

UNIVERSIDAD DE HUANUCO

ESCUELA DE POSGRADO

PROGRAMA ACADÉMICO DE MAESTRÍA EN INGENIERÍA DE
SISTEMAS E INFORMÁTICA, CON MENCIÓN EN GERENCIA DE
SISTEMAS Y TECNOLOGIAS DE INFORMACIÓN



TESIS

**“SISTEMA DE RECONOCIMIENTO FACIAL EN LÍNEA PARA
PREVENIR LA SUPLANTACIÓN Y EL PLAGIO EN EL EXAMEN DE
ADMISIÓN VIRTUAL EN LA UNIVERSIDAD DE HUÁNUCO 2020”**

PARA OPTAR EL GRADO ACADÉMICO DE MAESTRO EN
INGENIERÍA DE SISTEMAS E INFORMÁTICA, CON MENCIÓN EN
GERENCIA DE SISTEMAS Y TECNOLOGIAS DE INFORMACIÓN

AUTOR: Beraún Barrantes, José Guillermo

ASESOR: Jacha Rojas, Johnny Prudencio

HUÁNUCO – PERÚ

2021



UDH
UNIVERSIDAD DE HUANUCO
<http://www.udh.edu.pe>

U

D

H

TIPO DEL TRABAJO DE INVESTIGACIÓN:

- Tesis (X)
- Trabajo de Suficiencia Profesional ()
- Trabajo de Investigación ()
- Trabajo Académico ()

LÍNEAS DE INVESTIGACIÓN: Gestión y Desarrollo de Sistemas de Información

AÑO DE LA LÍNEA DE INVESTIGACIÓN (2020)

CAMPO DE CONOCIMIENTO OCDE:

Área: Ingeniería, Tecnología

Sub área: Ingeniería eléctrica, Ingeniería electrónica

Disciplina: Ingeniería de Sistemas y comunicaciones

DATOS DEL PROGRAMA:

Nombre del Grado/Título a recibir: Maestro en ingeniería de sistemas e informática, con mención en gerencia de sistemas y tecnologías de información

Código del Programa: P25

Tipo de Financiamiento:

- Propio ()
- UDH ()
- Fondos Concursables ()

DATOS DEL AUTOR:

Documento Nacional de Identidad (DNI): 41556658

DATOS DEL ASESOR:

Documento Nacional de Identidad (DNI): 40895876

Grado/Título: Maestro en ingeniería de sistemas e informática con mención en: gerencia de sistemas y tecnologías de información

Código ORCID: 0000-0001-7920-1304

DATOS DE LOS JURADOS:

N°	APELLIDOS Y NOMBRES	GRADO	DNI	Código ORCID
1	López De La Cruz, Edgardo Cristiam Iván	Magister en ciencias de la educación mención: educación ambiental y desarrollo sostenible	40394603	0000-0001-9815-7708
2	Camara Llanos, Frank Erick	Maestro en ciencias de la salud con mención en: salud pública y docencia universitaria	44287920	0000-0001-9180-7405
3	De Jesus Mendoza, Efer	Maestro en ingeniería, con mención en: gestión ambiental y desarrollo sostenible	43411558	0000-0002-5372-6345



UNIVERSIDAD DE HUÁNUCO

Escuela de Posgrado

ACTA DE SUSTENTACIÓN DEL GRADO DE MAESTRO EN INGENIERÍA DE SISTEMAS E INFORMÁTICA

En la ciudad de Huánuco, siendo las 16:00 horas del día 12 del mes de marzo del año 2021, en cumplimiento de lo señalado en el Reglamento de Grados y Títulos de la Universidad de Huánuco, se reunieron el sustentante y el Jurado Calificador mediante la plataforma virtual Google meet integrado por los docentes:

- Mg. EDGARDO CRISTIAM IVÁN LÓPEZ DE LA CRUZ
- Mg. FRANK ERICK CAMARA LLANOS
- Mg. EFER DE JESUS MENDOZA

Nombrados mediante resolución N° 047-2021-D-EPG-UDH; para evaluar la tesis intitulada **"SISTEMA DE RECONOCIMIENTO FACIAL EN LÍNEA PARA PREVENIR LA SUPLANTACIÓN Y EL PLAGIO EN EL EXAMEN DE ADMISIÓN VIRTUAL EN LA UNIVERSIDAD DE HUÁNUCO 2020"**; Presentado por el Bach. BERAUN BARRANTES, José Guillermo para optar el grado de maestro en ingeniería de sistemas e informática, con mención en gerencia de sistemas y tecnologías de información.

Dicho acto de sustentación se desarrolla en dos etapas: exposición y absolución de preguntas procediéndose luego a la evaluación por parte de los miembros de jurado.

Habiéndose absuelto las objeciones que le fueron formuladas por los miembros del jurado y de conformidad con las respectivas disposiciones reglamentarias procedieron a deliberar y calificar, declarándolo **aprobado** por **unanimidad** con calificativo cuantitativo de **17** y cualitativo de **Muy Bueno**.

Siendo las 17:16 horas del día viernes 12 del mes de marzo del año dos mil veintiuno, los miembros del jurado calificador firman la presente acta en señal de conformidad.

Presidente

Mg. Edgardo Cristiam Iván López De La Cruz

Secretario

Mg. Frank Erick Camara Llanos

Vocal

Mg. Efer De Jesús Mendoza

DEDICATORIA

A Dios por darme el don de la vida, a mis padres, a mi familia por su amor y apoyo incondicional, que siempre me dieron las fuerzas para continuar, enseñándome a salir adelante frente a todos los obstáculos.

AGRADECIMIENTO

Mi agradecimiento y reconocimiento a la Escuela de Posgrado de la Universidad de Huánuco, por brindarme los conocimientos fortaleciendo mis habilidades profesionales.

Así mismo, agradezco a todos los docentes de la Escuela de Posgrado de la Universidad de Huánuco por el valioso conocimiento brindado y apoyo ratificado a través de sus consejos y experiencias.

Por último, mi agradecimiento va dirigido a mi asesor, quien con toda su capacidad, conocimiento científico y consejos logró guiarme durante todo el desarrollo de la tesis.

ÍNDICE

DEDICATORIA	II
AGRADECIMIENTO	III
ÍNDICE.....	IV
ÍNDICE DE TABLAS	VI
ÍNDICE DE FIGURAS	VII
RESUMEN	VIII
SUMMARY.....	IX
INTRODUCCIÓN	X
CAPÍTULO I.....	12
PLANTEAMIENTO DEL PROBLEMA.....	12
1.1. Descripción del Problema de Investigación	12
1.2. Formulación del problema.....	16
1.3. Objetivo general.....	16
1.4. Objetivos específicos	16
1.5. Justificación de la investigación	17
CAPÍTULO II.....	18
MARCO TEÓRICO	18
2.1. Antecedentes de la investigación.....	18
2.1.1. Antecedentes Internacionales.....	18
2.1.2. Antecedentes Nacionales	22
2.1.3. Antecedentes Locales.....	23
2.2. Bases teóricas	23
2.2.1 Algoritmos de Detección Facial.....	23
2.2.2 Preprocesamiento de Imágenes	28
2.2.3 Algoritmos de Reconocimiento Facial	30
2.2.4 Software de Reconocimiento Facial de Código Abierto OpenFace	37
2.3. Definiciones conceptuales	37
2.4. Sistema de Hipótesis	39
2.5. Sistema de variables.....	39
- Variable independiente	39
- Variable dependiente	39

2.6. Operacionalización de las Variables	40
CAPITULO III	41
MARCO METODOLÓGICO	41
3.1. Tipo de investigación	41
3.1.1 Enfoque.....	41
3.1.2 Alcance o nivel	41
3.1.3 Diseño.....	41
3.2. Población y muestra.....	41
3.2.1. Población	41
3.2.2. Muestra	42
3.3. Técnicas e instrumentos de recolección de datos	42
3.3. Técnicas para el procesamiento y análisis de la información	42
CAPITULO IV.....	43
RESULTADOS.....	43
4.1. Descripción de los resultados	43
4.2. Análisis de los resultados.....	45
4.3. Prueba de Hipótesis.....	49
CAPITULO V.....	51
DISCUSIÓN DE RESULTADOS	51
CONCLUSIONES	53
RECOMENDACIONES	54
REFERENCIAS BIBLIOGRÁFICAS.....	55
ANEXOS	58

ÍNDICE DE TABLAS

Tabla N° 1 Resultados del proceso de reconocimiento de Reconocimiento de postulantes.....	43
Tabla N° 2 Pasos de reconocimiento positivo erróneo.....	44
Tabla N° 3 Casos de no reconocimiento detectados como fraude	45
Tabla N° 4 Casos de reconocimiento exitoso	46
Tabla N° 5 Casos de reconocimiento fallido	47
Tabla N° 6 Causas de errores en el reconocimiento facial	48

ÍNDICE DE FIGURAS

Figura N° 1 Proceso de reconocimiento de reconocimiento de postulantes - Examen admisión UDH.....	43
Figura N° 2 Pasos de reconocimiento positivo erróneo	44

RESUMEN

El presente trabajo de investigación tiene como finalidad plantear una estrategia de control biométrico usando reconocimiento facial, para el control de los exámenes en modalidad virtual que se realicen en la Universidad de Huánuco. El estudio es de tipo aplicada con alcance descriptiva, de diseño experimental y de enfoque cuantitativo; la muestra está compuesta por un total de 1,252 postulantes del examen de admisión del año 2020. Se realizó una exploración inicial del estado actual de la tecnología; para luego realizar la implementación y medir la efectividad y pertinencia del sistema.

El sistema de reconocimiento “sin entrenamiento” funciona sobre un entorno web, usando como tecnología de backend la plataforma, Net Core y como frontend utiliza Angular. La razón de adoptar un prototipo de estas características es la de poder atender a un gran número de usuarios disminuyendo la necesidad de acciones previas en la instalación del postulante o la utilización de software en entornos variantes y con poca certidumbre respecto a las condiciones de software y hardware de los postulantes. La aplicación de este sistema, permitió prevenir la suplantación y el fraude académico. Los resultados nos indica que la tasa de reconocimiento es alta, lo que les permite a los controladores de examen concentrar su atención sobre 120 postulantes del total de 1252 que participaron del experimento, podemos asumir que el sistema ayuda con el 90.42% de los reconocimientos, mientras en el 9.58% de los casos se requiere el apoyo de los controladores. En consecuencia, se acepta la hipótesis de la investigación la implementación de un sistema con reconocimiento facial permite reducir la posibilidad de suplantación y plagio en el examen de admisión virtual en la Universidad de Huánuco, 2020. Asimismo, la utilización de esta tecnología permite atender un número significativo de usuarios, minimizando la cantidad de controladores humanos necesarios para llevar adelante un proceso de evaluación masivo como lo es un examen de admisión.

