Francisco David Guillén Gámez[1] y Javier Bravo Agapito[2]

Autenticación facial como soporte extra en los entornos virtuales de aprendizaje para evitar el fraude académico

Extracto:

Actualmente, tanto los profesores como los estudiantes se están adaptando a las nuevas tecnologías que nos ofrece el siglo XXI. En el caso de los profesores, esta adaptación es mayor. Ya existe una necesidad de adaptar la enseñanza a los nuevos ambientes tecnológicos, estilos de vida y hábitos. Una de las posibilidades que ofrecen las nuevas tecnologías de la información y la comunicación (TIC) es proporcionar entornos de aprendizaje virtuales, flexibilizando el aprendizaje, permitiendo administrar y evaluar diferentes actividades de un proceso de aprendizaje *e-learning*.

A pesar de los avances producidos en el campo del *e-learning*, existe un número muy reducido de trabajos que permitan, mediante un mecanismo adecuado, la identificación correcta del alumnado cuando realiza sus actividades *on-line* con el objetivo de disminuir el número de engaños que se producen en estos sistemas. Si bien es cierto que los actuales sistemas virtuales de aprendizaje incluyen herramientas para la autenticación de los usuarios, estas herramientas solo verifican la identidad del usuario en el momento de inicio de sesión, normalmente, a través de un nombre de usuario y una contraseña, pero esta autenticación no garantiza que quien ha iniciado la sesión sea quien dice ser.

Ante este problema, el uso de un *software* de autenticación facial en las actividades en línea que tiene que hacer el alumnado puede permitir identificar y prevenir a aquellos que intentan engañar al sistema. Este trabajo propone un mecanismo o técnica que permita garantizar el ingreso de estudiantes legítimos en plataformas de teleaprendizaje durante todo el proceso de aprendizaje, es decir, garantiza que el alumnado sea realmente quien dice ser por medio de un *software* de reconocimiento facial llamado Smowl.

Palabras claves: *e-learning*, Moodle, autenticación facial, aprendizaje *on-line*.

Sumario

Fecha de entrada: 05-11-2015
Fecha de aceptación: 05-12-2015

[1] F. D. Guillén Gámez, profesor de la Universidad a Distancia de Madrid (udima).
[2] J. Bravo Agapito, profesor doctor de la Escuela de Ciencias Técnicas e Ingeniería de la Universidad a Distancia de Madrid (udima).

Facial authentication as an extra support in virtual learning environments to avoid academic fraud

Abstract:

Currently, both teachers and students are adapting themselves to the new technologies offered by the XXI century. In the case of teachers, this adaptation is greater since there is a need to adapt learning to new technologies, lifestyles and habits. One of the possibilities that information and communication technologies (ICT) offer us is to provide learning management systems, with flexible learning, that allows us to manage and evaluate different activities of an e-learning process.

Despite the progress made in the field of e-learning, there is a very low number of works that allow through proper mechanisms to a correct identification of students when they do their on-line activities to prevent cheating. Although current learning management systems include tools for user authentication, they only verify the user's identity at the time of login through a username and password, but it does not certify that it is the correct student.

Against this trouble, the use of facial authentication software in on-line activities which students have to do, allows us to identify and prevent those students who might cheat. This research project seeks to propose a mechanism or technique to ensure the correct access to the student within a learning platform, that is to say, the student is the one who really is, through a facial recognition software called Smowl.

Keywords: e-learning, Moodle, facial authentication, on-line e-learning.

1. INTRODUCCIÓN

La Ley Orgánica de Educación (LOE)[3] está haciendo un gran hincapié en el ámbito de las TIC, a la formación del profesorado y a la infraestructura de los centros educativos. Las TIC ofrecen un amplio rango de medios para poder acceder remotamente, y de manera virtual, desde cualquier lugar del planeta a internet, permitiendo la comunicación síncrona y a bajo coste (Lockwood, 2013). Sin embargo, dado que internet es una red pública, se debe garantizar la seguridad del alumnado (Etzioni, 2008).

