra

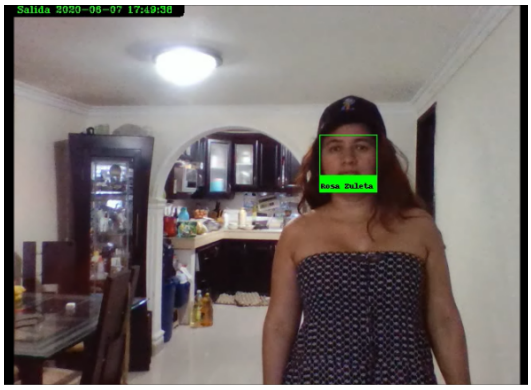


Fuente: autores

Cuando se realizó una segunda prueba con gorra, tanto la detección como la identificación fue exitosa. Como se observa en la Figura 10, lo que cambió fue la posición de la gorra. En la primera prueba la gorra se ubicó hasta cubrir las cejas, mientras que en la segunda se dejan descubiertas las cejas y parte de la frente de la usuaria. Lo anterior indica que, mientras se cubra la mayor parte del rostro con este accesorio, será posible la detección del rostro, pero no el reconocimiento del usuario.

Figura 10

Prueba 2 con gorra

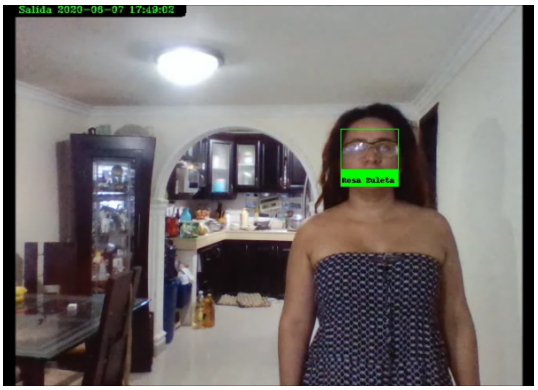


Fuente: autores

Por su parte la prueba con gafas de trabajo evidenció la detección y el reconocimiento sin ningún contratiempo como se observa en la Figura 11.

Figura 11

Prueba con gafas de trabajo



Fuente: autores

En el caso de la prueba con gafas de sol, este accesorio puede generar que el sistema detecte al usuario como desconocido, por lo cual, se debe tener en cuenta el tamaño de las gafas y si es necesario pedirle al usuario que se las retire al momento del registro e identificación en el sistema. En la Figura 12 se evidencia el resultado de esta prueba.

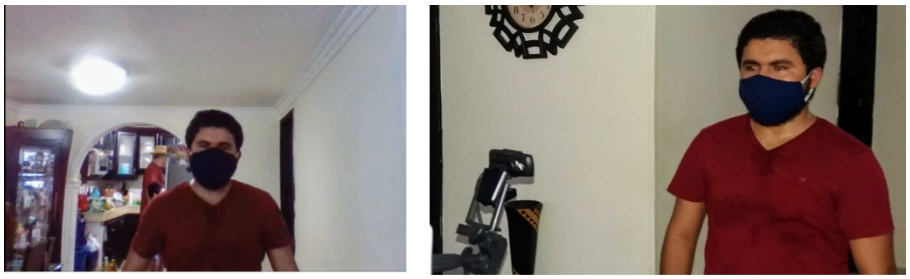
Figura 12

Prueba con Gafas de sol

Fuente: autores

Por otro lado, en las pruebas con tapabocas se evidenció que este accesorio también puede impedir tanto la detección del rostro como el reconocimiento tal como se observa en la Figura 13.

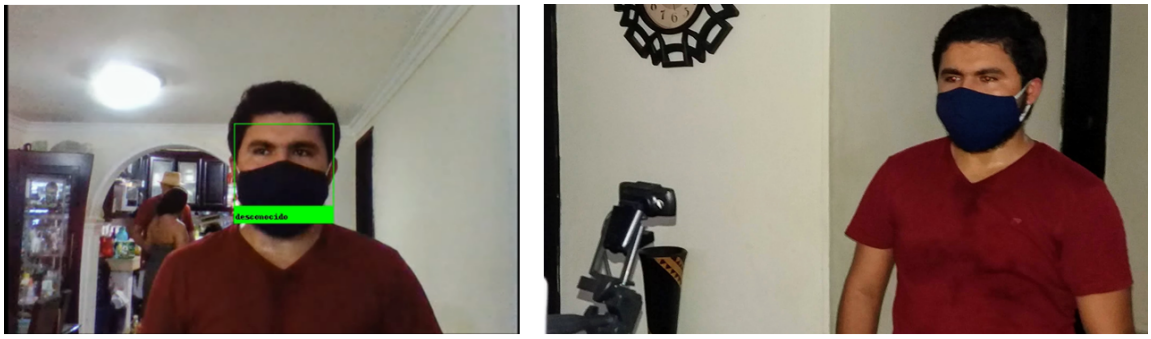
Figura 13
Prueba 1 con Tapabocas



Fuente: autores

En la segunda prueba con tapabocas, se pudo detectar el rostro del usuario, sin embargo, no fue posible el reconocimiento, el sistema arrojó, desconocido, tal como se observa en la Figura 14, la cámara 1 arrojó como resultado, desconocido, mientras que la cámara 2 no detectó el rostro.

