ISSN 1870-4069

Plataforma digital para la seguridad escolar mediante el control de acceso automatizado basado en el reconocimiento facial

Cynthia B. Perez[1], Jesus R. Villavicencio[1], Jessica Beltran[2], Roberto Limon-Ulloa[1], Perla Duran[1], Samuel Torres[1], Bryan García[1]

[1] Instituto Tecnológico de Sonora (ITSON), México

[2] Centro de Investigación y Desarrollo de Tecnología Digital (CITEDI-IPN), México

{cynthia.perez, roberto.limon, jesus.villavicencio162447, perla.duran204151, samuel.torres202413, bryana.garcia}@potros.itson.edu.mx, jbeltranm@ipn.mx

Resumen. Las condiciones de inseguridad pública ameritan que se desarrollen sistemas orientados a brindar seguridad dentro de instituciones educativas. Se pueden utilizar diferentes enfoques tecnológicos orientados a apoyar la seguridad, entre ellos, el uso de sistemas de monitoreo automático de personas para verificar que solo ingresan a los campus quienes tienen previa autorización. Una forma no intrusiva de abordar este problema es mediante el reconocimiento facial con técnicas de aprendizaje automático. En este trabajo, se describe el desarrollo de una plataforma digital para el control de acceso automático y notificación de alertas a los guardias de seguridad de una institución educativa. Se realizaron experimentos con la base de datos LFW [28] y con imágenes de estudiantes y profesores de una institución educativa para conocer y comparar la efectividad del reconocimiento facial. Así mismo, se utilizaron características extraídas con redes neuronales profundas y algoritmos de clasificación para identificar a la persona. Los resultados indican la viabilidad de implementar esta plataforma *in situ* y proporcionan direcciones para el trabajo futuro.

Palabras clave: Reconocimiento Facial, universidad inteligente, openface, seguridad escolar.

A Digital Platform for School Security through Automated Access Control based on Facial Recognition

Abstract. Public unsafe conditions justify the development of systems that help to provide security inside educational institutions. There can be different technological approaches to support security, including automatic systems to monitor that only authorized people can enter campus. A non intrusive way to address this problem, is through facial recognition with machine learning techniques. In this work, is described the development of a digital platform to control access automatically and to send alerts to security guards from an educational institution. Experiments were conducted using the data set LFW [28] and with images from students and professors from the

educational institute to know and compare the effectiveness of facial recognition. Thus, features extracted with deep learning and classification algorithms to identify persons were used. The results show the viability to implement the platform *in situ* and provide directions for future work.

Keywords: Facial recognition, smart campus, openface, school surveillance system.

1. Introducción

Hoy en día, el tema de seguridad pública urbana es una de las principales preocupaciones que tiene la sociedad alrededor del mundo, principalmente en aquellos países en vías de desarrollo. En México, de acuerdo con el Instituto Nacional de Estadística y Geografía (INEGI), en el año 2020, el 67.8% de la población mayores de 18 años considera que vivir en su ciudad es inseguro [1]. En ese sentido, debido a la situación que se vive en torno a la seguridad en el país, la ocurrencia de incidentes relacionados con la seguridad no es ajena a las instituciones educativas.

Es por ello que particularmente en las universidades, existe un gran interés por incorporar tecnologías de la información para facilitar la administración y seguridad de los campus. Para apoyar estas iniciativas, se han propuesto diferentes sistemas automatizados para el control de acceso en organizaciones públicas y/o privadas basadas en comunicación de campo cercano (Near Field Communication, NFC) [8], identificación por radio frecuencia (Radio-frequency Identification, RFID) [2-4], sistemas basados en iris y sistemas basados en reconocimiento facial [5-7].

El reconocimiento facial es una de las técnicas más populares para incorporar a los sistemas de seguridad por su facilidad de uso, su naturaleza sin contacto y que no es una técnica intrusiva ni agresiva [1,4,6,7]. De acuerdo con Victor Skinner [9], la Universidad de San Francisco hace uso de un sistema comercial basado en reconocimiento facial llamado iOmniscient [1] para administrar el acceso de los estudiantes a los dormitorios de la universidad, donde el objetivo es contar con una forma de controlar el acceso a las residencias universitarias que no sea intrusivo y que no requiera que los estudiantes se detengan en su acceso al campus.

Mediante este sistema de control de acceso basado en reconocimiento facial, la universidad puede tener un historial de los ingresos a las residencias e identificar a los visitantes no autorizados que necesitan registrarse. Por otro lado, la escuela de desarrollo infantil de la Universidad de Seattle y la academia católica St. Therese utilizan un sistema de control de acceso basado en reconocimiento facial llamado SAFR[2] donde el personal debe sonreír a la cámara para que el sistema les permita el acceso abriendo automáticamente la puerta de entrada, de lo contrario, deben pasar a una oficina a registrarse. Así mismo, este sistema se utiliza para monitorear pasillos y áreas comunes permitiendo activar alertas de sonido, envío de mensajes y llamar a la policía en caso que así lo requieran [10].

