ANÁLISIS DEL RECONOCIMIENTO FACIAL COMO MEDIDA DE CONTROL DE ACCESO Y SEGURIDAD

Analysis of facial recognition as a measure of access control and security

Mauricio Murillo Cortes[1]
Mauricio.murillo04@usc.edu.co

Julio Cesar Burgos[1]
julio.burgos00@usc.edu.co

Universidad Santiago de Cali, Facultad de Ingeniería, Programa de tecnología en sistemas de información (1)

Resumen
El presente trabajo consiste en el análisis de una de las técnicas de la biometría basadas en el reconocimiento facial, utilizando la visión artificial por computadora, Analizando las bibliotecas que ofrece Python, los algoritmos de clasificadores de cascada como Haar Cascade y LBPH (Local Binary Pattern Histogram), Los cuales se compararon con EigenFaces y FisherFaces obteniendo mejores resultados de reconocimiento con LBPH. Se analiza el proceso de reconocimiento en tres etapas, iniciando por la detección de rostro siendo esta la más importante del reconocimiento facial, seguido la etapa de entrenamiento y finalmente la etapa de reconocimiento facial. Todo este proceso se lleva a cabo de forma simultáneamente y requiere de una cantidad entre (10 y 150) rostros para lograr su propósito final, el cual es identificar si el rostro que está frente a la cámara es reconocido exitosamente como miembro de una entidad o desconocido en cuestión de segundos y de este modo poder tener un registro de control de acceso y seguridad gracias a las técnicas de biometría que brinda el reconocimiento facial haciendo uso de la biblioteca de OpenCV.

Palabras Clave: Reconocimiento facial; Detección de rostro; Entrenador facial; Open CV; LBPH; Haar Cascade; FisherFaces.

Abstract
This paper incorporates the analysis of one of the biometric techniques, based on the facial recognition, using the computerized artificial vision, analyzing the library offered by Python, and the cascade classifier algorithms like Haar Cascade and LBPH, which were compared to EigenFaces and FisherFaces, obtaining a better result with LBPH. The analysis is made within three stages, starting with the face detection, being the most important one, followed by the training stage and ending with the facial recognition by itself. This whole process is carried simultaneously and requires between 10 to 150 faces to achieve its purpose, which is to successfully identify if the face in front of the camera is a known member or a stranger within seconds, and so being able to keep a record of controlled access and security, thanks to the biometric techniques offered by facial recognition, using the OpenCV library.

Keywords: Facial recognition; Face detection; Facial trainer; Open CV; LBPH; Haar Cascade; Fisherfaces.

I. INTRODUCCIÓN

El reconocimiento facial ha sido un área de investigación que ha llamado mucho la atención durante las últimas décadas. Trabajos anteriores centrados en esta tarea han logrado grandes avances en términos de precisión de reconocimiento. Sin embargo, todavía existen desafíos importantes en entornos sin restricciones, donde el rendimiento de reconocimiento de los métodos existentes se ve afectado negativamente por las condiciones de iluminación variables, la variación de pose y la imagen borrosa (Zhao, Li, and Dong 2020).

Un sistema de reconocimiento facial funciona identificando y verificando a una persona a partir de una imagen digital o una secuencia de fotogramas de una fuente de video (Leong et al. 2020), los sistemas de reconocimiento facial buscan automatizar un proceso que se lleva de forma manual la percepción de rostros es una tarea realizada con éxito y casi sin esfuerzo por los humanos, pero no es una tarea muy fácil para las computadoras. El sistema visual humano acomoda caminos neuronales complejos para el procesamiento de características estáticas y dinámicas de los rostros para reconocer rostros en relación con el conocimiento contextual (Taskiran, Kahraman, and Erdem 2020). Todo esto conlleva a una

realización de algoritmos basado en un lenguaje de programación el cual permite realizar la identificación de los rostros de tal manera que pueda ofrecer un menor tiempo de respuesta para dar una solución a un inconveniente.

Las técnicas de reconocimiento facial de alto rendimiento en la actualidad se basan en redes neuronales convolucionales. Los sistemas DeepFace de Facebook y FaceNet de Google ofrecen la mayor precisión. Sin embargo, en el pasado, estas técnicas basadas en redes neuronales profundas se entrenaron con conjuntos de datos privados que contienen millones de imágenes de redes sociales que son órdenes de magnitud más grandes que los conjuntos de datos disponibles para la investigación.

Una red neuronal convolucional es una red neuronal artificial está formada por un conjunto de neuronas interconectadas y arregladas en forma de capas, las cuales están compuestas a su vez por un número de neuronas cada una. Existen capas de entrada (por donde se ingresan los datos), capas de salida (por donde se obtienen los resultados) y las capas ocultas (por donde pasan los datos).