Figura 14
Prueba 2 con Tapabocas



Fuente: autores

Cabe resaltar, que estas pruebas con accesorio se realizaron teniendo en cuenta los requisitos planteados por los usuarios encuestados, los cuales pedían que el sistema contara con la capacidad de reconocer a las personas con distintos accesorios.

4. Conclusiones

Según lo expuesto a lo largo de este artículo, debido a los altos índices de inseguridad que se presentan en instituciones públicas o privadas, la identificación facial sirve como apoyo reactivo en investigaciones por robo o pérdida de objetos al interior de entidades donde esté desplegado este sistema, el cual se puede implementar en la entrada y salida de entidades pública o privada, con el fin de tener mayor control sobre la hora de entrada y salida de las personas, además de alertar al personal de seguridad sobre el ingreso de desconocidos. Gracias al desarrollo de este proyecto y a la aplicación de la metodología expuesta, como principales conclusiones se puede resaltar las siguientes:

Uno de los puntos más importantes del proyecto fue la detección de personas con accesorios por parte del sistema, debido a que se tuvo en cuenta estos requisitos por parte de los usuarios para garantizar la calidad del producto software. Con los resultados se evidencia que el proyecto cumple con los requisitos planteados por parte de los usuarios para garantizar la correcta detección e identificación de personas en el lugar donde se realice el despliegue del sistema. De igual manera, teniendo en cuenta los requisitos obtenido en las encuestas se continuó con la arquitectura del proyecto, la cual fue parte importante para realizarlo, se elaboraron los diagramas y las vistas con las que se compone el sistema. Por último, en las pruebas realizadas se puedo

evidenciar que el sistema de reconocimiento facial es capaz de identificar a las personas a una distancia máxima aproximada a los 5 metros. Cabe resaltar que este proyecto fue desarrollado con distintos lenguajes de programación para obtener mejores resultados, y fue realizado desde cero.

Referencias bibliográficas

Andrejevic, M., & Selwyn, N. (2020). Facial recognition technology in schools: critical questions and concerns. Learning, Media and Technology, 45(2), 115-128.

Anscombe, L. (2017, Julio 25). Westfield is Using Facial Detection Software to Watch How You Shop. Retrieved from https://www.news.com.au/: https://www.news.com.au/finance/business/retail/westfield-is-using-facial-detection-software-to-watch-how-you-shop/news-story/7d0653eb21fe1b07be51d508bfe46262

Arévalo, V., González, J., & Ambrosio, G. (2004). La Librería de Visión Artificial OpenCV. Aplicación a la Docencia e Investigación. Base Informática, 40, 61-66.

Bakken, J., Varidireddy, N., & Uskov, V. (2020). Face Recognition Systems for Smart Universities. Springer, 423-439.

Cadena, J., Montaluisa, R., Flores, G., Chancúsig, J., & Guaypatín, O. (2017). Reconocimiento facial con base en imágenes. Revista Boletín Redipe, 6(5), 143-151.

El Tiempo. (2019, Mayo 17). Esposa de embajador de Corea fue a evento en Cartagena y la robaron. EL TIEMPO, p. 1.

Face-Recognition. (2020, 05). pypi.org. Retrieved from https://pypi.org/project/face-recognition/

Galeano, P., & Peña, D. (2019). Las nuevas oportunidades del Big Data para las instituciones financieras. Papeles de Economía Española, 78(162), 78-176.

Hernández, R., Fernández, C., & Baptista, M. (2014). Metodología de la investigación (Sexta ed.). México: Mc Graw Hill Education.

Hoang, V., Dang, V., Nguyen, T., & Tran, D. (2018). A solution based on combination of RFID tags and facial recognition for monitoring systems. In 2018 5th NAFOSTED Conference on Information and Computer Science (NICS) (pp. 384-387). IEEE Xplore.

Kruchten, P. (2004). The Rational Unified Process: An Introduction. Addison-Wesley Professional.

Martínez, A., & Martínez, R. (2014). Guía a Rational Unified Process. Escuela Politécnica Superior de Albacete– Universidad de Castilla la Mancha.

Morosan, C. (2020). Hotel facial recognition systems: insight into guests' system perceptions, congruity with selfimage, and anticipated emotions. Journal of Electronic Commerce Research, 21(1), 21-38.

Motato , O., & Loaiza , H. (2009). Identificación biométrica utilizando imágenes infrarrojas de IA. Revista Ingeniería e Investigación.

Murillo, W. (2008). La investigación científica. Madrid: Ed Semphis.

Nelson, E. (2018). A Qualitative Study Examining the Perception of College Students and Instructors in the Adoption of Biometrics in eLearning. Doctoral dissertation, Northcentral University.

Numpy. (2020, 08 15). Numpy. Retrieved from https://numpy.org/

OpenCV. (2020, 05). OpenCV. Retrieved from https://opencv.org/about/

Park, U., & Jain, A. (2007). 3D model-based face recognition in video. Springer, 1085-1094.

Scarel, G., & Müller, O. (2010). Sistema de reconocimiento facial. Universidad Nacional del Litoral.

Serratosa, F. (2012). La biometría para la identificación de las personas. España: Edi-torial UOC.

Trivikram, C., Samarpitha, S., Madhavi, K., & Mose, D. (2017). Evaluation of Hybrid Face and Voice Recognition Systems for Biometric Identification in Areas Requiring High Security. I-manager's Journal on Pattern Recognition, 4(3).

Esta obra está bajo una Licencia Creative Commons
Attribución-NoCommercial 4.0 International

(cc) BY-NC