En China, la Universidad Normal de Beijing hace uso de sistemas de reconocimiento facial en todos los dormitorios para el control de acceso donde los estudiantes tienen tres opciones para activar el sistema de reconocimiento facial como pasar su credencial

[1] https://iomni.ai/
[2] https://es.safr.com/

(ID) del campus, decir su nombre o ingresar los últimos cuatro dígitos de la contraseña de su credencial para que se les permita el acceso al edificio de dormitorios [11]. Así mismo, la Universidad de Pekín en China desarrolló un sistema de reconocimiento facial para identificar tanto a estudiantes como personal académico y administrativo cuando ingresan al campus.

En este caso, la universidad acondicionó el acceso instalando torniquetes electrónicos con lectores de credencial y tabletas con cámaras incorporadas para que el estudiante o el personal tengan la opción de ingresar a la institución por medio de su credencial o por medio del sistema de reconocimiento facial [12]. De esta manera, el control de acceso en instituciones educativas mediante reconocimiento facial se está considerando como una herramienta tecnológica que ofrece una solución eficiente, precisa, de acceso rápido e imparcial ayudando a las instituciones a mejorar la seguridad del campus permitiendo el acceso a solo personas autorizadas.

Sin embargo, implementar de forma eficiente este tipo de sistemas a gran escala es desafiante y representa un costo que muchas veces las instituciones educativas no pueden costear [13]. Es por ello, que este documento describe el desarrollo de una plataforma digital para el control de acceso por medio de reconocimiento facial basado en aprendizaje profundo que permita identificar personas autorizadas y no autorizadas en los diferentes puntos de entrada/salida de una institución educativa utilizando librerías de código abierto como OpenFace [14].

El resto del artículo está organizado como sigue. En la Sección 2, se describe el problema de reconocimiento facial basado en aprendizaje profundo. En la Sección 3 se presenta el diseño e implementación de la plataforma digital. La Sección 4 presenta la experimentación y resultados obtenidos. Finalmente, las conclusiones y trabajo futuro son presentados en la Sección 5.

2. Reconocimiento facial basado en aprendizaje profundo

El reconocimiento facial es un problema clásico de la visión por computadora que hasta la fecha continúa siendo de gran interés para la comunidad científica, así como también para la sociedad a través de aplicaciones comerciales. La Figura 1 presenta el proceso que se sigue para llevar a cabo el reconocimiento facial de forma automatizada de tal forma que primero es necesario que el sistema reciba como entrada una imagen (offline/online); posteriormente, se lleva a cabo el proceso de detección y alineación del rostro para que inicie el proceso de extracción de características y a su vez, el sistema compare mediante el proceso de correspondencia/clasificador, las características extraídas de la imagen de entrada con el conjunto de características de los rostros que se encuentran en la base de datos. Finalmente, se evalúa el rendimiento del algoritmo mediante diferentes métricas y se muestra la imagen con los datos de la persona que ha sido reconocida.

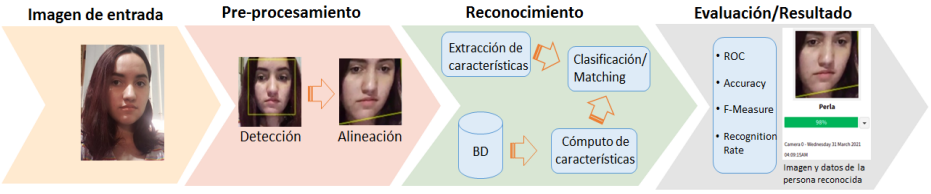

Fig. 1. Esquema tradicional del reconocimiento facial.

Los algoritmos de reconocimiento facial utilizados en aplicaciones reales hacen uso de cámaras donde las imágenes pueden tener variaciones como cambios de iluminación, baja resolución, movimientos del rostro, oclusiones, difuminación en la calidad de la imagen, entre otros. Es por ello que la mayoría de los sistemas de reconocimiento facial trabajan adecuadamente en entornos controlados como el de la iluminación y un posicionamiento frontal del rostro.

En este tipo de variaciones, los algoritmos descriptivos han mostrado ser eficaces. Algunas de las técnicas descriptivas más populares se encuentran SIFT [15], LBP [16] y HOG [17]. Pérez y Olague propusieron operadores descriptivos evolucionados llamados $RDGP_2$ que mejoraron en un 26.7% el rendimiento de los algoritmos de reconocimiento de objetos por imágenes de SIFT, SURF y GLOH [18]. Es por ello, que existe un interés en abordar el reconocimiento facial bajo este tipo de condiciones llamadas no restrictivas en donde el uso de técnicas de aprendizaje profundo ha ganado popularidad ya que ofrece mayor robustez contra las diferentes variaciones que pueden afectar el proceso de reconocimiento [19].