La autenticación correcta de un estudiante es un requisito fundamental en un *learning management system* (LMS), pues si algún tercero intenta ingresar usurpando la identidad de un alumno autorizado, puede comprometer la seguridad de todo el sistema (Henríquez, 2014).

En este sentido, existen diferentes tecnologías para verificar la identidad de los usuarios, y uno de esos métodos biométricos que está ocupando un gran peso en los últimos años es la autenticación facial (Subban y Mankame, 2014).

[3] Ley Orgánica 2/2006, de 3 de mayo, de Educación.

2. CONCEPTO Y CARACTERÍSTICAS

La **biometría** se define como la ciencia que estudia las características físicas, químicas y conductuales de un individuo, para que este pueda ser identificado, y donde el reconocimiento es totalmente personal e intransferible (Sayed y Jradi, 2014). Para realizar este proceso, no son necesarias llaves, tarjetas de identificación, claves personales o cualquier otro dispositivo que se deba llevar con uno mismo. Se trata de un proceso similar al que habitualmente realiza el ser humano reconociendo e identificando a otras personas por su aspecto físico, su voz y su forma de andar, entre otras características (García-Hernández y Paredes, 2005).

Por su parte, un sistema de reconocimiento facial es un *software* dirigido por un computador para identificar de forma automática a una persona en una imagen digital mediante la comparación de determinadas características faciales (Jain, Flynn y Ross, 2008).

Noguera (2012) afirma que este tipo de autenticación es un método pasivo y no invasivo, ya que es una característica común de cualquier ser humano y que no requiere de un *software* especial para la captura de fotografías debido a que solo es necesario tener una cámara web (dispositivo electrónico con un coste relativamente bajo para su adquisición y con el valor añadido de ser algo común que los computadores portátiles lo incorporan habitualmente).

El reconocimiento facial requiere de tres etapas:

- La detección del rostro en una fotografía.
- La extracción de las características faciales.
- La identificación y/o verificación de la cara mediante la clasificación de las características. En la identificación, el sistema proporciona la identidad de la persona, mientras que en la verificación confirma o rechaza esta.

El reconocimiento facial requiere de tres etapas:

- **La detección del rostro en una fotografía.**
- **La extracción de las características faciales.**
- **La identificación y/o verificación de la cara mediante la clasificación de las características.**

3. AVANCES EN EL USO DE LA AUTENTICACIÓN FACIAL EN EL ÁMBITO EDUCATIVO

El reconocimiento facial es una de las tecnologías más recientes, que se está popularizando gracias a la gran cantidad de aplicaciones que ofrece, siendo una de estas aplicaciones en la educación a distancia.

Por ejemplo, con el fin de poder monitorizar la asistencia de los alumnos a las clases, Dehnavi y Fard (2011) presentaron un sistema para comprobar que los estudiantes estaban realmente asistiendo a las clases virtuales. Los resultados mostraron que se necesita un nivel muy bajo de colaboración de los estudiantes al ser un sistema pasivo, permitiendo llevar a cabo un seguimiento con mayor precisión y más completo. En la misma línea de este trabajo, Kalikova, Koukol y Krcal (2015) desarrollaron un sistema biométrico llamado «Biotest» con el fin de identificar repetidamente a los alumnos durante los exámenes y pruebas en intervalos aleatorios. A través de este *software*, el profesor ve si la identificación de un estudiante fue positiva. Si la identidad de un estudiante no se verifica positivamente en tres ocasiones, el *software* enviará un aviso al profesor.