Los procedimientos únicos de identificación y correspondencia de usuarios siguen siendo desafíos clave para brindar atención de alta calidad (Ampamya, Kitayimbwa, and Were 2020).

La ejecución de un sistema de reconocimiento facial típico sigue en general tres pasos, (1) detección y extracción de rostro, (2) Extracción y representación de características y (3) reconocimiento de rostro. La detección de rostros comienza confirmando la presencia de un rostro en una imagen determinada. El siguiente paso es encontrar la ubicación de la cara en esa imagen y segmentar la región de interés. La representación de la cara segmentada se realiza mediante un vector de características adecuado que resalta las características únicas de la cara (Jayaraman et al. 2020).

Actualmente existen diferentes algoritmos para el reconocimiento facial como, por ejemplo: Fisherfaces, LBPH (Local Binary Patterns Histograms) y Eigenfaces. Estos métodos de reconocimiento facial en esencia comparan la imagen facial de entrada con todas las imágenes faciales almacenadas con el objetivo de encontrar al usuario que coincida con el rostro. Cada método tiene un enfoque diferente para extraer la información de entrada, pero finalmente se obtiene el mismo resultado el cual identifica el usuario.

La problemática radica en que las técnicas usadas tradicionalmente para la identificación donde se utilizan varios métodos como usuario y contraseña, carnet, número de identificación siendo estos métodos fáciles de olvidar, compartir, perder o robar.

El objetivo de nuestro estudio es revisar diferentes técnicas para realizar el reconocimiento facial como mecanismo biométrico para control de acceso, analizando bibliotecas de Python, Haar Cascade, Open CV y aplicando características de histogramas de patrones locales binarios LBPH y fisherface.

II. RECONOCIMIENTO FACIAL

El reconocimiento facial tiene muchas aplicaciones en los campos del procesamiento de imágenes y la visión por computadora. Los avances en tecnologías relacionadas permiten su integración eficiente y precisa en muchas áreas, desde el reconocimiento facial individual para desbloquear un dispositivo móvil hasta la vigilancia de multitudes (Chamikara et al. 2020). Incluso para automatizar procesos antiguos como la muestra de una identificación para acceder a un sitio.

Por otro lado, el reconocimiento facial es uno de los temas de investigación más antiguos pero dinámicos, es necesario para aplicaciones de seguridad y biométricas. Los primeros sistemas de reconocimiento facial se basaban en funciones manuales y clasificadores tradicionales. Algunas características hechas a mano incluyen patrón binario local (LBP), descriptores locales de Weber (WLD), análisis de componentes principales (PCA) e histograma de gradientes orientados (HOG) (Masud et al. 2020).

Teniendo en cuenta que un sistema biométrico es esencialmente un sistema de reconocimiento de patrones que utiliza datos biométricos de individuos. Dependiendo del contexto de la aplicación, un sistema biométrico puede operar en el modo de aprendizaje, modo de verificación o modo de identificación. La elección de utilizar el reconocimiento facial como modalidad biométrica está motivada por el hecho de que es sin contacto, natural, bien aceptado y requiere solo un sensor muy económico (Webcam) que está prácticamente disponible en todos los dispositivos electrónicos. Además, requiere una pequeña cooperación de los usuarios durante la fase de adquisición de los rasgos faciales (Hamdan and Mokhtar 2018).

Los principales desafíos para los sistemas exitosos de detección y reconocimiento de rostros son; condiciones de iluminación, escala, oclusión, pose, fondo, expresión, etc. (Bah and Ming 2020). Otro gran desafío que se ha generado con la implementación de estos sistemas es la forma de cómo se puede vulnerar en muchos casos lo realizan con una foto de la persona incluso con una máscara modelada en 3d con los rasgos del rostro de una persona que tiene acceso y es identificada por el sistema.