En ese sentido, las técnicas descriptivas han sido utilizadas en algoritmos de aprendizaje profundo como las redes neuronales convolutivas en un entorno de IoT [13,20-21], demostrando recientemente una mejora significativa en la precisión del reconocimiento facial, como por ejemplo el algoritmo DeepFace de Facebook [22], el FaceNet de Google [23], COCOLoss [24] y ArcFace [25]. En este trabajo, se utilizó la versión de código abierto de FaceNet llamada OpenFace [14] para llevar a cabo el proceso de reconocimiento facial bajo un enfoque de aprendizaje profundo.

OpenFace es uno de los algoritmos de reconocimiento facial de código abierto más preciso que combina la técnica Triplet Loss de Deepface [22] con una red neuronal convolucional profunda basada en la red de FaceNet [23]. Openface se entrenó con 500k imágenes combinando dos bases de datos utilizadas para reconocimiento facial, CASIA-WebFace [26] y FaceScrub [27] obteniendo un modelo de red llamado *nn4.small2* con un menor número de parámetros para la base de datos utilizada. Para la etapa de detección del rostro se puede utilizar HOG (Histogram of Oriented Gradient) y SVM (Support Vector Machine) de DLib, o bien, Haar cascade de OpenCV.

De acuerdo con Amos et. al. [14], HOG y SVM obtienen mejor precisión que el detector de OpenCV en la etapa de detección. Una vez que el modelo de red es obtenido y se obtienen las características de los rostros, se utilizan técnicas de clasificación para completar la tarea de reconocimiento. Finalmente, para evaluar el rendimiento de OpenFace, Amos et. al. utilizaron la base de datos LFW [28] con el modelo de red *nn4.small2.v1* obteniendo una precisión de 0.9292± 0.0134.

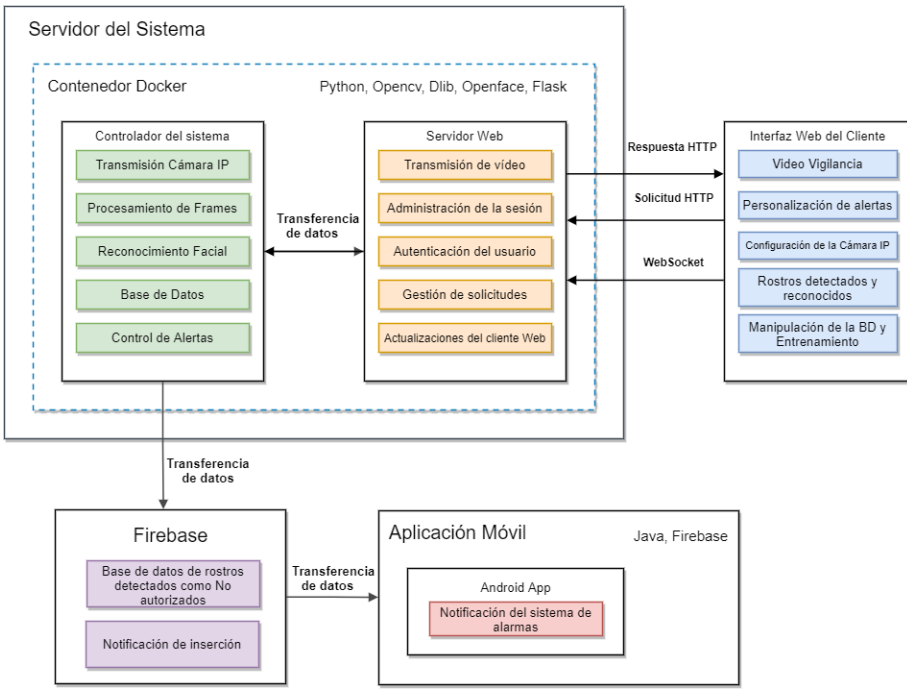

Fig. 2. Diseño de la arquitectura de la plataforma para el control de acceso universitario.

La etapa de clasificación permite que el sistema pueda identificar quién es quién no solamente saber si la persona se encuentra o se parece a alguien almacenada en la base datos. En ese sentido, existen diferentes clasificadores que han sido utilizados en el reconocimiento facial como la máquina de vectores de soporte (SVM, por sus siglas en inglés), Naive Bayes y Árboles de decisión (Decision Trees) por mencionar algunos.