Palabras claves: sistema con reconocimiento facial, suplantación, fraude, examen de admisión.

SUMMARY

The purpose of this research work is to propose a biometric control strategy using facial recognition, for the control of examinations in virtual mode that are carried out at the University of Huánuco. The study is of an applied type with a descriptive scope, an experimental design and a quantitative approach; The sample is made up of a total of 1,252 applicants for the 2020 admission exam. An initial exploration of the current state of technology was carried out; and then carry out the implementation and measure the effectiveness and relevance of the system.

The recognition system "without training" works on a web environment, using the platform, Net Core, as the backend technology, and Angular as a frontend. The reason for adopting a prototype of these characteristics is to be able to serve a large number of users, reducing the need for prior actions in the installation of the applicant or the use of software in varying environments and with little certainty regarding the software conditions and Applicant hardware. The application of this system made it possible to prevent impersonation and academic fraud. The results indicate that the recognition rate is high, which allows the exam controllers to focus their attention on 120 applicants out of the total of 1252 who participated in the experiment, we can assume that the system helps with 90.42% of the recognitions, while in 9.58% of the cases the support of the controllers is required. Consequently, the research hypothesis is accepted: the implementation of a system with facial recognition allows reducing the possibility of impersonation and plagiarism in the virtual admission exam at the University of Huánuco, 2020. Likewise, the use of this technology allows to attend a significant number of users, minimizing the number of human controllers required to carry out a massive evaluation process such as an admission exam.

Keywords: facial recognition system, impersonation, fraud, admission test.

INTRODUCCIÓN

La pandemia del COVID19 nos ha obligado a replantear casi todos los aspectos de nuestro quehacer diario. Desde las actividades más sencillas, como ir a la tienda por algo de pan, hasta aquellas más complejas y que representan cambios muy profundos en nuestros estilos de vida.

Una de las primeras actividades que en nuestro país fueron impactadas por la declaración del estado de emergencia y de la cuarentena fue la educación. Se suspendieron las actividades educativas presenciales en todos los niveles desde el nivel inicial hasta el postgrado. El gobierno y las instituciones que se dedican a estas actividades se vieron en la imperiosa necesidad de correr contra el tiempo para implementar soluciones que permitan la no presencialidad y la virtualidad.

El camino no ha sido sencillo y aún estamos transitándolo. La pandemia ha evidenciado las brechas que existen en términos de conectividad y acceso a la tecnología en nuestro país. La virtualidad ha surgido como una oportunidad para superar los problemas que ha originado el aislamiento, aunque esto también ha implicado la aparición de nuevos desafíos para los cuales no estábamos preparados. Tanto La formación de competencias para adaptarse a la virtualidad también ha sido un tema de mucha importancia. docentes como alumnos han tenido que cambiar el aula, la pizarra y el proyector; por el computador conectado a Internet desde el lugar que mejor puedan adaptar dentro de sus hogares y de acuerdo con sus posibilidades económicas.

Un problema que ha sido transversal, a todos los niveles del quehacer educativo, ha sido el tema de la evaluación. No sólo se presentan desafíos desde la pertinencia y efectividad de la evaluación, sino desde la perspectiva de su transparencia. El presente trabajo, en el marco de estudio de los sistemas y tecnologías de información, busca desarrollar un prototipo tecnológico, producto de software, para reducir la incertidumbre de los docentes respecto a la transparencia de las evaluaciones.

Para este fin se planteó usar una tecnología que lleva bastante tiempo y desarrollo en el escenario de la tecnología informática, específicamente dentro del campo de la biometría: nos referimos al reconocimiento facial.

El primer desafío que se plantea este estudio es investigar respecto a la tecnología disponible, de preferencia de código abierto, para la selección de un entorno de desarrollo y librerías que permitan llegar al segundo objetivo del estudio, que es la construcción de un prototipo funcional.

Finalmente, se realizaron pruebas controladas para experimentar si el prototipo ayuda a probar la hipótesis que nos planteamos. Creemos firmemente que en épocas de crisis como la que atravesamos, estudios que permitan afrontar la “nueva normalidad”, que poco a poco va surgiendo, serán de vital importancia para darle continuidad a nuestro desarrollo personal y profesional.

CAPÍTULO I

PLANTEAMIENTO DEL PROBLEMA

1.1. Descripción del Problema de Investigación

La pandemia por COVID19 ha obligado a virtualizar la totalidad de actividades educativas, en todos los niveles, en el Perú. Si bien todos los niveles educativos tienen problemas comunes, cada cual tiene características particulares, centradas en el usuario principal del servicio que es el alumno. Para este estudio, vamos a circunscribir la situación problemática al rubro de la educación superior.

En la mayoría de los países en el mundo, la pandemia ha obligado a la suspensión de toda actividad que implique aglomeración de personas. La educación superior, y en general toda actividad educativa presencial, ha sido catalogada como una actividad que puede convertirse fácilmente en una fuente de contagio, debido a la gran cantidad de alumnos que se movilizan en el desarrollo de la actividad académica presencial. Al respecto la SUNEDU (2020) indica: “En el pregrado, la matrícula ha experimentado un incremento significativo entre los años 2008 y 2019. ... a nivel nacional, se pasó de cerca de 771 900 estudiantes de pregrado en el 2008 a casi 1 509 400 en el 2019” (p.33). Resulta evidente entonces que el riesgo de continuar con la presencialidad de la educación superior es muy alto. Con más de un millón de personas expuestas al contagio, las universidades se convertirían fácilmente en un factor desencadenante de contagio masivo.

En nuestro país, la SUNEDU a través de la Resolución de Consejo Directivo 039-2020-SUNEDU-CD publicada en el diario oficial El Peruano (2020) se decreta: “Aprobar los “Criterios para la supervisión de la adaptación de la educación no presencial, con carácter excepcional, de las asignaturas por parte de universidades y escuelas de posgrado como consecuencia de las medidas para prevenir y controlar el COVID-19”, que constan de diez (10) artículos y cinco (5) disposiciones complementarias finales.”(p.8)

Dentro de los criterios establecidos por SUNEDU se definen una serie de condiciones a observar, por parte de las universidades, en el proceso de adaptación de las clases presenciales a una modalidad no presencial. Cada criterio presenta desafíos singulares, pero hay uno que hemos considerado bastante difícil de cumplir por las características particulares de la actividad que se pretende supervisar, sobre la cual SUNEDU en la misma resolución de la cita anterior indica en su capítulo 7 numeral 7.6 literal d: “Adaptar de forma no presencial las evaluaciones previstas con el objeto de que logren acreditar los aprendizajes requeridos y, además, se evite el plagio, la suplantación o el fraude.”(p.9)

La prevención del plagio, la suplantación y el fraude son tareas que han acompañado a la educación presencial desde sus labores y en la cual, el ejecutor del fraude y el controlador, están en igualdad de condiciones. Con esto nos referimos a que existe control de entrada al claustro universitario, el docente controla el espacio físico usado para la evaluación y controla las interacciones entre los alumnos y con cualquier otro agente externo.

La evaluación virtual plantea un escenario completamente diferente. El docente ha perdido el control del entorno y no puede vigilar simultáneamente a todos los alumnos evaluados. Esta tarea se torna más compleja a medida que se incrementa la cantidad de alumnos que se deben evaluar. Resulta evidente en este punto que requerimos el desarrollo de estrategias para facilitarle esta tarea a los docentes, más aún, cuando la evaluación determinará el éxito del proceso de enseñanza aprendizaje. Respecto a el aporte de la I+D a tareas como ésta en el contexto de la pandemia el Instituto Internacional de la UNESCO para la Educación Superior (IESALC) (2020) dice:

Más allá de la investigación relativa a la crisis, existen otras áreas que requieren de las capacidades de la educación superior para producir nuevos conocimientos y desarrollar renovadas capacidades. Una de ellas, entre otras, es precisamente la educación. En ese momento de crisis no es posible cuantificar el

aprendizaje que se está produciendo en este, desde lo pedagógico hasta lo económico, psicosocial, etc. Con seguridad en el futuro próximo se podrá sacar partido del conocimiento que están generando los aprendizajes, en algunos casos “forzados”, que esta situación está generando. Se podrá pensar así en un sistema de alerta temprana para prever y mitigar los efectos de crisis como esta sobre los sistemas educativos y los aprendizajes de estudiantes, docentes y de los propios sistemas. Sin duda se generará también una gran cantidad de investigación relativa a los efectos de esta crisis en áreas como la sostenibilidad ambiental, la industria, la economía y otros. (p.32)

Resulta obvia la preocupación por la generación de conocimiento y tecnología que nos ayude a sortear los desafíos que la educación y la evaluación virtuales, en específico, nos presentan. El problema de la evaluación en línea o evaluación virtual tiene varias aristas. Una primera que es pedagógica que tiene que ver con la pertinencia y eficacia de los instrumentos de evaluación y otra que tiene que ver con el soporte tecnológico para la accesibilidad y seguridad del proceso de evaluación. Por nuestro campo de estudio nos concentraremos sobre el segundo aspecto.

Si hablamos de accesibilidad, en el mercado hoy existen productos tecnológicos que nos permiten diseñar, desplegar y ejecutar la evaluación de los alumnos. Entre los productos más conocidos tenemos Google Forms, Socrative, etc. Ahora, si de seguridad hablamos, ninguna de las plataformas de mayor uso ofrece un esquema de seguridad lo suficientemente efectivo para verificar la identidad y la presencia del estudiante.

Al respecto Termini y Hayes (2014) nos dicen:

Student identity authentication for distance education programs is an important factor in the successful implementation of an e-learning program. This check is necessary to ensure an institution is giving credit to the student who completed the work

and protects the reputation of the institution. It is also important in efforts to safeguard Title IV funding and reducing institutional liability in federal financial aid fraud cases. Between 2009 and 2012, federal financial aid fraud grew 82 percent, with more than 85,000 people potentially participating in fraud rings, accounting for \$874 million during this disbursement period. A February 2014 Education Department Inspector General audit found that federal rules regarding identity verification in distance education programs “do not sufficiently mitigate the risks of fraud, abuse, and noncompliance.” The audit highlights the need for new standards and regulation regarding financial aid disbursement in distance education programs. [La autenticación de la identidad de los estudiantes para los programas de educación a distancia es un factor importante en la implementación exitosa de un programa de aprendizaje electrónico. Esta verificación es necesaria para garantizar que una institución otorgue crédito al estudiante que completó el trabajo y protege la reputación de la institución. También es importante en los esfuerzos por salvaguardar los fondos del Título IV y reducir la responsabilidad institucional en casos de fraude de ayuda financiera federal. Entre 2009 y 2012, el fraude de ayuda financiera federal creció un 82 por ciento, con más de 85,000 personas potencialmente participando en redes de fraude, lo que representa \$ 874 millones durante este período de desembolso. Una auditoría del Inspector General del Departamento de Educación de febrero de 2014 encontró que las reglas federales con respecto a la verificación de identidad en los programas de educación a distancia "no mitigan suficientemente los riesgos de fraude, abuso e incumplimiento". La auditoría destaca la necesidad de nuevos estándares y regulaciones con respecto al desembolso de ayuda financiera en los programas de educación a distancia.]