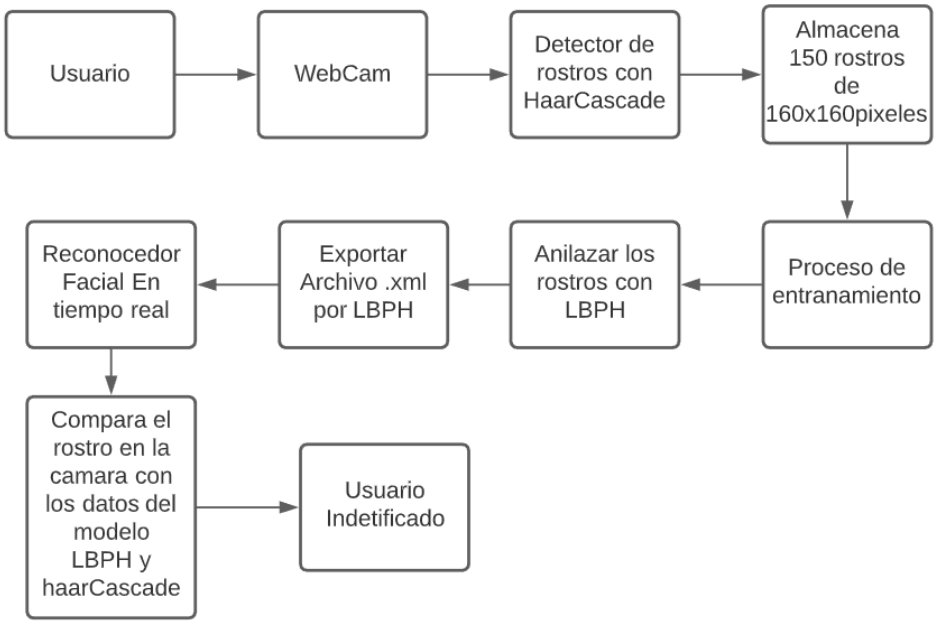
Tabla 1. Áreas de aplicación de los métodos de reconocimiento facial.

Áreas de aplicación	Aplicaciones especificas
Seguridad, salud	Seguridad de la información, autenticación de usuarios.
	Iniciar sesión en dispositivos electrónicos
	Interacción de robot humano, acceso a edificios.
	Reconocer rostros de videos de vigilancia
	Aplicaciones relacionadas con la salud: hogares inteligentes, automóviles inteligentes
	Asistentes robóticos.
Cumplimiento de la ley	Monitoreo fronterizo, análisis de eventos ilegales, rastreo de sospechosos.
	Pasaportes, tarjetas de identificación nacionales, licencias de conducir.
	Inmigración.
Entretenimiento, educación, marketing	Juegos, realidad virtual.
	Gestión de fotografías.
	Análisis de video, recuperación de video.
	Aprendizaje en línea, seguimiento de los estudiantes, participación de los usuarios.
	Campañas publicitarias, moderación de redes sociales.

Fuente: Adaptado de (Taskiran et al. 2020)

A continuación, en la Figura 1 podemos ver el proceso que se lleva a cabo para que el reconocedor facial funcione con éxito identificando el usuario.

Figura 1 Proceso del reconocimiento facial



Fuente: Elaboración propia

III. DETECCIÓN DE ROSTRO

La detección de rostros es un paso importante en el reconocimiento de rostros que corresponde a la localización del rostro en una imagen determinada. Una vez que se detecta la cara, se recorta para su reconocimiento (Jayaraman et al. 2020).

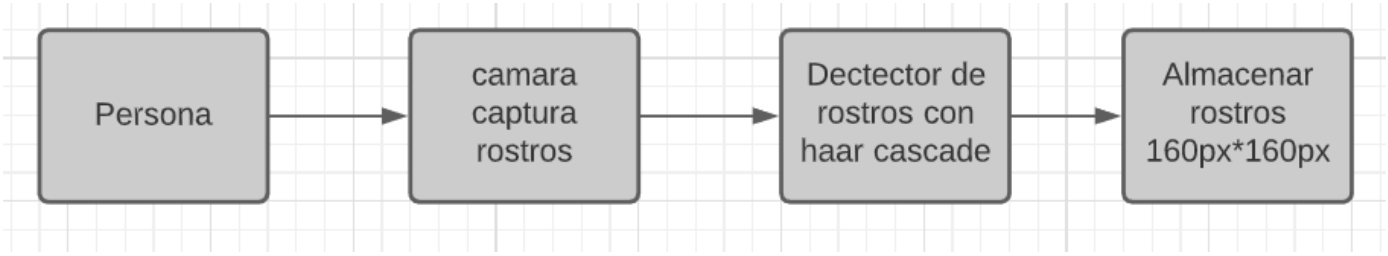
Para aplicaciones en la detección de personas se utilizan los clasificadores cascada de haar, de distribución y uso libre desarrolladas por OpenCV quienes implementan los métodos correspondientes. La biblioteca proporciona una gran variedad de clasificadores para detectar (extensión *.xml), por ejemplo:

- Rostro: "haarcascade_frontalface_alt_tree" y "haarcascade_frontalface_alt".

En este proyecto se utiliza: "haarcascade_frontalface_default.xml" para hacer la detección del rostro (Caballero Julián et al. 2016).