El algoritmo SVM, es un algoritmo de aprendizaje supervisado que se utiliza en problemas de clasificación; éste encuentra los parámetros óptimos de un hiperplano separador que maximiza el margen entre los objetos de entrenamiento. Se utiliza el truco del kernel, que consiste en mapear las entradas, que no son linealmente separables en el espacio de entrada, a un espacio de alta dimensión. El kernel lineal entre dos objetos $\boldsymbol{x}$ y $\boldsymbol{x}'$ se define como $Klineal = \boldsymbol{x} \cdot \boldsymbol{x}'$, mientras que el kernel radial, o Gaussiano, se define como $Kradial = e\text{^}(-(\|x - x\text{^}' \|\text{^}2/(2\sigma\text{^}2))$). Adicionalmente, para incluir regularización, se agrega el parámetro C en el proceso de optimización [30].

El algoritmo probabilístico de clasificación Bayes ingenuo o *Naive Bayes* en inglés, se basa en el teorema de Bayes y supone que las características de los objetos son independientes. En la etapa de entrenamiento, se calculan las probabilidades a *priori* y se encuentran los parámetros que maximizan la verosimilitud dadas las características obtenidas para los objetos de cada clase. Se obtiene la probabilidad *posteriori* de que un objeto evaluado pertenece a una clase con base a sus características [31]. Por otro lado, los modelos de árboles de decisión para clasificación consisten en un conjunto de

reglas para estratificar el espacio de predicción en subgrupos más pequeños y homogéneos [32].

3. Descripción de la plataforma digital

En esta sección, presentamos la descripción de la plataforma digital para el control de acceso en un campus universitario mediante reconocimiento facial. El objetivo es detectar a las personas autorizadas/no autorizadas que desean ingresar al campus de forma automática por medio de reconocimiento facial.

Cuando una persona no autorizada desea entrar a la institución, se manda automáticamente una alerta a una aplicación móvil diseñada para los guardias de seguridad del campus quienes están capacitados para tomar la acción correspondiente; por ejemplo, tomar sus datos y permitirle la entrada temporalmente, registrarlo en el sistema, o bien, no permitirle la entrada.

El diseño de la plataforma se basó en la propuesta de Brandon Joffe [29], en donde considera un servidor dedicado al procesamiento de reconocimiento facial. Para ello, se usa una comunicación basada en web que permite la interacción con el usuario y manipulación de la plataforma. Adicionalmente, se desarrolló una aplicación móvil para el manejo de alertas, la cual se comunica con el servidor central por medio de Firebase[3], obteniendo de esta manera, información sobre el proceso de reconocimiento facial que se enviará como alerta a la aplicación móvil, ver Figura 2.

La plataforma está diseñada para establecer comunicación con cámaras IP por medio de las cuales se obtendrá el rostro de las personas. Una vez que se obtiene la información de la(s) cámara(s) se procede a realizar el proceso de reconocimiento y automáticamente se envía la alerta a la aplicación móvil cuando se identifica una persona no autorizada por la institución, ver Figura 3. En este caso, el objeto IPCamera transmite el video directamente desde una cámara IP para que sea procesado y transmitirlo al cliente web.

Cada cámara tiene su propio objeto MotionDetector y FaceDetector que son utilizados por otros procesos para llevar a cabo el reconocimiento facial. En ese sentido, el proceso de reconocimiento está basado en el algoritmo OpenFace usando el modelo de red neuronal pre-entrenado *nn4.small2.v1.t7* y el clasificador LinearSVM.

4. Experimentación y resultados

Esta sección describe la experimentación llevada a cabo para la etapa de clasificación del proceso de reconocimiento facial descrito en la Sección 2 y se presenta la implementación de una plataforma digital.

3 https://firebase.google.com/

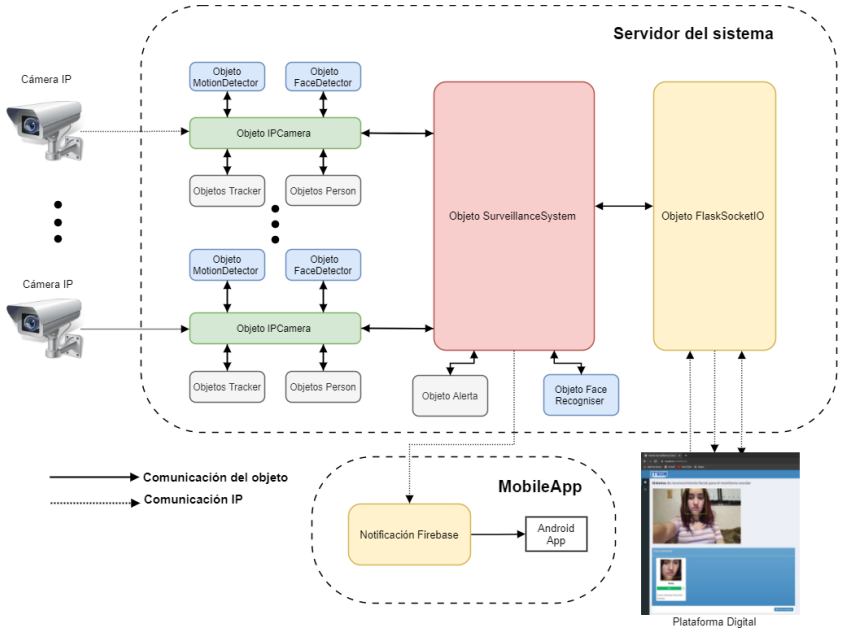

Fig. 3. Funcionamiento de la plataforma para el control de acceso y envío de alertas.