En resumen, nos encontramos frente a una problemática compleja que tiene incluso implicancias legales y económicas, sin contar con el

impacto sobre la reputación de las entidades académicas y sobre la calidad de la formación académica que se imparte en las mismas.

En la Universidad de Huánuco, se ha iniciado por las razones conocidas el proceso de adaptación de las clases presenciales a entorno virtual. El proceso ha sido exitoso y se ha logrado programar la totalidad de cursos teóricos de la malla curricular. Sin embargo, la problemática de la evaluación aún está presente. Si bien existe la plataforma para la evaluación virtual o remota, existe la preocupación por la transparencia del proceso, dado que el control de las evaluaciones es complicado por diversos factores como la propia esencia remota del proceso, la cultura de valores de nuestra sociedad y el temor del alumno de perder lo invertido o su deseo de alcanzar mejores calificaciones más allá de su nivel de preparación.

Queda claro entonces que la situación problemática que afrontaremos con este proyecto de investigación está relacionada con la poca confiabilidad de la evaluación en línea en términos de prevención de suplantación, plagio y fraude.

1.2. Formulación del problema

¿En qué medida un sistema con reconocimiento facial permite reducir la posibilidad de suplantación y plagio en el examen de admisión virtual en la Universidad de Huánuco, 2020?

1.3. Objetivo general

Desarrollar un sistema con reconocimiento facial que permita reducir la posibilidad de suplantación y plagio en el examen de admisión virtual en la Universidad de Huánuco, 2020.

1.4. Objetivos específicos

- Seleccionar un entorno y marco de desarrollo de código abierto para la construcción del prototipo
- Desarrollar un prototipo funcional para demostrar la confiabilidad de la propuesta

- Reducir los intentos de suplantación y plagio en la evaluación en línea de la Universidad de Huánuco
- Identificar los campos de acción adicionales en los que se podría utilizar este prototipo.

1.5. Justificación de la investigación

Esta investigación encuentra su justificación en la importancia de dotar de confiabilidad a la evaluación en línea frente al plagio, la suplantación y el fraude. En el marco del proceso de enseñanza aprendizaje, la evaluación es una de las actividades clave en la tarea de verificar si se han alcanzado los objetivos pedagógicos que se ha planteado el docente.

Es más, podríamos estar andando ciegos o engañados pensando que la educación virtual rinde resultados equivalentes o superiores a la educación presencial si no nos aseguramos de que la medición de los resultados es confiable y no posee sesgos producto de intervenciones indeseadas o ayudas indebidas.

La importancia de investigar la problemática y de encontrar un modelo o prototipo que ayude a mitigar la prevalencia de la situación problemática tiene adicionalmente la ventaja de ser escalable con facilidad a otros ámbitos o niveles de la educación más allá de la educación superior.

Las estrategias de evaluación virtual, sumadas a la reducción de la brecha de conectividad y acceso a la tecnología, pueden ser una herramienta increíblemente potente para el estado, de cara a tener datos reales e inmediatos respecto a la condición de las competencias de los estudiantes en los distintos niveles.

Sólo con información de este tipo es posible desarrollar estrategias efectivas para diseñar un modelo educativo acorde con nuestras debilidades y fortalezas que nos permita superar nuestro subdesarrollo.

CAPÍTULO II

MARCO TEÓRICO

2.1. Antecedentes de la investigación

2.1.1. Antecedentes Internacionales

La educación virtual no es un invento producto de la pandemia por COVID19, sino que tiene mucho tiempo con nosotros. Tampoco han sido pocos los acercamientos con la biometría para dotar a la educación virtual de diversas características que mejoren su posicionamiento frente a la educación tradicional. Por ejemplo, hay estudios que intentan usar el reconocimiento de las emociones del rostro, para determinar el estado de ánimo del alumno y definir estrategias para captar mejor su atención. Un estudio en esta línea es el de Ayvaz et. al. (2017) que indica:

The purpose of the study is to develop a new Facial Emotion Recognition System (FERS), which recognize the emotional states and motivation levels of students in videoconference type e-learning systems. In order to create a more interactive educational environment, this system transfers the emotional states of the students to the educator instantaneously. Our study is supportive of the studies that make possible to observe the motivation level of both the individual and the virtual classroom in the e-learning systems. [El propósito del estudio es desarrollar un nuevo Sistema de Reconocimiento de Emociones Faciales (FERS), que reconozca los estados emocionales y niveles de motivación de los estudiantes en sistemas de e-learning tipo videoconferencia. Para crear un ambiente educativo más interactivo, este sistema transfiere instantáneamente los estados emocionales de los estudiantes al educador. Nuestro estudio apoya los estudios que permiten observar el nivel de motivación

tanto del aula individual como virtual en los sistemas de e-learning.] (p.97)

El estudio citado es muy interesante porque permite ampliar el horizonte respecto a la utilidad de la biometría en el campo del e-learning, buscando no sólo control sino también mitigar la frialdad y la falta de contacto humano que la educación virtual implica.

Gianni et. al. (2017) identifican también la necesidad de implementar sistemas de autenticación que permitan prevenir el plagio y la suplantación. Al respecto dicen:

In addition, educational institutions must face challenges in anticipating cheating by online students, especially when the exam is in progress. [Además, las instituciones educativas deben enfrentar desafíos para anticipar las trampas de los estudiantes en línea, especialmente cuando el examen está en curso.] (pp.1–10)

Sucianna et. al. (2018) proponen un método para la autenticación usando un método de detección y reconocimiento facial para evitar la suplantación en la educación en línea especialmente durante los exámenes. En este planteamiento el reconocimiento facial es utilizado para autenticar el acceso del alumno al entorno virtual. Textualmente sostienen:

In E-Learning, FR (Face Recognition) can be used as a login system and as a verifactor, so the system can authenticate an account that is logged in as an original or a person who imitates the original user. [En E-Learning, RF (reconocimiento facial) se puede utilizar como sistema de inicio de sesión y como verificador, por lo que el sistema puede autenticar una cuenta que haya iniciado sesión como original o como una persona que imita al usuario original.] (p.474)

Balraj y Abirami (2020) conducen un estudio muy interesante respecto a un sistema de autenticación multibiométrico para el cual crean una matriz con las distintas técnicas de identificación

biométrica que pueden ser usadas por este sistema y las analizan y califican en base a parámetros de aceptabilidad, distinción (precisión), esquivé, recolección, performance y universalidad.

Como puede observarse, existen una multiplicidad de técnicas de biometría que podemos utilizar, sin embargo, la utilización de la mayoría de ellas requiere equipamiento especial en el lado del cliente, que por lo general es de difícil acceso por costo y disponibilidad en el mercado. Otra conclusión interesante del estudio es la baja puntuación del reconocimiento facial en términos de precisión y performance.

Respecto a este último punto, cabe resaltar que, si bien es aceptada la posición respecto a la falta de precisión de los algoritmos de reconocimiento facial en contraposición a los de lectura de iris o huella digital, resultan obvias también sus ventajas respecto a aceptabilidad de resultados y facilidad de recolección de datos, especialmente en entornos como la educación virtual, en donde no existe una estandarización respecto a la tecnología disponible por parte del alumno. Sobre este punto Penteadó y Marana (2009) dicen: "Face recognition performance is not as accurate as fingerprint or iris recognition, but its acceptability and easiness of collection are distinctive" [El rendimiento del reconocimiento facial no es tan preciso como el reconocimiento de huellas dactilares o iris, pero su aceptabilidad y facilidad de recopilación son distintivas] (p.771)

Si bien se habla de la falta de precisión de las técnicas de reconocimiento facial frente a otras técnicas biométricas, hay que tener en cuenta que se puede incrementar la seguridad de las implementaciones acompañando el reconocimiento facial a otras formas de autenticación de datos de usuario, como contraseñas. Al respecto, Penteadó y Marana (2009) dicen:

There are two modes for biometric authentication: (i) verification, which consists in comparing the biometric trait collected against the credentials provided by the person,

checking if he is who he claims to be and (ii) identification, which attempts to check if the user is enrolled and whose sample is matched from the database, comparing the biometric trait without further credentials. [Existen dos modos de autenticación biométrica: (i) verificación, que consiste en comparar el rasgo biométrico recolectado con las credenciales proporcionadas por la persona, verificando si es quien dice ser y (ii) identificación, que intenta verificar si el usuario está inscrito y cuya muestra coincide con la base de datos, comparando el rasgo biométrico sin más credenciales.] (p.771)

Queda claro que para nuestro caso de estudio conviene la aproximación al concepto de verificación. De esta manera se reduce la posibilidad de que por problemas de precisión la solución genere más problemas de confiabilidad que los que se pretenden solucionar.

Kalikova et. al. (2015) desarrollaron un sistema de control biométrico llamado Biotest con el propósito de identificar a los alumnos durante el desarrollo de un examen en intervalos aleatorios. Si la identificación del alumno falla en más de tres ocasiones el sistema envía una notificación al profesor.

Fayyumi y Zarrad (2014) desarrollaron también un sistema de identificación facial para los alumnos que desarrollaban exámenes en línea. El sistema no sólo funcionaba para la autenticación del alumno, sino que hacía un monitoreo continuo en cortos intervalos de tiempo durante el examen para verificar que el alumno que había iniciado la sesión era el mismo que se encontraba rindiendo el examen.

Owayjan et. al. (2015) presentan un sistema dividido en dos partes, una primera que realizaba la detección del rostro a través de la cámara web y una segunda que se encargaba de la identificación y verificación del usuario. El funcionamiento es similar a los casos anteriores, en el cual se registran imágenes de la cámara web y se

comparan contra los registros de la base de datos del sistema, si el reconocimiento no es posible se emite una alerta.