En la realización de este proceso se usan clasificadores en cascada (haar cascade) que permite detectar si hay un rostro al frente de la cámara o una imagen encerrando solo la parte del rostro en un rectángulo, una vez detectados los rostros se almacenan con un tamaño de 160 pixeles X 160 Pixeles

Figura 2. Proceso de detención de rostro



Fuente: Elaboración propia.

IV. ENTRENADOR FACIAL

Los procesos de reconocimiento facial están sujetos a un entrenamiento de datos los cuales son analizados y se extraen sus características guardando un archivo.xml, en esta etapa se entrena al sistema para poder reconocer un rostro posteriormente.

Para lograr un entrenamiento eficiente es necesario tener una buena cantidad de imágenes de la persona. El proceso de entrenamiento consiste en los siguientes pasos:

Lectura del cuadro de video en tiempo real.
Detección del rostro preprocesado comparación y predicción de identificación.

1. En cada imagen recogida, se detectará el rostro y se preprocesa de tal manera que de solo obtener el rostro.
2. Con las imágenes preprocesadas, se pasa a la etapa de extracción de características con los clasificadores de Haar.
3. Por último, se procede a usar el modelo LBP (Local Binary Patterns), al cual entrenamos con las imágenes y los labels. Para finalmente obtener los coeficientes de las imágenes de entrenamiento (Llapapasca Montes and Ochoa Zevallos 2019).

En el texto anterior se evidencia el entrenamiento de un proyecto que se llevó a cabo con un reconocimiento para identificación de trabajadores de una empresa, el cual lleva los mismos pasos de entrenamiento que son aplicables para el ingreso de estudiantes de la universidad al parqueadero por medio del modelo exportado por LBPH.

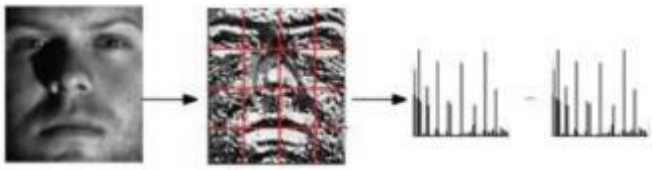
4.1 Características del proceso de entrenamiento

- En la etapa de entrenamiento se toman las imágenes capturadas con un tamaño de 160px * 160px siendo esta la medida donde abarca totalmente el rostro, con el objetivo de ahorrar espacio en el almacenamiento.
- En el proceso de entrenamiento se requieren una gran cantidad de imágenes (entre 10 y 150) para un mejor aprendizaje y obtener más características faciales.
- Analizar y dividir las imágenes en regiones para identificar qué elementos del rostro se encuentran en cada pixel y así mismo guardar en el modelo las características del rostro tales como distancia entre ojos, nariz, boca y finalmente la intensidad e iluminación de la fotografía que tiene una relación única para la identificación.
- Por ejemplo, es una mecánica similar a cuando trabajamos con identificación de personas mediante el reconocimiento de voz que tiene sus características tales como:
  - las pausas al hablar
  - los tonos altos

– los tonos bajos de la voz

Las cuales se extraen y son analizadas para llevar a cabo el proceso de verificación e identificación de la persona o de algunos elementos personales de la misma.

Figura 3 Extracción de características



Fuente: Adaptado de (Mi et al. 2020)