4.1. Clasificación de características para el reconocimiento facial

Para llevar a cabo la comparación de clasificadores se utilizó una computadora Lenovo, Intel Core i5 con 8GB de RAM y sistema operativo Linux Ubuntu kernel 5.3.0-40. En ese sentido, para los experimentos se utilizó la base de datos LFW [28] la cual es ampliamente utilizada en el reconocimiento facial. Esta base de datos cuenta con 5749 clases (personas) y 13233 fotos.

Se observó que la mayoría de las clases cuentan con una sola foto lo cual para este tipo de experimentación es insuficiente. 5591 clases tienen entre 1 y 10 fotos; 96 clases tienen entre 10 y 20 fotos; 28 clases tienen entre 20 y 30 fotos; 15 clases tienen entre 30 y 40 fotos; 7 clases tienen entre 40 y 50; 4 clases tienen entre 50 y 60 fotos y el resto de clases más de 60 fotos por clase.

Considerando esto, se decidió utilizar el grupo de 28 clases que contiene un total de 653 fotos y el grupo de 4 clases que contiene un total de 212 fotos. Los resultados de este experimento se pueden observar en las Figuras 4 y 5.

Para llevar a cabo el entrenamiento y la prueba de cada uno de los clasificadores, se dividió la base de datos en un 80% para entrenamiento y un 20% para pruebas para cada uno de los grupos (28 y 4 clases). Como se puede observar en la Tabla 1, LinearSVM y GaussianNB son mejores que RadialSVM y DecisionTrees en ambos grupos de clases. Es por ello, que se decidió utilizar LinearSVM como clasificador en el proceso de reconocimiento facial.

Adicionalmente, se evaluó el sistema de reconocimiento de la plataforma utilizando una base de datos de la institución con 91 fotos de 3 estudiantes y 1 profesor (4 clases)

Tabla 1. Comparación del rendimiento de 4 clasificadores utilizados en el reconocimiento facial sobre la base de datos LFW.

Clasificador	28 clases		4 clases	
	% Reconocimiento	F-Measure	% Reconocimiento	F-Measure
LinearSVM	96.15	0.9804	100	1
RadialSVM	95.38	0.9764	100	1
DecisionTrees	70.77	0.8288	92.86	0.96295
GaussianNB	96.15	0.9804	100	1

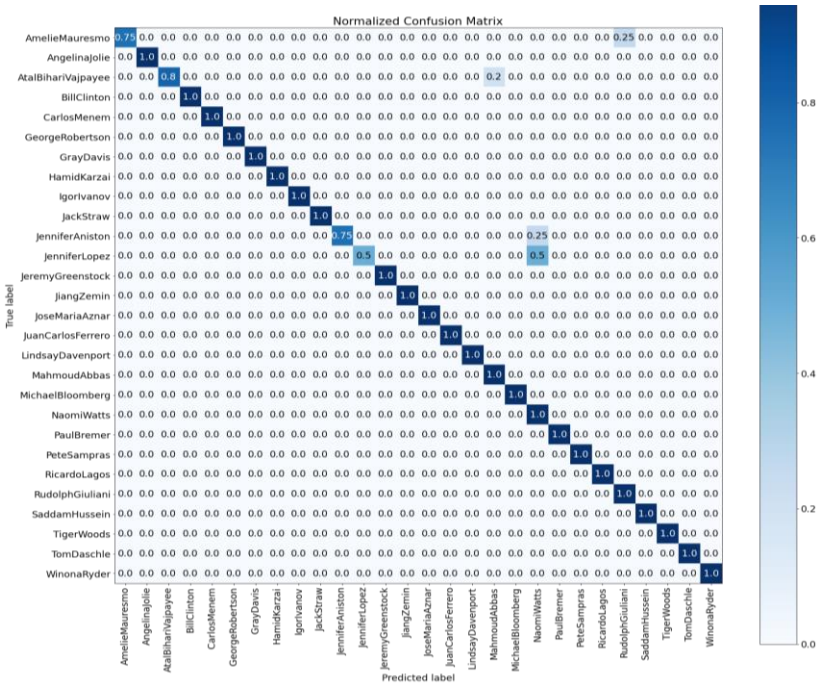

Fig. 4. Matriz de confusión normalizada para 28 clases de la base de datos LFW [28] utilizando Linear SVM.

obteniendo como resultado un porcentaje de reconocimiento del 95.24% y una F-Measure de 0.9978, ver Figura 6.