Acorde a estas investigaciones, González-Agulla et ál. (2010) propusieron una solución para obtener registros fiables de sesión de estudiantes en un LMS (Moodle). El objetivo que buscaban era garantizar que el estudiante que estaba en línea era quien decía ser, y también para saber exactamente la cantidad de tiempo que pasaba delante del ordenador realizando las tareas *on-line*. En este estudio, 16 alumnos de la Escuela

de Ingeniería de Telecomunicaciones de la Universidad de Vigo fueron monitorizados mientras realizaban una prueba, que consistía en:

- Creación de la plantilla de la cara utilizando el módulo de verificación.
- El estudiante realizaba un breve cuestionario utilizando Moodle.
- El estudiante se movía al ordenador de su izquierda tomando el papel de impostor.
- El estudiante regresaba a su ordenador para comprobar los resultados obtenidos.

Obtuvieron que el 54 % del tiempo que duró la actividad, el alumnado era quien decía ser, mientras que solo un 29 % del tiempo estuvieron frente al ordenador correcto.

Respecto a los exámenes *on-line*, Fayyoumi y Zarrad (2014) proporcionaron una solución para sistemas de exámenes en línea mediante el uso de la autenticación facial de los estudiantes. Además, los autores no solo llevaron a cabo la identificación correcta del alumnado al inicio de la sesión *on-line*, sino que realizaron una monitorización continua (en cortos intervalos de tiempo) durante el periodo de los exámenes para asegurar que el alumno que había iniciado el examen era el mismo que se mantuvo hasta el final y evitar la posibilidad de que pudiera hacer fraude. El experimento fue presentado a ocho instructores expertos en *e-learning* y a 32 estudiantes, donde los resultados mostraron que casi todos los instructores estaban de acuerdo en que el sistema proporcionaba resultados fiables, reflejando los logros del alumnado al tener que estudiar con más firmeza. Además, los sujetos del experimento afirmaron que el engaño se vería disminuido y que el uso de este sistema animaría y motivaría a los estudiantes a estudiar más.

La autenticación correcta de un estudiante es un requisito fundamental en un *learning management system* (LMS), pues si algún tercero intenta ingresar usurpando la identidad de un alumno autorizado, puede comprometer la seguridad de todo el sistema

Por otro lado, numerosas investigaciones han analizado el uso de herramientas telemáticas en el rendimiento académico del alumnado. Por ejemplo, Valencia (2014) investigó si sus estudiantes *on-line* mejoraron sus resultados en promedio respecto a los que realizaron sus tareas de manera presencial. Soler et ál. (2009) concluyen que herramientas colaborativas 2.0, como Google Docs, wikis, blogs o glosarios de Moodle, mejoran significativamente el aprendizaje de los estudiantes.

El uso de las TIC dentro del campo educativo, en especial, con la utilización de una tecnología de autenticación facial podría modificar el entorno académico y las formas de impartir la docencia, por ello, se torna importante investigar la influencia que tendría su aplicación en el rendimiento académico del alumnado que realiza estudios a distancia.

El principal propósito de este trabajo frente a los proyectos anteriores es proponer un mecanismo que ayude a los profesores a implantar un *software* de autenticación facial, llamado Smowl, en las diferentes herramientas que proporciona la plataforma Moodle, intentando evitar posibles fraudes en las actividades evaluativas del alumnado y que, por consiguiente, este *software* no influya en su rendimiento académico. También este trabajo pretende conocer las percepciones del alumnado sobre su uso en tareas *on-line*.

4. MÉTODO

4.1. Procedimiento

La Udima, a través del proyecto de investigación Desarrollo de un Módulo de Autenticación y Monitorización Biométrica de Usuarios en Entornos Virtuales de Aprendizaje, financiado por la propia universidad, con número de referencia UD-019, ha llevado a cabo una prueba piloto que radica en la aplicación de un *software* de autenticación facial dentro de la plataforma Moodle para identificar de forma correcta al alumnado en el transcurso de sus actividades didácticas y conocer las percepciones que han podido tener respecto a su aplicación. Con la ayuda de este *software*, los profesores fueron conscientes de si el estudiante que realizaba las actividades era quien decía ser o, por el contrario, si las actividades habían sido llevadas a cabo por otros usuarios, o bien si el estudiante había tenido ayuda externa.