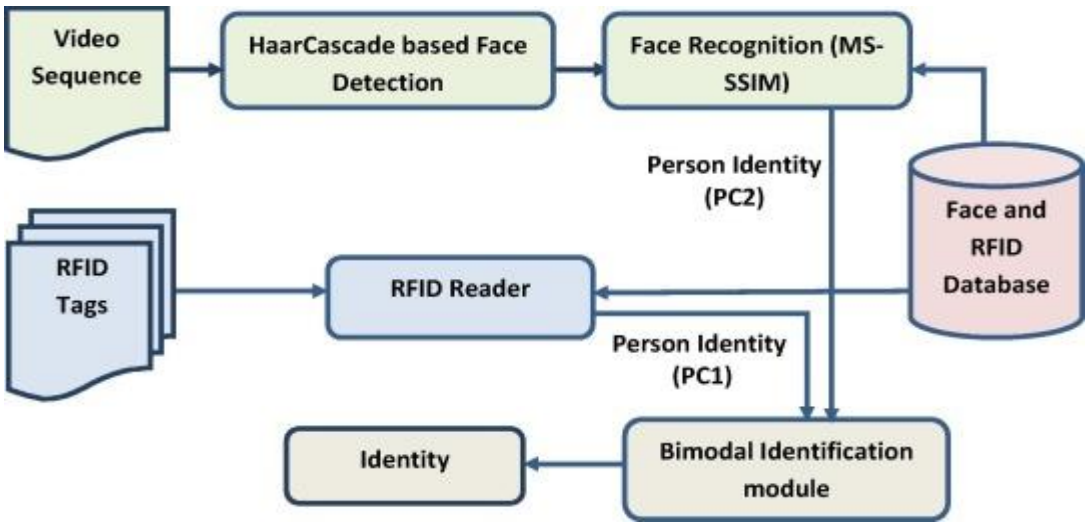
V. HAAR CASCADE

El marco de impulso en cascada de Viola y Jones es un hito en la detección de rostros. La asombrosa velocidad en tiempo real y la alta precisión de detección del detector facial se pueden atribuir a tres factores: la representación integral de la imagen, el marco en cascada y el uso de adaboost para entrenar nodos en cascada (Zhan, Tao, and Li 2016).

El mayor problema de La detección de rostros mientras se usa un clasificador en cascada de Haar es que la imagen contiene tanto simple como fondo complejo (Singh and Furtado n.d.).

En la Figura 4 se puede observar el diagrama de funcionamiento de Haar Cascade utilizado para un sistema de gestión de asistencia estudiantil multimodal (Multimodal student attendance management system (MSAMS)).

Figura 4 Identificación de personas multimodo basado en Haar Cascade.



Fuente: Adaptado de (Mohammed, Tolba, and Elmogy 2018)

En un estudio realizado para un sistema de asistencia automatizado competente basado en el reconocimiento facial y la clasificación de género usando Haar – Cascade y el método de Kanade-Lucas-Tomasi ambos utilizados en el campo de visión artificial para reconocimiento facial se ponen a prueba obteniendo gran diferencia en los resultados. Haar- Cascade & Kanade-Lucas-Tomasi. El sistema ha capturado la imagen de la entidad mientras la entidad se mueve y la cámara se coloca como cámara de vigilancia. La imagen capturada se ha categorizado como:

a) mirando al frente

b) izquierda hasta el hombro
c) derecho al hombro
d) hasta el suelo
e) hasta el suelo

Las tres primeras categorías se dividieron en cuatro subcategorías: brillante, muy brillante, oscuro y muy oscuro. Haar-cascade detectó el 87% del resultado total mientras que Kanade-Lucas-Tomasi solo detectó 45%. Se observó que Haar-cascade era capaz de detectar con éxito rostros que el algoritmo Kanade-Lucas-Tomasi no pudo. Así que está probado que el algoritmo de cascada de Haar funciona en cada escenario (Shrivastava et al. 2018).

Una cascada de Haar es generalmente un clasificador de objetos el cual necesita entre (10 y 150) imágenes positivas y negativas en este caso rostros y de tal forma entrenar al clasificador extrayendo características que se obtienen en el proceso de análisis que realiza Haar-cascade guardando valores únicos de los rostros los cuales finalmente permiten la identificación de cada rostro.

OpenCV es una biblioteca de software para visión de código abierto. Esta biblioteca ofrece muchos algoritmos optimizados, incluida la detección y el reconocimiento de rostros que se pueden utilizar en muchas áreas relacionadas con IoT.

5.1 Open CV

OpenCV es una biblioteca de software de código abierto que permite a los desarrolladores acceder a rutinas utilizadas para aplicaciones de visión por computadora en la API (Interfaz de programa de aplicación) (Zhu and Cheng 2020).

Mediante las bibliotecas que ofrece OpenCV y Python es posible realizar un aplicativo para la identificación de personas.

OpenCV es la biblioteca de visión artificial quizás una de las más importantes y utilizadas en el mundo ya que ha sido aplicada para automatizar diferentes procesos tales como:

- Reconocimiento facial
- Reconocimiento de gestos
- Reconocimiento de placas vehiculares
- Clasificador y reconocimiento de objetos
- Detección de movimiento (Tracking)
- Escáner de documentos
- Robótica y la realidad aumentada

Finalmente, OpenCV ha obtenido un avance notorio en el campo de la visión artificial permitiendo que las maquinas puedan ver, analizar e identificar los procesos que se llevan a cabo por la visión humana pudiendo tomar decisiones y realizando las tareas con éxito al igual que un humano y en el menor tiempo posible.