4.2. Plataforma digital para el control de acceso universitario

La plataforma se implementó en una computadora Lenovo, Intel Core i5 con 8GB de RAM y sistema operativo Linux Ubuntu kernel 5.3.0-40 y se utilizó la aplicación IP WebCam en un teléfono móvil con sistema operativo Android para usar la cámara del

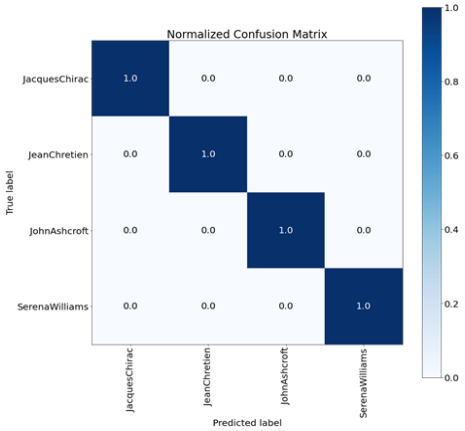

Fig. 5. Matriz de confusión normalizada para 4 clases de la base de datos LFW [28] utilizando LinearSVM.

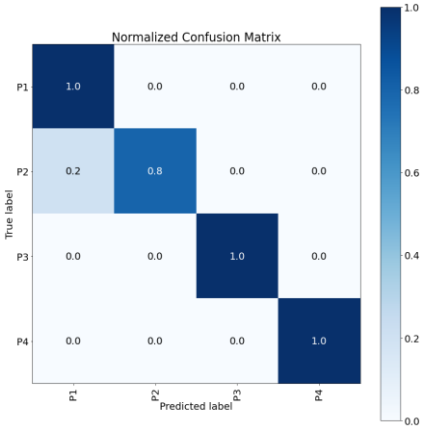

Fig. 6. Matriz de confusión normalizada utilizando la base de datos de la Institución (4 clases).

teléfono como una cámara IP. En el caso de la aplicación móvil, ésta fue desarrollada con Java en Android Studio en un Huawei Nova 3 y probada en un Samsung S9.

Por otro lado, la plataforma cuenta con la opción de agregar personas al sistema en tiempo real. Si esto sucede, se debe de re-entrenar el clasificador en la misma plataforma para que la persona sea reconocida como persona autorizada en el futuro.

En ese sentido, la Figura 7 presenta un ejemplo de la plataforma mostrando una persona autorizada por el sistema, en donde se despliegan datos como nombre de la persona y el porcentaje de confianza indicando con ello, la certeza del reconocimiento

Por otro lado, la Figura 8 presenta un ejemplo de la plataforma cuando una persona no autorizada se detecta, si esto sucede, se envía automáticamente una alerta a la aplicación móvil, ver Figura 9b. De lo contrario, cuando el sistema reconoce a una persona autorizada la aplicación móvil se presenta sin cambios, ver Figura 9a.

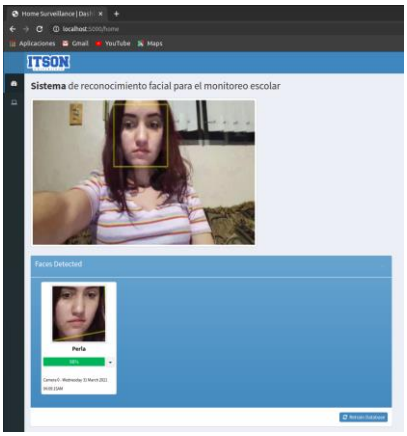

Fig. 7. Ejemplo de la plataforma reconociendo a una persona autorizada por el sistema.

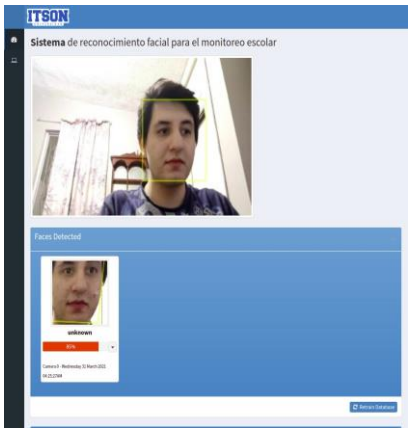

Fig. 8. Ejemplo de la plataforma mostrando a una persona NO autorizada.