2.1.2. Antecedentes Nacionales

Guillén-Gómez (2017) hace una interesante recopilación de sistemas de reconocimiento facial disponibles en el mercado y reseña sus características. Entre ellos destacan Securexam Remote Proctor, ProctorU, Kryterion Webassessor y Smowl entre las soluciones de tipo propietario y OpenFace entre las soluciones libres y de código abierto. Respecto a OpenFace indica:

Since OpenFace is an open-source project based in a research project of google, its creators have uploaded the source code to their website so everyone who is interested in the project can download it and consult it for free. To use it is necessary to previously introduce the information of every subject (name and a minimum of 10 pictures of this person) so OpenFace can learn how to differentiate every person using his features. This way, once the information of some subjects has been introduced, the system can find out who is who in real-time. It implements state-of-the-art facial behaviour analysis algorithms including: facial landmark detection, head pose tracking, eye gaze tracking, eye gaze and facial Action Unit estimation. [Dado que OpenFace es un proyecto de código abierto basado en un proyecto de investigación de google, sus creadores han subido el código fuente a su sitio web para que todos los interesados en el proyecto puedan descargarlo y consultarlo de forma gratuita. Para utilizarlo es necesario introducir previamente la información de cada sujeto (nombre y un mínimo de 10 fotografías de esta persona) para que OpenFace aprenda a diferenciar a cada persona utilizando sus características. De esta forma, una vez introducida la

información de algunos temas, el sistema puede averiguar quién es quién en tiempo real. Implementa algoritmos de análisis de comportamiento facial de última generación que incluyen: detección de puntos de referencia faciales, seguimiento de la postura de la cabeza, seguimiento de la mirada, estimación de la mirada y la unidad de acción facial.] (p.5-6)

Resulta evidente en este punto, que los esfuerzos en la investigación de esta problemática apuntan en la misma dirección con la que se alinea el presente estudio.

2.1.3. Antecedentes Locales

No existen investigaciones a nivel local

2.2. Bases teóricas

Hemos dividido la fundamentación teórica del presente estudio en cuatro etapas. La primera y segunda donde se analizan los principios teóricos de la detección, procesamiento de imágenes y el reconocimiento facial y una cuarta donde se analizan los productos de código abierto disponibles para la construcción del prototipo que persigue esta investigación.

2.2.1 Algoritmos de Detección Facial

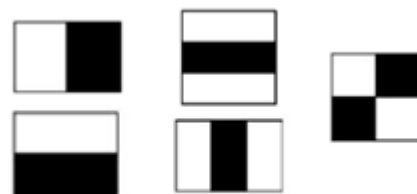
Antes de involucrarse en la tarea de reconocimiento facial, debemos enfrentar un prerequisite indispensable que es la detección del rostro en una imagen. Existen distintos algoritmos que permiten atacar este problema y que reseñaremos a continuación.

Haar-cascade Classifier

Wilson y Fernandez (2006) se refieren a este método de la siguiente manera:

The core basis for Haar classifier object detection is the Haar-like features. These features, rather than using the intensity values of a pixel, use the change in contrast values between adjacent rectangular groups of pixels. The contrast variances between the pixel groups are used to determine relative light and dark areas. Two or three adjacent groups with a relative contrast variance form a Haar-like feature. [La base principal para la detección de objetos del clasificador Haar son las características similares a las de Haar. Estas características, en lugar de utilizar los valores de intensidad de un píxel, utilizan el cambio en los valores de contraste entre grupos de píxeles rectangulares adyacentes. Las variaciones de contraste entre los grupos de píxeles se utilizan para determinar las áreas relativas claras y oscuras. Dos o tres grupos adyacentes con una variación de contraste relativa forman una característica similar a Haar.] (p.128)

Delbiaggio (2017) también hace un estudio recopilatorio respecto a los algoritmos de detección facial, sobre el clasificador de Haar-cascade dice:



The 5 Haar-like features used for detecting faces

Haar-cascade is a method, invented by Viola and Jones (Viola & Jones, 2001), which trains a machine learning for detecting objects in a picture. In this context, it can be used to detect faces. The name of this method is composed of two important words, Haar and Cascade. Haar belongs to Haar-like features

which is a weak classifier and will be used for the face recognition. A weak classifier is a classifier which is only slightly better than a random prediction. A Haar-like feature is a rectangle which is split into two, three or four rectangles. Each rectangle is black or white. [Haar-cascade es un método, inventado por Viola y Jones (Viola & Jones, 2001), que entrena un aprendizaje automático para detectar objetos en una imagen. En este contexto, se puede utilizar para detectar rostros. El nombre de este método se compone de dos palabras importantes, Haar y Cascade. Haar pertenece a características similares a Haar, que es un clasificador débil y se utilizará para el reconocimiento facial. Un clasificador débil es un clasificador que es solo un poco mejor que una predicción aleatoria. Una característica similar a Haar es un rectángulo que se divide en dos, tres o cuatro rectángulos. Cada rectángulo es blanco o negro] (p.6) Delbiaggio (2017), A comparison of facial recognition's algorithms (Figure p.6)

Histogram of Oriented Gradients (HOG)

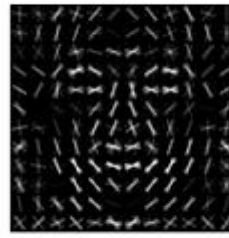
Es otro método para detección de objetos, que puede ser usado también en la tarea de detección de rostros. Delbiaggio (2017) hace una interesante definición de esta técnica:

HOG (Dalal & Triggs, 2005) (Geitgey, 2016) is another method for detecting objects which can also be used for detecting faces. In this case, we will use HOG for detecting any front face in a picture. This method requires an image in grayscale. Each pixel of the image is represented by an integer due to the grayscale. The HOG method compares each pixel with its neighbors. Most of the time, a pixel is

surrounded by eight other pixels. The aim is to find the direction where the picture is getting darker. A white arrow will be drawn to represent this direction. So, the smaller is the number of the pixel then the darker is the pixel. This treatment is done for each pixel of the picture. The strength of this method is that it is not sensitive to a change in luminosity. If a picture is darker, all the pixels will be darker. The arrow representing the direction where it is getting darker will not change in a brighter picture. Indeed, this is not true if only a part of the picture is affected by a change in luminosity, which could be caused, for example, by a lamp. [HOG (Dalal & Triggs, 2005) (Geitgey, 2016) es otro método para detectar objetos que también se puede utilizar para detectar caras. En este caso, usaremos HOG para detectar cualquier cara frontal en una imagen. Este método requiere una imagen en escala de grises. Cada píxel de la imagen está representado por un número entero debido a la escala de grises. El método HOG compara cada píxel con sus vecinos. La mayoría de las veces, un píxel está rodeado por otros ocho píxeles. El objetivo es encontrar la dirección en la que la imagen se oscurece. Se dibujará una flecha blanca para representar esta dirección. Entonces, cuanto menor es el número de píxeles, más oscuro es el píxel. Este tratamiento se realiza para cada píxel de la imagen. El punto fuerte de este método es que no es sensible a cambios de luminosidad. Si una imagen es más oscura, todos los píxeles serán más oscuros. La flecha que representa la dirección en la que se oscurece no cambiará en una imagen más brillante. De hecho, esto no es cierto si solo una parte de la imagen se ve afectada por un cambio en la

luminosidad, que podría ser causado, por ejemplo, por una lámpara.]

This step gives us the shape of the analyzed face in detail, but too many details are caught. The aim is to recognize any face, but too many details can only detect one specific face. Thus, only the relevant directions need to be kept. The next step is to split the pictures into squares of 16x16 pixels. We count how many times each direction has been discovered beforehand, and only one arrow is drawn in the square with the direction which was the most frequently found. This action is done for each block of 16x16 in the picture. This treatment gives a better representation of a general face. All the steps will be performed with a vast number of frontal faces for determining the best pattern for face detection. [Este paso nos da la forma del rostro analizado en detalle, pero se captan demasiados detalles. El objetivo es reconocer cualquier rostro, pero demasiados detalles solo pueden detectar un rostro específico. Por lo tanto, solo deben mantenerse las instrucciones relevantes. El siguiente paso es dividir las imágenes en cuadrados de 16x16 píxeles. Contamos cuántas veces se ha descubierto cada dirección de antemano, y solo se dibuja una flecha en el cuadrado con la dirección que se encontró con más frecuencia. Esta acción se realiza para cada bloque de 16x16 en la imagen. Este tratamiento da una mejor representación de un rostro en general. Todos los pasos se realizarán con una gran cantidad de caras frontales para determinar el mejor patrón de detección de rostros.] (p.7)



Visualization of the HOG detector from the library

Delbiaggio (2017), A comparison of facial recognition's algorithms (Figure p.8)

2.2.2 Preprocesamiento de Imágenes

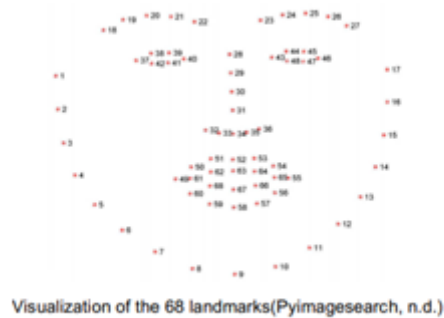
Una vez detectado el rostro en la imagen se requiere un preprocesamiento para que el proceso de reconocimiento facial sea lo más preciso posible. Por ejemplo, Delbiaggio (2017) sostiene lo siguiente:

The next step is to pre-process these faces in order to make the training phase easier and improve the probability to recognize a person correctly. The training data will be standardized. Not all the pictures have the same zoom on the face and have maybe not all the same size. Most of the algorithms for facial recognition require the same size for the entire training set. Pre-processing includes different modifications. First of all, the faces need to be centered in the picture in the same way. The location of the two eyes and the nose is often used as a landmark for centering faces. The aim is to have the eyes at the same level and the nose at the same position for all images. To apply these modifications, the coordinates of the landmarks are needed. For that, it is possible to use a Haar-cascade classifier for detecting nose and eyes. It is also possible to use the facial landmarks detector, which is available inside the dlib library which is based on the work of Kazemi &

Sullivan (Kazemi & Sullivan). The landmark detector has been trained to recognize 68 specific points on a face which are shown in figure 5. This method has been trained with many pictures, which have been manually labeled before for each landmark. [El siguiente paso es preprocesar estas caras para facilitar la fase de entrenamiento y mejorar la probabilidad de reconocer a una persona correctamente. Los datos de entrenamiento estarán estandarizados. No todas las imágenes tienen el mismo zoom en la cara y tal vez tampoco el mismo tamaño. La mayoría de los algoritmos de reconocimiento facial requieren el mismo tamaño para todo el conjunto de entrenamiento. El preprocesamiento incluye diferentes modificaciones. En primer lugar, las caras deben centrarse en la imagen de la misma manera. La ubicación de los dos ojos y la nariz se utiliza a menudo como punto de referencia para centrar caras. El objetivo es tener los ojos al mismo nivel y la nariz en la misma posición para todas las imágenes. Para aplicar estas modificaciones se necesitan las coordenadas de los puntos de referencia. Para eso, es posible utilizar una cascada de clasificación de Haar para detectar nariz y ojos. También es posible utilizar el detector de puntos de referencia faciales, que está disponible dentro de la biblioteca dlib que se basa en el trabajo de Kazemi & Sullivan (Kazemi y Sullivan). El detector de puntos de referencia ha sido entrenado para reconocer 68 puntos específicos en una cara que se muestran en la figura 5. Este método ha sido entrenado con muchas imágenes, que se han etiquetado manualmente antes para cada punto de referencia.] (p.9)

Delbiaggio (2017), A comparison of facial recognition's algorithms (Figure p.9)

2.2.3 Algoritmos de Reconocimiento Facial



Ya sea para la fase de entrenamiento o de reconocimiento, hasta este momento se han cubierto las tareas de detección del rostro dentro de una imagen y el preprocesamiento necesario para aislar las características relevantes sobre las cuales se operará. En este punto abordaremos los algoritmos más conocidos usados para reconocimiento facial.