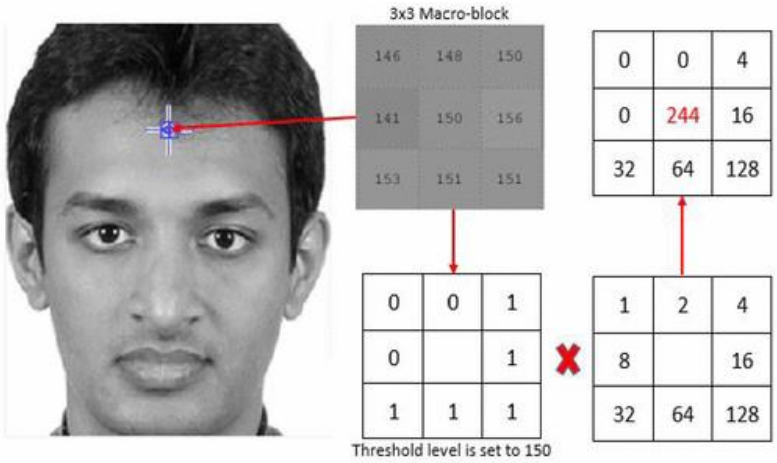
VI. LBPH

LBPH (Histogramas de patrones locales binarios). El algoritmo calcula patrones binarios locales para generar vectores de características. Para calcular las características de LBP, la ventana examinada se divide en varias celdas. Cada celda contiene un subbloque de 3 x 3 píxeles. Luego, cada píxel del subbloque se compara con sus píxeles vecinos. Si el valor del píxel central es mayor que el píxel vecino, se almacena 1 en la ubicación de ese píxel. Si los valores del píxel central son menores que el píxel vecino, el valor gris de ese píxel se reemplaza por 0. Esto hace que el subbloque sea un bloque

binario que contiene 0 y 1 dependiendo de sus valores de píxel. Esto se conoce como etiquetado de píxeles. Estos píxeles etiquetados generan un patrón binario que luego se convierte en un valor decimal. El valor gris del píxel central se reemplaza por el valor decimal. Este procedimiento se repite en toda la imagen y se obtiene una imagen LBP. A continuación, se calcula un histograma sobre la frecuencia de aparición de cada número. Este histograma proporciona un vector de características de la ventana. Para realizar el reconocimiento facial, la imagen facial se divide en varios bloques o regiones. Luego, para cada bloque o región se calcula un histograma LBP como se explicó anteriormente. El vector de características de toda la imagen es una combinación de todos los histogramas de LBP de todas las regiones de una imagen (Yaseen et al. 2018).

El valor del píxel central es un umbral para el resto de sus vecinos. Cualquier valor que sea igual o mayor que 150 se establece en 1 y si son menores, se establecen en 0 como se muestra en la Figura 5 (Wang and Siddique 2020).

Figura 5 Representación de LBPH

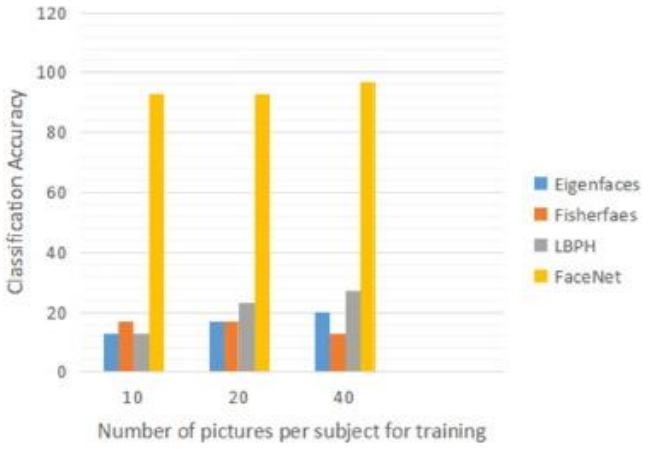


Fuente: Adaptado de (Wang and Siddique 2020).

Teniendo en cuenta que LBPH es uno de los descriptores de textura más poderosos para representar estructuras locales. Las propiedades conjuntas de LBPH lo convierte excelente opción para el análisis de imágenes (Acharya et al. 2017).

Existen otros algoritmos como EigenFace, FisherFaces que permiten de igual forma que LBPH reconocer un rostro a continuación podemos ver como LBPH tiene más precisión al momento de realizar el reconocimiento que los métodos anteriores, omitiendo los resultados de FaceNet se logra notar que LBPH está por encima de EigenFace y FisherFace.

Figura 6 Comparación de precisión de diferentes algoritmos



Fuente: Adaptado de (Rameswari et al. 2020).