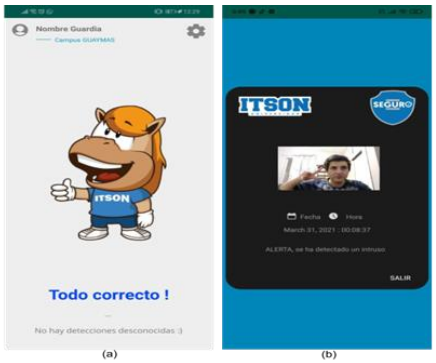

Fig. 9. Alerta enviada de la plataforma a la aplicación móvil. (a) Persona autorizada (b)

5. Conclusiones y trabajo futuro

Este trabajo presenta el diseño e implementación de una plataforma digital para el control de acceso del personal académico, administrativo y estudiantil a un campus universitario mediante reconocimiento facial. La plataforma digital fue implementada en un equipo local, sin embargo, se tiene programado migrarla a un servidor institucional con cuatro cámaras IP HikVision H.265+ instaladas en los accesos de entrada al campus.

Esta plataforma permite ingresar nuevas personas al sistema y cuenta con el envío de alertas a una aplicación móvil de forma automática cuando una persona no autorizada intenta ingresar a la institución. Para la etapa de reconocimiento facial se utilizó el algoritmo de código abierto OpenFace con el modelo de red neuronal pre-entrenado *nn4.small2.v1.t7* y el clasificador LinearSVM.

Para esto, se presenta una comparación de 4 clasificadores utilizando la base de datos LFW con 28 y 4 clases mostrando un rendimiento superior al 95%. Adicionalmente, se evaluó la plataforma con 4 clases utilizando imágenes del personal académico y estudiantil mostrando un porcentaje de reconocimiento del 95.24% y un valor de F-Measure de 0.9978.

En ese sentido, como trabajo futuro se tiene pensado implementar la plataforma digital *in situ*, y para ello será necesario preparar una base de datos institucional y proponer un esquema de reconocimiento a gran escala ya que la institución cuenta con alrededor de 21,818 estudiantes y 2,820 trabajadores, lo que representa alrededor de 24,638 clases para el sistema de reconocimiento facial.

Agradecimientos. Este trabajo fue financiado por el programa para el desarrollo profesional docente (PRODEP) 2019.

Referencias

1. INEGI. Departamento de comunicación social. Encuesta Nacional de Seguridad Pública Urbana (ENSU) México. https://www.inegi.org.mx/contenidos/saladeprensa/boletines/2020/ensu/ ensu2020_10.pdf (2021)
2. Gonzalez-Garcia, C., Meana-Llorián, D., Pelayo G-Bustelo, B. C., Cueva-Lovelle, J. M., Garcia-Fernandez, N.: Midgar Detection of people through computer vision in the internet of things scenarios to improve the security in Smart Cities, Smart Towns, and Smart Homes. Future Generation Computer Systems, Elsevier, vol. 76, pp. 301–313 (2017) doi: 10.1016/j.future.20 16.12.033
3. Dong, X., Kong, X., Zhang, F., Chen, Z., Kang, J.: On campus a mobile platform towards a smart campus. SpringerPlus, pp. 1–9 (2016) doi: 10.1186/s40064-016-2608- 4
4. Kumar, P. M., Gandhi, U., Varatharajan, R., Manogaran, G., Jidhesh, R., Vadivel, T.: Intelligent face recognition and navigation system using neural learning for smart security in internet of things. Cluster Computing, no. 22, pp. 7733–7744 (2019) doi: 10.1007/s10586-017-1323-4
5. Rameswari, R., Kumar, S. N., Aananth, M. A., Deepak, C.: Automated access control system using face recognition. Materials Today Proceedings. vol. 45, pp. 1251–1256 (2020) doi: 10.1016/j.matpr.2020.04.664
6. Lee, H., Park, S. H., Yoo, J. H., Jung, S. H., Huh, J. H.: Face recognition at a distance for a stand-alone access control system. Sensors, vol. 20, pp. 1–18 (2020) doi: 10.3390/s20030785
7. Tisse, C. L., Martin, L., Torres, L., Robert, M.: Person identification technique using human iris recognition. In: Proceedings of. Vision Interface Canadian Image Processing and Pattern Recognition Society (CIPPRS), 15th International Conference on Vision Interface. pp. 294–299 (2002)
8. Bueno-Delgado, M. V., Pavón-Marino, P., De-Gea-Garcia, A., Dolon-Garcia, A.: The smart university experience: An NFC-based ubiquitous environment. In: Proceedings of the IEEE International Conference on Innovative Mobile and Internet Services in Ubiquitous Computing, pp. 799–804 (2012) doi: 10.1109/IMIS.2012.110
9. Skinner, V.: Universitiy of San Francisco using facial recognition to track dorm activity. EAG. News.org (2014). https://www.eagnews.org/2014/11/university-of-san-francisco-using-facial-recognition-to-track-dorm-activity/