Eigenfaces

Este algoritmo, creado por Turk y Pentland en 1991, utiliza una aproximación estadística para reconocer un rostro. Esto quiere decir que analiza las características de un rostro y determina mediante un score porcentual la posibilidad de que el rostro consultado sea el mismo que el de la referencia o el conjunto de entrenamiento. En su recopilación Delbiaggio (2017) sostiene lo siguiente:

Eigenfaces (Turk & Pentland, 1991) (Jaiswal, Gwalior, & Gwalior, 2011) (Morizet, Ea, Rossant, Amiel, & Amara, 2006) is a method for performing facial recognition based on a statistical approach. The aim of this method is to extract the principal components which affect the most the variation of the images. This

is a holistic approach, the treatment for predicting a face is based on the entire training set. There is no specific treatment between images from two different classes. A class represents a person. Pre-processed pictures with grayscale are required for training the machine learning. Each pixel of a picture represents one dimension, it means a 96x96 pixels image is represented into $96 \times 96 = 9216$ dimensions. Eigenfaces is based on Principal Component Analysis (PCA) (Turk & Pentland, 1991) (Jaiswal & al., 2011) (Morizet & al., 2006) for reducing the number of dimensions while preserving the most important information. The training part of Eigenfaces is to calculate the eigenvectors and the related eigenvalues of the covariance matrix of the training set. [Eigenfaces (Turk y Pentland, 1991) (Jaiswal, Gwalior y Gwalior, 2011) (Morizet, Ea, Rossant, Amiel y Amara, 2006) es un método para realizar el reconocimiento facial basado en un enfoque estadístico. El objetivo de este método es extraer los componentes principales que afectan más la variación de las imágenes. Este es un enfoque holístico, el tratamiento para predecir una cara se basa en todo el conjunto de entrenamiento. No existe un tratamiento específico entre imágenes de dos clases diferentes. Una clase representa a una persona. Se requieren imágenes preprocesadas con escala de grises para entrenar el aprendizaje automático. Cada píxel de una imagen representa una dimensión, significa que una imagen de 96x96 píxeles se representa en $96 \times 96 = 9216$ dimensiones. Eigenfaces se basa en el análisis de componentes principales (PCA) (Turk & Pentland, 1991) (Jaiswal & al., 2011) (Morizet & al., 2006) por reducir el número

de dimensiones conservando la información más importante. La parte de entrenamiento de Eigenfaces es calcular los autovectores y los autovalores relacionados de la matriz de covarianza del conjunto de entrenamiento.] (p.10)

En este algoritmo se identifican 7 pasos que son: (i) transformar la imagen en una matriz, (ii) adaptar la matriz a un vector, (iii) calcular el promedio de los vectores, (iv) sustraer a cada vector el promedio de todos los vectores, (v) calcular la matriz de covarianza, (vi) calcular los autovectores y los autovalores relacionados; y finalmente, (vii) Ordenar los autovectores.

De los autovectores ordenados se puede identificar que imagen dentro del grupo de entrenamiento está a menor distancia de la imagen de consulta. Esto es explicado por Delbiaggio (2017):

A Euclidean distance can be used to find the closest face. However, it has been proved that the Mahalanobis distance (Turk & Pentland, 1991) is most of the time more accurate. $F(e)$ can be compared to a threshold and if is smaller, we can determine that the face belongs to a person who is not in the training set, thus the image is added to the training set as a new person. Otherwise, the image is used as a new picture for training the recognized person and is also added into the training set with the related label. This algorithm is a constant machine learning and is supposed to become more reliable each time a new test is performed because the size of the training set increases constantly. [Se puede usar una distancia euclidiana para encontrar la cara más cercana. Sin embargo, ha sido probado que la distancia de Mahalanobis (Turk y Pentland, 1991) es la mayoría de

las veces más precisa. $F(e)$ ¹ se puede comparar con un umbral y si es más pequeño, podemos determinar que la cara pertenece a una persona que no está en el conjunto de entrenamiento, por lo que la imagen se agrega al conjunto de entrenamiento como una nueva persona. De lo contrario, la imagen se utiliza como una nueva imagen para entrenar a la persona reconocida y también se agrega al conjunto de entrenamiento con la etiqueta relacionada. Este algoritmo es un aprendizaje automático constante y se supone que se vuelve más confiable cada vez que se usa nuevamente porque el tamaño del conjunto de entrenamiento aumenta constantemente.] (p.14)

Fisherfaces

Este algoritmo es una modificación del algoritmo Eigenfaces, en el sentido de que toma en cuenta el concepto de clases. Eigenfaces, no hace discriminación entre dos imágenes de distinta clase en la etapa de entrenamiento. Para mejorar el proceso de reconocimiento de características Fisherfaces utiliza el método de Análisis Linear Discriminatorio (Jaiswal et. al., 2011) (Morizet et. al., 2006) (Belhumeur et. al., 1997) para establecer diferencias entre imágenes de diferente clase. Esta modificación implica una mejora en la precisión del algoritmo dado que se minimiza la distorsión en el valor de la distancia euclidiana producto de la comparación de imágenes de clase diferente. Al respecto, Delbiaggio (2017) sostiene: “The aim is to minimize the variation within a class compared to the variation between classes. For that 15 (images)² not only the total average of faces is used, but the average per class will also be an essential operation” [El

¹ En el texto original de usa la expresión e_r ; por cuestiones de diagramación se ha cambiado por $F(e)$. En cualquier caso, este valor representa la imagen con menor distancia a la imagen de consulta

² Añadido al texto original para mejorar la comprensión

objetivo es minimizar la variación dentro de una clase en comparación con la variación entre clases. Para esas 15 (imágenes) no solo se usa el promedio total de caras, sino que el promedio por clase también será una operación fundamental] (p.14-15)

LBPH (Local Binary Patterns Histograms)

Este algoritmo fue creado por Ahonen, Hadid y Pietik en 2004 (Delbiaggio, 2017 p.16). Utiliza una aproximación distinta a la de los algoritmos vistos anteriormente. Mientras en los casos anteriores las imágenes son convertidas en matrices primero para ser pasados a vectores unidimensionales, en este caso la imagen es separada en regiones de 3x3 pixeles. Luego el píxel central es comparado contra los 8 pixeles adyacentes, en caso de que el valor del píxel adyacente sea igual o superior al valor del píxel central se le asigna el valor de 1 en una nueva matriz que será usada con fines de cálculo, en caso contrario se asignará el valor de 0. Luego se usará una matriz de las mismas dimensiones en la que se establecen pesos en base 2 (1, 2, 4, 8, 16, 32, 64 y 128). El valor de la zona será calculado por la multiplicación del peso por el valor binario definido en el primer paso. Finalmente, se extrae un histograma con la información de todas las zonas obtenidas de la imagen. El histograma más cercano al conjunto de histogramas del conjunto de entrenamiento será la predicción del algoritmo. A continuación, podemos observar gráficamente cómo se manejan las zonas de la imagen en este algoritmo:

$$\text{LBP} = 1 + 16 + 32 + 128 = \mathbf{177}$$

5	2	9
7	4	4
3	2	3

example

1	0	1
1		1
0	0	0

thresholded

128	64	32
1		16
2	4	8

weights

Delbiaggio (2017), A comparison of facial recognition's algorithms (Figure p.16)

Respecto al proceso de predicción para el reconocimiento de este algoritmo Delbiaggio (2017) dice:

When this process has been completed for each part of the picture, the picture is divided into a certain number of regions. Then, a histogram is extracted from each region and all the histograms are concatenated. For recognizing a face, exactly the same process is performed, and the final histogram is compared to each final histogram in the training data. The label related to the closest histogram is the prediction of the algorithm. As for the hog detector, this algorithm is not sensitive to a variation of luminosity. [Cuando este proceso se ha completado para cada parte de la imagen, la imagen se divide en un cierto número de regiones. Luego, se extrae un histograma de cada región y se concatenan todos los histogramas. Para reconocer una cara, se realiza exactamente el mismo proceso y el histograma final se compara con cada histograma final en los datos de entrenamiento. La etiqueta relacionada con el histograma más cercano es la predicción del algoritmo. En cuanto al método de detección HOG, este algoritmo tampoco es sensible a una variación de luminosidad] (p.16)

Red neuronal convolucional (CNN)

Las redes neuronales son modelos computacionales inspirados en el funcionamiento de las neuronas del cerebro humano. Estos modelos son usados para una variedad de tareas de IA, siendo una de estas tareas el reconocimiento

facial. Se le denomina convolucional a aquella red neuronal donde las neuronas están organizadas de una manera similar a la disposición de las neuronas en la corteza visual del cerebro humano. Al respecto Jianxin Wu (2020) nos dice:

CNNs are useful in a lot of applications, especially in image related tasks. Applications of CNNs include image classification, image semantic segmentation, object detection in images, etc. We will focus on image classification (or categorization) in this chapter. In image categorization, every image has a major object that occupies a large portion of the image. An image is classified into one of the classes based on the identity of its main object—e.g., dog, airplane, bird, etc. [Las CNN son útiles en muchas aplicaciones, especialmente en tareas relacionadas con imágenes. Las aplicaciones de las CNN incluyen clasificación de imágenes, segmentación semántica de imágenes, detección de objetos en imágenes, etc. Nos centraremos en la clasificación de imágenes (o categorización) en este capítulo. En la categorización de imágenes, cada imagen tiene un objeto principal que ocupa una gran parte de la imagen. Una imagen se clasifica en una de las clases según la identidad de su objeto principal, por ejemplo, perro, avión, pájaro, etc.] (p.2-3)