VII. FISHERFACES

Los métodos basados en extracción de características lineales se han utilizado ampliamente en el reconocimiento facial. Entre ellos, hay dos técnicas más famosas: Eigenfaces y Fisherfaces. Eigenfaces se basa en la técnica de Análisis de Componentes Principales (PCA). Fue propuesto originalmente por Kirby y Sirovich y popularizado por Turk y Pentland. Fisherfaces se basa en el análisis discriminante lineal de Fisher (LDA) y fue propuesto por Swets y Belhumeur , respectivamente. Fisherfaces ha demostrado ser mejor que Eigenfaces, especialmente en las condiciones en las que se producen variaciones en la iluminación y la expresión facial (Yang, Yang, and Frangi 2003).

Fisherfaces realiza un LDA, donde se busca aprovechar la información disponible, sobre la clasificación de las imágenes de entrenamiento, para buscar una proyección que maximice la separación entre imágenes de diferentes personas (o clases) y minimice la distancia entre imágenes de una misma clase. Así logra concentrar las imágenes mejorando, en forma importante, la tasa de reconocimiento (Franco et al. 2017).

FisherFace funciona similar a LBPH donde Fisherface extrae los rasgos faciales luego los exporta en un modelo .xml que son analizados en la etapa de entrenamiento para finalmente ser importados en la etapa de reconocimiento facial y cumplir con éxito su objetivo.

VIII. CONCLUSIONES

Este estudio está basado en los sistemas biométricos como el reconocimiento facial que han demostrado un alto nivel de precisión al momento de efectuar la identificación de una persona, siendo utilizado como una modalidad de seguridad que tiene como objetivo a través de una cámara y una serie de datos recopilados mediante un sistema realizado con algoritmos pueda hacer una identificación de una manera automática en tiempo real y permitir ingreso a un sitio.

La implementación de un sistema de reconocimiento facial para el ingreso a un sitio se plantea como una propuesta tecnológica innovadora que apoya de manera sistemática la verificación del personal que se realiza de manera manual ahorrando pérdida de tiempo al momento de no llevar una identificación que valide si es posible darle ingreso al sitio.

Realizando varios análisis con diferentes algoritmos de reconocimiento facial se comprobó que con LBPH se obtienen mejores resultados presentado menos errores frente a los cambios de iluminación y menos tiempo de ejecución

El reconocimiento facial elimina la necesidad de tarjetas físicas y dispositivos de proximidad, evita el contacto con otras personas previniendo la exposición de enfermedades.

OpenCV es una de las bibliotecas que ha sido mas utilizadas gracias a su amplitud de aplicaciones en diferentes ámbitos utilizando la inteligencia artificial, demostrando resultados completamente exitosos como lo ha sido el reconocimiento facial.

Los clasificadores en cascada facilitan el proceso de reconocimiento facial gracias a las bibliotecas que poseen modelos ya pre entrenados que permiten capturar el rostro y posteriormente identificarlo.

A futuro a partir de este análisis se puede implementar un prototipo de reconocimiento facial automatizando el proceso que realiza un vigilante para control de acceso y seguridad en un determinado sitio.

IX. REFERENCIAS

- Acharya, U. Rajendra, Wei Lin Ng, Kartini Rahmat, Vidya K. Sudarshan, Joel E. W. Koh, Jen Hong Tan, Yuki Hagiwara, Arkadiusz Gertych, Farhana Fadzli, Chai Hong Yeong, and Kwan Hoong Ng. 2017. "Shear Wave Elastography for Characterization of Breast Lesions: Shearlet Transform and Local Binary Pattern Histogram Techniques." Computers in Biology and Medicine 91:13–20. doi: 10.1016/j.compbiomed.2017.10.001.
- Ampamya, Sight, John M. Kitayimbwa, and Martin C. Were. 2020. "Performance of an Open Source Facial Recognition System for Unique Patient Matching in a Resource-Limited Setting." *International Journal of Medical Informatics* 141:104180.
- Bah, Serign Modou, and Fang Ming. 2020. "An Improved Face Recognition Algorithm and Its Application in Attendance Management System." Array 5:100014. doi: 10.1016/j.array.2019.100014.
- Caballero Julián, Franco Gabriel, Martín Vidal Reyes, Antonia López Sánchez, and Carlos Alberto Jerónimo Ríos. 2016. "Reconocimiento Facial Por El Método De Eigenfaces." Pistas Educativas 39(04):66–81.
- Chamikara, M. A. P., P. Bertok, I. Khalil, D. Liu, and S. Camtepe. 2020. "Privacy Preserving Face Recognition Utilizing Differential Privacy." Computers and Security 97:101951. doi: 10.1016/j.cose.2020.101951.
- Franco, C. E., Ospina, C. T., Cuevas, E. S., & Capacho, D. V. (2017). RECONOCIMIENTO FACIAL BASADO EN EIGENFACES, LBHP Y FISHERFACES EN LA BEAGLEBOARD-XM. Revista colombiana de tecnologias de avanzada (rcta), 2(26). https://doi.org/10.24054/16927257.v26.n26.2015.2387
- Hamdan, Bensenane, and Keche Mokhtar. 2018. "The Detection of Spoofing by 3D Mask in a 2D Identity Recognition System." Egyptian Informatics Journal 19(2):75–82.
- Jayaraman, Umarani, Phalguni Gupta, Sandesh Gupta, Geetika Arora, and Kamlesh Tiwari. 2020. "Recent

Development in Face Recognition." Neurocomputing 408:231–45. doi: 10.1016/j.neucom.2019.08.110.