10. Mikkelsen, D.: Two Seattle schools among first to use facial recognition software in the US. K5 News (2018). https://www.king5.com/article/news/education/two-seattle-schools-amongfirst-to-use-facial-recognition-software-in-us/281-609937626
11. Xiaofei, Du.: Facial recognition system introduced to Beiging Normal University dorms. People's Daily Online (2017) http://en.people.cn/n3/2017/0516/c90000-9216437.html
12. Gan, N.: Want to get into Peking University? Just show your face. Inkstone news (2018). https://www.inkstonenews.com/tech/peking-university-installs-facial-recognition-system-students-and-staff-campus-gate/article/2152893
13. Oh, S. H., Kim, G. W., Lim, K. S.: Compact deep learned feature-based face recognition for visual internet of things. The Journal of Supercomputing, vol. 74, pp. 6729–6741 (2018) doi: 10.1007/s11227-017-2198-0
14. Amos, B., Ludwiczuk, B., Satyanarayanan, M.: Openface: A general-purpose face recognition library with mobile applications. Technical Report, CMU-CS-16-118, CMU School of Computer Science (2016)
15. Lowe, D.: Distinctive image features from scale-invariant keypoints. International Journal of Computer Vision, vol. 60, pp. 91–110 (2004) doi: 10.1023/B:VISI.0000029664.99615.94
16. Ahonen, T., Hadid, A., Pietikainen, M.: Face description with local binary patterns: Application to face recognition. IEEE Transactions on Pattern Analysis & Machine Intelligence, vol. 28, pp. 2037–2041 (2006) doi: 10.1109/TPAMI.2006.244
17. Déniz, O., Bueno, G., Salido, J., De la Torre, F.: Face recognition using histograms of oriented gradients. Pattern Recognition Letters, vol. 32, pp. 1598–1603 (2011) doi: 10.1016/j.patrec.2 011.01.004
18. Perez, C. B., Olague, G.: Learning invariant region descriptor operators with genetic programming and the f-measure. In: Proceedings of the 19th International Conference on Pattern Recognition, pp. 1–4 (2008) doi: 10.1109/ICPR.2008.4761178
19. Guo, G., Zhang, N.: A survey on deep learning based face recognition. Computer vision and image understanding, 189, pp-1–47 (2019) doi:10.1016/j.cviu.2019.102805
20. Yang, S., Luo, P., Loy, C. C., Tang, X.: From facial parts responses to face detection: A deep learning approach. In: Proceedings of the IEEE International Conference on Computer Vision, pp. 3676–3684 (2015)
21. Farfade, S. S., Saberian, M. J., Li, L. J.: Multi-view face detection using deep convolutional neural networks. In: Proceedings of the 5th ACM on International Conference on Multimedia Retrieval, pp. 643–650 (2015) doi: 10.1145/2671188.2749408
22. Parkhi, O. Vedaldi, M., Zisserman A.: Deep face recognition. In British Machine Vision Conference, pp. 1–12 (2015)
23. Schroff, F., Kalenichenko, D., Philbin, J.: Facenet A unified embedding for face recognition and clustering. In: Proceedings of the IEEE conference on computer vision and pattern recognition, pp. 815–823 (2015)
24. Liu, Y., Li, H., Wang, X.: Rethinking feature discrimination and polymerization for large-scale recognition. arXiv preprint arXiv (2017) doi: 10.48550/arXiv.1710.00870
25. Deng, J., Guo, J., Xue, N., Zafeiriou, Arcface S.: Additive angular margin loss for deep face recognition. In: Proceedings of the IEEE/CVF Conference on Computer Vision and Pattern Recognition, pp. 4690–4699 (2019)
26. Yi, D., Lei, Z., Liao, S., Li, Stan. Z.: Learning face representation from scratch arXiv preprint arXiv. (2014) doi: 10.48550/arXiv.1411.7923
27. Ng. H. W., Stefan, W.: A data-driven approach to cleaning large face datasets. IEEE International Conference on Image Processing, pp. 343–347 (2014) doi: 10.1109/ICIP.2014.7025068
28. Huang, G., B., Mattar, M., Berg, T., Learned-Miller, E.: Labeled Faces in the Wild A database for studying face recognition in unconstrained environments. Workshop on Faces in 'Real-Life' Images: Detection, Alignment, and Recognition, Erik Learned-Miller and Andras Ferencz and Frédéric Jurie (2008)

29. Joffe, B.: Home Surveillance with facial recognition. https://github.com/BrandonJoffe/home_ surveillance#features
30. Muller, K. R., Mika, S., Ratsch, G., Tsuda, K., Scholkopf, B.: An introduction to kernel-based learning algorithms. IEEE transactions on neural networks, pp. 181–201 (2001)
31. Duda, R. O., Hart, P. E., Stork, D. G.: Pattern Classification, 2nd edition, Jhon Wiley & Sons, Inc (2001)
32. James, G., Witten, D., Hastie, T., Tibshirani, R.: An introduction to statistical learning. Ed. Springer, 112, pp. 3–7 (2013) doi: 10.1007/978-1-0716-1418-1.pdf