Delbiaggio (2017) también incluye este tipo de red neuronal en su recopilación de algoritmos y nos indica:

Using a convolutional neural network (CNN) (CS231n) (Deshpande, 2016c) (Deshpande, 2016a) (Deshpande, 2016b) is another way to perform face recognition. CNN has an architecture that enables it to use 2d pictures as inputs. A CNN consists of several layers called hidden layers. The layers are composed

of several neurons. A neuron has specific weight and receives an input. After applying its logic to the input, it will provide an output. The input of the first layer is a picture of a face. The output of the last layer is the predicted class which is the person. [El uso de una red neuronal convolucional (CNN) (CS231n) (Deshpande, 2016c) (Deshpande, 2016a) (Deshpande, 2016b) es otra forma de realizar el reconocimiento facial. CNN tiene una arquitectura que le permite utilizar imágenes 2d como entradas. Una CNN consta de varias capas llamadas capas ocultas. Las capas están compuestas por varias neuronas. Una neurona tiene un peso específico y recibe una entrada. Después de aplicar su lógica a la entrada, proporcionará una salida. La entrada de la primera capa es una imagen de una cara. La salida de la última capa es la clase predicha que es la persona.] (p.18)

2.2.4 Software de Reconocimiento Facial de Código Abierto OpenFace

OpenFace es una implementación de software basada en Python y Torch que utiliza CNN para reconocimiento facial (B. Amos, B. Ludwiczuk, M. Satyanarayanan, "Openface: A general-purpose face recognition library with mobile applications".

<https://cmusatyalab.github.io/openface/#openface>). Se basa en la investigación plasmada en el paper

OpenCV

face-api.js

2.3. Definiciones conceptuales

- **Software de Reconocimiento Facial de Código Abierto OpenFace.-** es una implementación de software basada en Python

y Torch que utiliza CNN para reconocimiento facial (B. Amos, B. Ludwiczuk, M. Satyanarayanan, "Openface: A general-purpose face recognition library with mobile applications". <https://cmusatyalab.github.io/openface/#openface>). Se basa en la investigación plasmada en el paper OpenCV face-api.js

- **Eigenfaces.**- “Este algoritmo, una aproximación estadística para reconocer un rostro. Esto quiere decir que analiza las características de un rostro y determina mediante un score porcentual la posibilidad de que el rostro consultado sea el mismo que el de la referencia o el conjunto de entrenamiento”(Turk y Pentland ,1991).
- **FaceLogin.**- Instrumento utilizado para esta investigación fue el sistema de reconocimiento facial desarrollado como prototipo para el presente estudio. Su desempeño fue medido en tiempo real y en condiciones de producción durante el examen de admisión 2020 en la Universidad de Huánuco.
- **Red neuronal convolucional (CNN).**- Las CNN son "útiles en muchas aplicaciones, especialmente en tareas relacionadas con imágenes. Las aplicaciones de las CNN incluyen clasificación de imágenes, segmentación semántica de imágenes, detección de objetos en imágenes, etc. Nos centraremos en la clasificación de imágenes (o categorización) en este capítulo. En la categorización de imágenes, cada imagen tiene un objeto principal que ocupa una gran parte de la imagen. Una imagen se clasifica en una de las clases según la identidad de su objeto principal, por ejemplo, perro, avión, pájaro, etc.(Jianxin Wu, 2020.p.2-3)
- **Plagio.**- El delito de plagio se encuentra tipificado en el artículo 219 del Código penal, modificado por el artículo 1 de la Ley N ° 28289. Al hablar de propiedad intelectual se hace referencia a un amplio espectro de derechos de distinta naturaleza: mientras algunos se originan en un acto de creación intelectual y son reconocidos para estimular y recompensar la misma.
- **Sistema de reconocimiento facial.**- “sin entrenamiento” que funciona sobre un entorno web, usando como tecnología de backend

la plataforma .Net Core y como frontend utiliza Angular. La razón de adoptar un prototipo de estas características es la de poder atender a un gran número de usuarios disminuyendo la necesidad de acciones previas en la instalación del postulante o la utilización de software en entornos variantes y con poca certidumbre respecto a las condiciones de software y hardware de los postulantes.

- **Suplantación. Virtual.** - Es una actividad malintencionada que consiste en hacerse pasar por otra persona por diversos motivos, como para alcanzar mayor puntaje en el examen de admisión virtual y cometer fraude académico.

2.4. Sistema de Hipótesis

H1: La implementación de un sistema con reconocimiento facial permite reducir la posibilidad de suplantación y plagio en el examen de admisión virtual en la Universidad de Huánuco, 2020.

H0: La implementación de un sistema con reconocimiento facial no permite reducir la posibilidad de suplantación y plagio en el examen de admisión virtual en la Universidad de Huánuco, 2020.

2.5. Sistema de variables

- **Variable independiente**

Implementación de un sistema de reconocimiento facial

- **Variable dependiente**

.

Control de casos de suplantación y plagio

2.6. Operacionalización de las Variables

VARIABLE	DIMENSIONES	INDICADORES
VARIABLE INDEPENDIENTE Implementación de un sistema de reconocimiento facial.	Capacitación	Nivel de capacitación de aplicadores de prueba
	Funcional	Nivel de implementación de control facial.
	Confiabilidad	Porcentaje de suplantación.
	Confidencialidad	Criticidad de vulnerabilidad en la integridad
VARIABLE DEPENDIENTE Control de casos de suplantación y plagio	Reconocimiento “sin entrenamiento”	Tecnología de backend la plataforma .Net Core y como frontend - Angular

CAPITULO III

MARCO METODOLÓGICO

3.1. Tipo de investigación

La presente investigación es de tipo aplicada, dado que busca la generación de conocimiento mediante la aplicación de la tecnología de reconocimiento facial en un problema de la realidad y en una institución específica. Se trata de una investigación cuantitativa, de diseño descriptivo y de método hipotético deductivo. Por su temporalidad es una investigación transversal, dado que todos los participantes del estudio interactúan con la plataforma en un momento específico.

3.1.1 Enfoque

La investigación por su naturaleza es de un enfoque cuantitativo ya que las variables son contrastadas empleando métodos estadísticos y la interpretación de datos. (Sánchez y Meza, 2017).

3.1.2 Alcance o nivel

Nivel descriptivo, dado que, si bien se utiliza un prototipo, el mismo no se modifica o se restringe a ningún postulante, sino que se utiliza para todos los participantes del estudio sin distinción. Mejor dicho, no hay control de variables

3.1.3 Diseño.

El diseño de esta investigación es no experimental trasversal, (Carrasco, 2006) afirma que, este diseño se utiliza para realizar estudios de hechos y fenómenos de la realidad, en un momento determinado del tiempo.

3.2. Población y muestra

3.2.1. Población

La población de esta investigación lo constituyen todos los postulantes a los exámenes de admisión virtual de la Universidad de Huánuco.

3.2.2. Muestra

Se utilizó la muestra probabilística, muestreo aleatorio simple lo cual está compuesta por un total de 1,252 postulantes del examen de admisión para el año 2020.

3.3. Técnicas e instrumentos de recolección de datos

Para participar del estudio el postulante debe registrar una imagen previamente durante el proceso de inscripción. Los parámetros requeridos para asegurar el correcto funcionamiento del prototipo son de tipo técnico y forman parte de los requisitos establecidos por la Oficina Central de Admisión para la realización del examen de admisión virtual 2020, y son los siguientes (requisitos mínimos): 1. Computador Core i3 de 2da generación con 4GB RAM
Cámara web con resolución mínima de 1MP.
Conexión a internet con ancho de banda mínimo de 4MB

3.3. Técnicas para el procesamiento y análisis de la información

El instrumento principal utilizado para esta investigación fue el sistema de reconocimiento facial FaceLogin desarrollado como prototipo para el presente estudio. Su desempeño fue medido en tiempo real y en condiciones de producción durante el examen de admisión 2020 en la Universidad de Huánuco.

El sistema diseñado es un sistema de reconocimiento “sin entrenamiento” que funciona sobre un entorno web, usando como tecnología de backend la plataforma .Net Core y como frontend utiliza Angular. La razón de adoptar un prototipo de estas características es la de poder atender a un gran número de usuarios disminuyendo la necesidad de acciones previas en la instalación del postulante o la utilización de software en entornos variantes y con poca certidumbre respecto a las condiciones de software y hardware de los postulantes.

CAPITULO IV

RESULTADOS

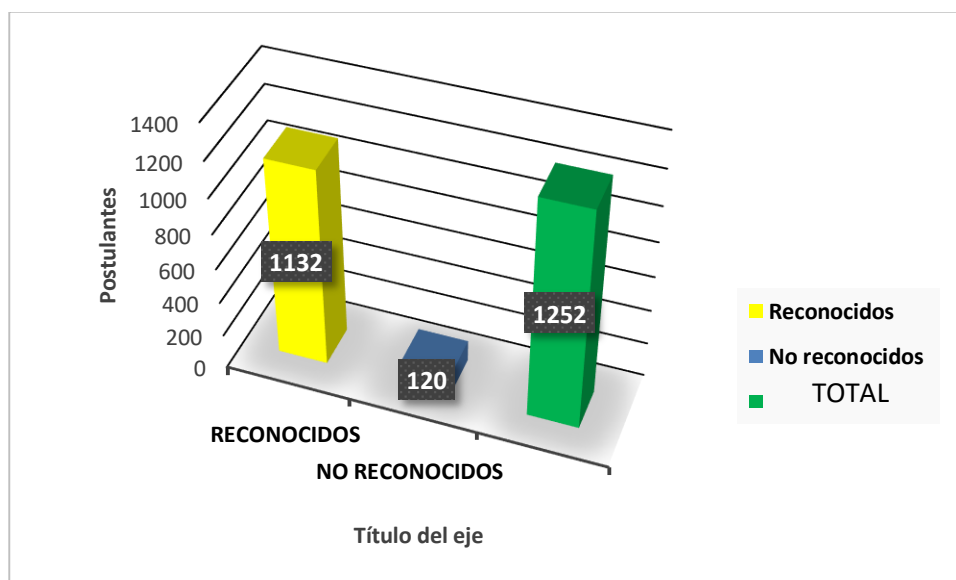
4.1. Descripción de los resultados

Durante el proceso de admisión virtual 2020 en la Universidad de Huánuco se ejecutó, de manera complementaria al control humano de docentes asignados a las salas virtuales donde los postulantes rendían examen, el control biométrico por reconocimiento facial. Los resultados obtenidos fueron los siguientes:

Tabla N° 1 Resultados del proceso de reconocimiento de Reconocimiento de postulantes

	CANTIDAD	PORCENTAJE
Reconocidos	1132	90.42%
No reconocidos	120	9.58%
TOTAL POSTULANTES	1252	100.00%

Fuente: Sistema de Reconocimiento Facial FaceLogin



Fuente: Datos de la tabla N° 1

Elaboración: Propia

Figura N° 1 Proceso de reconocimiento de reconocimiento de postulantes - Examen admisión UDH

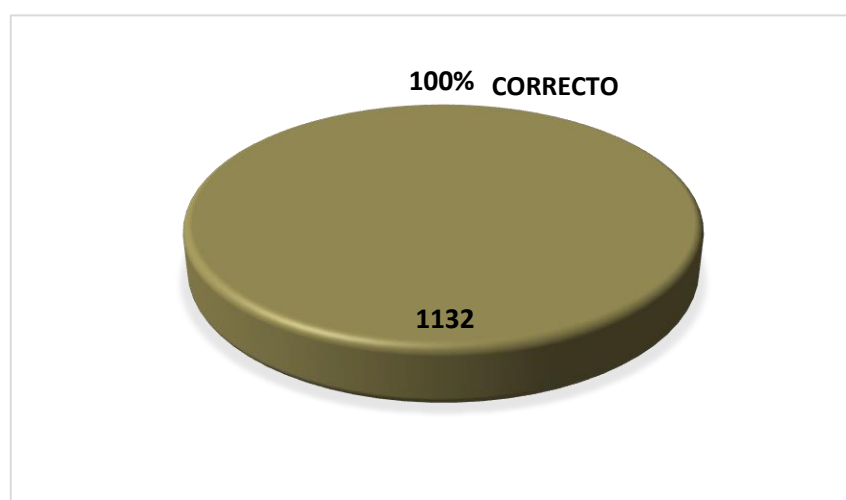
Interpretación

De la tabla y figura adjunta se evidencia que el sistema facial facelogin reconoció a 1132 postulantes lo que corresponde al 90.42%, asimismo existe 120 postulantes que no fueron reconocidos lo que se interpreta el 9.58% del total de la muestra.

Tabla N° 2 Pasos de reconocimiento positivo erróneo

	CANTIDAD	PORCENTAJE
Correcto	1132	100.00%
Falso positivo	0	0.00%
TOTAL CASOS RECONOCIDOS	1132	100.00%

Fuente: Sistema de Reconocimiento Facial FaceLogin



Fuente: Datos de la tabla N° 2

Elaboración: Propia

Figura N° 2 Pasos de reconocimiento positivo erróneo

Interpretación

La tabla y figura evidencia que no existió falso positivo erróneo.

Tabla N° 3 Casos de no reconocimiento detectados como fraude

	CANTIDAD	PORCENTAJE
Error Sistema	120	100.00%
Fraude	0	0.00%
TOTAL CASOS NO RECONOCIDOS	120	100.00%

Fuente: Sistema de Reconocimiento Facial FaceLogin

Interpretación

La tabla demuestra que el sistema de reconocimiento facial facelogin , funciona correctamente en consecuencia que no existió fraude 0%.

4.2. Análisis de los resultados

El primer dato relevante de la presente investigación es el alto porcentaje de reconocimiento obtenido por el sistema, aún cuando se trata de su primera prueba en un entorno de producción real y con altos niveles tanto de concurrencia como de variabilidad de las condiciones ambientales de los participantes. Estamos hablando de que en el 90.42% de los casos obtuvimos un resultado de reconocimiento positivo.

Para todos los casos positivos se ha emitido un reporte que se adjunta como anexo de la presente investigación y podemos observar la capacidad del algoritmo para obtener buenos resultados a pesar de los cambios de iluminación, posición e incluso de la inclusión de elementos ajenos a la foto de control.

Tabla N° 4 Casos de reconocimiento exitoso

FOTO DE CONTROL	FOTO DEL EXAMEN	NIVEL DE CONFIANZA
		0.91431
		0.79602
		0.84494
		0.92602
		0.92619

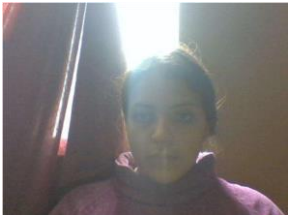
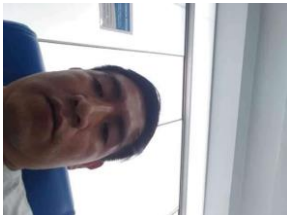
Fuente: Sistema de Reconocimiento Facial FaceLogin

Como puede observarse en las imágenes de la tabla N° 4, el sistema permite identificar a los postulantes incluso en condiciones en las cuales existen variaciones significativas sobre la imagen de control (imagen de la izquierda).

Con la ayuda de los docentes controladores se revisó la totalidad del reporte, llegando a la certeza de que no hubo falsos positivos en el reconocimiento de postulantes, tal como se puede observar en la Tabla 2. Esto nos indica que la confiabilidad de los resultados entregados por el sistema es muy alta.

En 120 casos el sistema no pudo reconocer correctamente a los postulantes. De la verificación del reporte de postulantes no reconocidos se determinó que no fueron casos de fraude, sino que el sistema no tuvo éxito al reconocerlos. El personal encargado del control de los entornos virtuales verificó con el reporte en línea y la herramienta de videoconferencia Google Meet, la identidad de los postulantes que no superaron el proceso de reconocimiento facial. Ejemplos de estos inconvenientes pueden ser observados en la tabla N° 5.

Tabla N° 5 Casos de reconocimiento fallido

FOTO DE CONTROL	FOTO DEL EXAMEN	NIVEL DE CONFIANZA
		0
		0
		0
		0
		0

Fuente: Sistema de Reconocimiento Facial FaceLogin

Entre los casos de reconocimiento fallido, del análisis del reporte, se han identificado las causas del error y las podemos encontrar en la Tabla N° 4.

Tabla N° 6 Causas de errores en el reconocimiento facial

	CANTIDAD	PORCENTAJE
Mala calidad de imagen	66	55.00%
Mala Iluminación	34	28.33%
Ningún rostro en la Imagen	15	12.50%
Más de una persona en La Imagen	5	4.17%
TOTAL CASOS NO RECONOCIDOS	120	100.00%

Fuente: Sistema de Reconocimiento Facial FaceLogin

Es interesante observar que el 83.33% de los casos se refieren a problemas con la calidad de las imágenes o mala iluminación al momento de las tomas. Los demás casos, 16.67%, se deben a que el postulante no se encontraba frente a la cámara al momento del control de identidad o que una segunda persona estuvo en la toma. Durante el examen estos casos fueron supervisados por los controladores de examen y en ningún caso se detectó intento de fraude. Todos los casos de error pueden superarse con un proceso de inducción adicional para evitar errores en el momento del control de identidad y una mejor selección, por parte de los postulantes, del ambiente en el cual se desarrollará el examen.

Ahora, desde el punto de vista de nuestra hipótesis, podemos determinar que la aplicación de este sistema si ayuda a prevenir la suplantación y el fraude. La observación de los datos nos indica que la tasa de reconocimiento es alta, lo que les permite a los controladores de examen concentrar su atención sobre 120 postulantes del total de 1252 que participaron del experimento. De los datos de la Tabla 1, podemos asumir que el sistema ayuda con el 90.42% de los reconocimientos, mientras en el 9.58% de los casos se requiere el apoyo de los controladores.

Es decir, la utilización de esta tecnología permite atender un número significativo de usuarios, minimizando la cantidad de controladores humanos necesarios para llevar adelante un proceso de evaluación masivo como lo es un examen de admisión.

Esto es de vital importancia en la actualidad. La pandemia por COVID-19 nos ha obligado a replantear las formas tradicionales en que nos veníamos relacionando entre los que componemos de la sociedad. La tecnología ha cobrado vital importancia en este proceso, y más allá de que superemos esta época difícil nos ha marcado los desafíos y las tareas que tenemos que cumplir en el futuro. La oportunidad de reducir la brecha digital ha sido tomada y se ha logrado que seres humanos de todas las generaciones, en todo el mundo, se vuelquen a los medios digitales para dotarse de las herramientas que les permitan continuar produciendo en esta nueva normalidad.

4.3. Prueba de Hipótesis

H1: La implementación de un sistema con reconocimiento facial permite reducir la posibilidad de suplantación y plagio en el examen de admisión virtual en la Universidad de Huánuco, 2020.

H0: La implementación de un sistema con reconocimiento facial no permite reducir la posibilidad de suplantación y plagio en el examen de admisión virtual en la Universidad de Huánuco, 2020.

Conclusión

La aplicación de este sistema si ayuda a prevenir la suplantación y el fraude. La observación de los datos nos indica que la tasa de reconocimiento es alta, lo que les permite a los controladores de examen concentrar su atención sobre 120 postulantes del total de 1252 que participaron del experimento. De los datos de la Tabla 1, podemos asumir que el sistema ayuda con el 90.42% de los reconocimientos, mientras en el 9.58% de los casos se requiere el apoyo de los controladores. Es decir que se acepta la hipótesis de la investigación la implementación de un sistema con reconocimiento facial permite reducir la posibilidad de

suplantación y plagio en el examen de admisión virtual en la Universidad de Huánuco, 2020.

Asimismo, la utilización de esta tecnología permite atender un número significativo de usuarios, minimizando la cantidad de controladores humanos necesarios para llevar adelante un proceso de evaluación masivo como lo es un examen de admisión.

CAPITULO V

DISCUSIÓN DE RESULTADOS

La pandemia ha evidenciado las brechas que existen en términos de conectividad y acceso a la tecnología en nuestro país. La virtualidad ha implicado la aparición de nuevos desafíos para la educación, los cuales no estábamos preparados, tanto docentes como alumnos han tenido que cambiar el aula, la pizarra y el proyector; por el computador conectado a Internet desde el lugar que mejor puedan adaptar. Un problema que ha sido transversal, a todos los niveles de educación, incluyendo el superior universitario, ha sido el tema de la evaluación. No solo se presentan desafíos desde la pertinencia y efectividad de la evaluación, sino desde la perspectiva de su transparencia.