- Leong, Shu-Min, Raphaël C. W. Phan, Vishnu Monn Baskaran, and Chee-Pun Ooi. 2020. "Privacy-Preserving Facial Recognition Based on Temporal Features." *Applied Soft Computing* 96:106662. doi: https://doi.org/10.1016/j.asoc.2020.106662.
- Llapapasca Montes, Antonio Marco, and Manuel Alexander Ochoa Zevallos. 2019. "' Creación de Una Librería de Software de Reconocimiento Facial Enfocado a La Identificación de Trabajadores de Una Empresa ' Ingeniería de Software." Universidad Tecnológica Del Perú.
- Masud, Mehedi, Ghulam Muhammad, Hesham Alhumyani, Sultan S. Alshamrani, Omar Cheikhrouhou, Saleh Ibrahim, and M. Shamim Hossain. 2020. "Deep Learning-Based Intelligent Face Recognition in IoT-Cloud Environment." Computer Communications 152:215–22. doi: 10.1016/j.comcom.2020.01.050.
- Mi, Jian Xun, Yueru Sun, Jia Lu, and Heng Kong. 2020. "Robust Supervised Sparse Representation for Face Recognition." Cognitive Systems Research 62:10–22. doi: 10.1016/j.cogsys.2020.02.001.
- Mohammed, Khaled, A. S. Tolba, and Mohammed Elmogy. 2018. "Multimodal Student Attendance Management System (MSAMS)." Ain Shams Engineering Journal 9(4):2917–29. doi: 10.1016/j.asej.2018.08.002.
- Rameswari, R., S. Naveen Kumar, M. Abishek Aananth, and C. Deepak. 2020. "Automated Access Control System Using Face Recognition." Materials Today: Proceedings. doi: 10.1016/j.matpr.2020.04.664.
- Shrivastava, Kritika, Shweta Manda, S. Chavan, T. B. Patil, and S. T. Sawant-Patil. 2018. Conceptual Model for Proficient Automated Attendance System Based on Face Recognition and Gender Classification Using Haar-Cascade, LBPH Algorithm along with LDA Model. Vol. 13.
- Singh, A., and F. Furtado. n.d. "Modified Haar-Cascade Model for Face Detection Issues." doi: 10.22105/riej.2020.226857.1129.
- Taskiran, Murat, Nihan Kahraman, and Cigdem Eroglu Erdem. 2020. "Face Recognition: Past, Present and Future (a Review)." *Digital Signal Processing* 106:102809. doi: https://doi.org/10.1016/j.dsp.2020.102809.
- Wang, Li, and Ali Akbar Siddique. 2020. "Facial Recognition System Using LBPH Face Recognizer for Anti-Theft and Surveillance Application Based on Drone Technology." Measurement and Control 002029402093234. doi: 10.1177/0020294020932344.
- Yang, J., Yang, J. Y., & Frangi, A. F. (2003). Combined Fisherfaces framework. Image and Vision Computing, 21(12), 1037–1044. https://doi.org/10.1016/j.imavis.2003.07.005
- Yaseen, Muhammad Usman, Ashiq Anjum, Omer Rana, and Richard Hill. 2018. "Cloud-Based Scalable Object Detection and Classification in Video Streams." Future Generation Computer Systems 80:286–98. doi: 10.1016/j.future.2017.02.003.
- Zhan, Shu, Qin Qin Tao, and Xiao Hong Li. 2016. "Face Detection Using Representation Learning." Neurocomputing 187:19–26. doi: 10.1016/j.neucom.2015.07.130.
- Zhao, Chen, Xuelong Li, and Yongsheng Dong. 2020. "Learning Blur Invariant Binary Descriptor for Face Recognition." Neurocomputing 404:34–40. doi: 10.1016/j.neucom.2020.04.082.
- Zhu, Zhiguo, and Yao Cheng. 2020. "Application of Attitude Tracking Algorithm for Face Recognition Based on OpenCV in the Intelligent Door Lock." Computer Communications 154:390–97. doi: 10.1016/j.comcom.2020.02.003.