En ese sentido el presente estudio, busca desarrollar un sistema tecnológico, producto de software, para reducir la incertidumbre de los docentes respecto a la transparencia del examen de admisión virtual en la Universidad de Huánuco. Los resultados demuestran que efectivamente el sistema de reconocimiento facial ayudó de manera significativa a prevenir la suplantación y el fraude en el examen de admisión 2020 de la Universidad de Huánuco, dado que contribuyó a minimizar la carga de verificación sobre los controladores humanos en un 90%, estos resultados coinciden con los estudios, de Sucianna et. al. (2018) donde proponen un método para la autenticación usando un método de detección y reconocimiento facial para evitar la suplantación en la educación en línea especialmente durante los exámenes. En este planteamiento el reconocimiento facial es utilizado para autenticar el acceso del alumno al entorno virtual. Asimismo, la investigación determina que la aplicación de este sistema si ayuda a prevenir la suplantación y el fraude. La observación de los datos nos indica que la tasa de reconocimiento es alta, lo que les permite a los controladores de examen concentrar su atención sobre 120 postulantes del total de 1252 que participaron del experimento. De los datos de la Tabla 1, podemos asumir que el sistema ayuda con el 90.42% de los

reconocimientos, mientras en el 9.58% de los casos se requiere el apoyo de los controladores. Es decir, la utilización de esta tecnología permite atender un número significativo de usuarios, minimizando la cantidad de controladores humanos necesarios para llevar adelante un proceso de evaluación masivo como lo es un examen de admisión. Aspectos que se relacionan con Gianni et. al. (2017), cuando señala que existe la necesidad de implementar sistemas de autenticación que permitan el prevenir el plagio y la suplantación para evaluaciones, las cuales permitirán identificar la transparencia de las evaluaciones que suelen darse en los centros de enseñanza superior, así tratar de controlar el fraude académico y que este sistema permite identificar estos casos, que es de vital importancia en la actualidad.

La pandemia por COVID-19 nos ha obligado a replantear las formas tradicionales de enseñanza, la tecnología ha cobrado vital importancia en este proceso, y más allá de que superemos esta época difícil nos ha marcado los desafíos y las tareas que tenemos que cumplir en el futuro en la educación adaptado a la virtualidad.

CONCLUSIONES

- El sistema de reconocimiento facial ayudó a prevenir la suplantación y el fraude en el examen de admisión 2020 de la Universidad de Huánuco dado que contribuyó a minimizar la carga de verificación sobre los controladores humanos en un 90%.
- El prototipo con una estrategia “sin entrenamiento” y sobre una plataforma web permitió alcanzar con mínimo esfuerzo, hacia la infraestructura del postulante, el objetivo de verificación biométrica para el examen de admisión virtual 2020 de la Universidad de Huánuco.
- La experiencia puede extenderse a los exámenes de medio curso, fin de curso y fin de carrera en la Universidad de Huánuco.
- La plataforma puede portarse para servir como un sistema de identificación multipropósito. Ejemplos son el voto electrónico, reuniones de directorio, trámites judiciales, etc.

RECOMENDACIONES

- El sistema se puede mejorar con inducción a los postulantes en posteriores iteraciones del examen de admisión en la universidad de Huánuco.
- Las clases presenciales han tenido que migrar a clases en línea como consecuencia del COVID 19, por ello se recomienda el uso del sistema de reconocimiento facial para la detección de suplantación en exámenes, clases virtuales y actividades educativas de forma virtual.

REFERENCIAS BIBLIOGRÁFICAS

- Ayvaz Uğur, Gürüler Hüseyin, Devrim Mehmet Osman (2017). Use Of Facial Emotion Recognition In E-Learning Systems. Information Technologies and Learning Tools. Vol. 60(4). 95-104.
- B. Amos, B. Ludwiczuk, M. Satyanarayanan, "Openface: A general-purpose face recognition library with mobile applications," CMU-CS-16-118, CMU School of Computer Science, Tech. Rep., 2016.
- Balraj E. y Dr. T. Abirami (2020). A Multibiometric Authentication System Using Fusion Level Techniques. International Journal Of Scientific & Technology Research. Vol. 9(1). 3332-3335
- Belhumeur, P. N., Hespanha, J. P., & Kriegman, D. J. (1997). Eigenfaces vs . Fisherfaces: Recognition Using Class Specific Linear Projection, 19(7), 711–720.
- Carrasco, S. 2006. Metodología de la investigación científica: Pautas metodológicas para diseñar y elaborar el proyecto de investigación. Lima, Perú, San Marcos. 474 p.
- Delbiaggio Nicolas (2017). A comparison of facial recognition's algorithms. Bachelor's Thesis Degree Programme in BIT. 1-39. Disponible en: <https://core.ac.uk/download/pdf/84801048.pdf>
- Fayyumi, A., &Zarrad, A. (2014). Novel Solution Based on Face Recognition to Address Identity Theft and Cheating in Online Examination Systems. Advances in Internet of Things, Vol. 4(2), 5-12.
- Gianni F., M. Mirko, and B. Ludovico (2017). "A multi-biometric system for continuous student authentication in e-learning platforms," Pattern Recognit. Lett. Vol. 0. 1-10
- Guillén-Gámez Francisco D. (2017). Biometrics and education: a review about facial authentication software for the identification and verification of

students who use virtual learning platform (LMS). *Advances in Educational Technology and Psychology*. 1-8

Instituto Internacional de la UNESCO para la Educación Superior (IESALC) (2020). COVID-19 y educación superior: De los efectos inmediatos al día después. Análisis de impactos, respuestas políticas y recomendaciones. UNESCO. Disponible en: <http://www.iesalc.unesco.org/wp-content/uploads/2020/04/COVID-19-060420-ES-2.pdf>

Jaiswal, S., Gwalior, M. I. T. S., & Gwalior, M. I. T. S. (2011). Comparison between face recognition algorithm-eigenfaces, fisherfaces and elastic bunch graph matching, 2(7), 187–193.

Jianxin Wu (2020). Convolutional neural networks. National Key Lab for Novel Software Technology. Nanjing University, China. 1-35

Kalikova, J., Koukol, M., & Krcal, J. (2015). User authentication system for testing students in computer sciences subjects. In *The 4th International Symposium on Next-Generation Electronics (ISNE 2015)*, (pp. 1-4). IEEE.

Morizet, N., Ea, T., Rossant, F., Amiel, F. D. R., & Amara, A. (2006). Revue des algorithmes PCA, LDA et EBGM utilisés en reconnaissance 2D du visage pour la biométrie, 13.

Owayjan, M., Dergham, A., Haber, G., Fakh, N., Hamoush, A., & Abdo, E. (2015). Face Recognition Security System. In *New Trends in Networking, Computing, E-learning, Systems Sciences, and Engineering* (pp. 343-348). Springer International Publishing.

Penteado Bruno Elias y Marana Aparecido Nilceu (2009). A Video-Based Biometric Authentication for e-Learning Web Applications. *International Conference on Enterprise Information Systems*. 770-779

Sucianna Ghadati Rabiha, Aditya Kurniawan, Jurike Moniaga, Daud Iqram Wahyudi, Eric Wilson, Sasmoko (2018). Face Detection and Recognition Based E-Learning for Students Authentication: Study Literature Review.

Proceedings of 2018 International Conference on Information Management and Technology, ICIMTech 2018. Article N° 8528088. 472-476

SUNEDU © Superintendencia Nacional de Educación Superior Universitaria (2020). II Informe bienal sobre la realidad universitaria en el Perú. Superintendencia Nacional de Educación Superior Universitaria. Disponible en: https://cdn.www.gob.pe/uploads/document/file/1230044/INFORME_BIENAL-2020_compressed.pdf

SUNEDU © Superintendencia Nacional de Educación Superior Universitaria (2020). II RESOLUCIÓN DEL CONSEJO DIRECTIVO N° 039-2020-SUNEDU-CD. Superintendencia Nacional de Educación Superior Universitaria. Disponible en: <https://busquedas.elperuano.pe/download/url/aprueban-los-criterios-para-la-supervision-de-la-adaptacion-resolucion-n-039-2020-sunedu-cd-1865206-1>

Turk, M., & Pentland, A. (1991). Eigenfaces for Face Detection / Recognition. Journal of Cognitive Neuroscience, 3(1), 1–11. <https://doi.org/10.1162/jocn.1991.3.1.71>

Vincent Termini y Franklin Hayes (2014). Student Identity Authentication Tools And Live Proctoring In Accordance With Regulations To Reduce Financial Aid Fraud Liability. Online Learning Consortium. https://secure.onlinelearningconsortium.org/effective_practices/student-identity-authentication-tools-and-live-proctoring-accordance-regulations

Wilson, P. I., & Fernandez, J. (2006). Facial Feature Detection Using Haar Classifiers. Journal of Computing Sciences in Colleges, Vol. 21(4), 127–133. <https://doi.org/10.1109/CVPR.2001.990517>

ANEXOS

MATRIZ DE CONSISTENCIA

“SISTEMA DE RECONOCIMIENTO FACIAL EN LÍNEA PARA PREVENIR LA SUPLANTACIÓN Y EL PLAGIO EN EL EXAMEN DE ADMISIÓN VIRTUAL EN LA UNIVERSIDAD DE HUÁNUCO 2020”

PROBLEMA	OBJETIVO	HIPÓTESIS	VARIABLES	METODOLOGÍA
¿En qué medida un sistema con reconocimiento facial permite reducir la posibilidad de suplantación y plagio en el examen de admisión virtual en la Universidad de Huánuco, 2020?	OG: Desarrollar un sistema con reconocimiento facial que permita reducir la posibilidad de suplantación y plagio en el examen de admisión virtual en la Universidad de Huánuco, 2020. OE1: Seleccionar un entorno y marco de desarrollo de código abierto para la construcción del prototipo OE2: Desarrollar un prototipo funcional para demostrar la confiabilidad de la propuesta OE3: Reducir los intentos de suplantación y plagio en la evaluación en línea de la Universidad de Huánuco OE4: Identificar los campos de acción adicionales en los que se podría utilizar este prototipo.	H1: La implementación de un sistema con reconocimiento facial permite reducir la posibilidad de suplantación y plagio en el examen de admisión virtual en la Universidad de Huánuco, 2020 H0: La implementación de un sistema con reconocimiento facial no permite reducir la posibilidad de suplantación y plagio en el examen de admisión virtual en la Universidad de Huánuco, 2020	Dependiente (Y): Y: Control de casos de suplantación y plagio Independiente (X_n): Implementación de un sistema de reconocimiento facial	Tipo: Aplicada Enfoque: Cuantitativo Nivel o alcance: Descriptivo Diseño de la investigación: No experimental trasversal

Fuente: Elaboración propia.