La investigación se centró en el uso de dos herramientas de Moodle donde se implanto el *software* de autenticación facial:

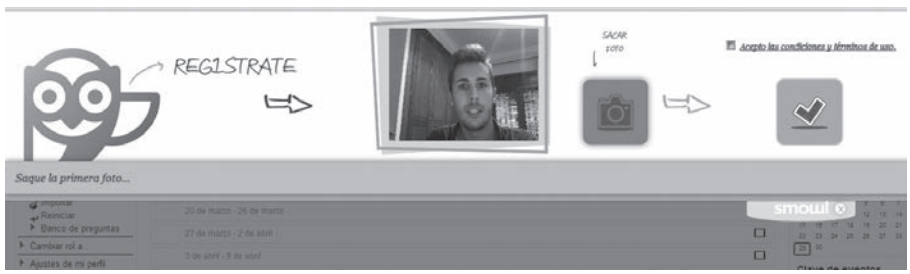
- Controles tipo test.
- Glosarios.

Se eligieron estas herramientas debido a que el alumnado tenía que permanecer dentro de la propia herramienta para hacer la actividad, evitando en parte salir de la plataforma, y de esta forma asegurar que la autentificación facial se estaría llevando a cabo durante todo el proceso de aprendizaje del alumno.

Hay que indicar que todo el trabajo que se ha realizado ha seguido dos caminos paralelos pero fuertemente entrelazados en diversos momentos. Por un lado, la recolección de las percepciones del alumnado sobre la aplicación de la herramienta de autenticación facial en sus actividades didácticas y, por otro lado, el análisis estadístico extraído del rendimiento académico del alumnado al usar el *software* facial.

El *software* utilizado para la autenticación facial es Smowl (2015), el cual fue implantado como un *plugin* dentro de las herramientas de Moodle. Los creadores del *software*, Labayen et ál. (2014), establecen que al comienzo del curso el *software* captura diferentes fotografías del estudiante y las compara con algún dato del alumno (por ejemplo, pasaporte o tarjeta de identidad nacional) para comprobar su correcta identidad. La figura 1 muestra la interfaz gráfica de Smowl.

Figura 1. **Interfaz gráfica de Smowl. Registro del usuario**

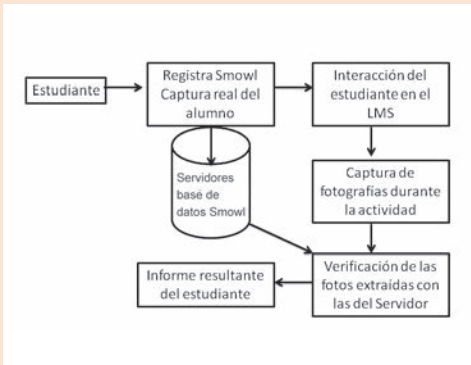


Fuente: elaboración propia.

(...) un sistema de reconocimiento facial es un *software* dirigido por un computador para identificar de forma automática a una persona en una imagen digital mediante la comparación de determinadas características faciales

Una vez que estas imágenes han sido tomadas, son almacenadas en la nube del *software*. Durante el transcurso de la actividad, las fotografías son capturadas constantemente a través de la cámara web del computador del alumno, las cuales son comparadas con las que el *software* tiene en sus servidores a través de un algoritmo que autentica su identidad. Los resultados obtenidos reportan un informe que se va actualizando constantemente cada vez que el *software* comienza a funcionar. Smowl pone a disposición de la universidad el informe que se ha generado, pero nunca las fotografías tomadas del estudiante, asegurando de esta forma la privacidad del estudiante. La figura 2 visualiza el funcionamiento general que tiene un *software* de autenticación facial dentro de una plataforma virtual de aprendizaje.

Figura 2. **Funcionamiento de un *software* facial en un LMS**



Fuente: elaboración propia.

4.2. Diseño y muestra

La investigación se llevó a cabo con 67 estudiantes procedentes de la Udima durante el primer semestre del curso académico 2013/2014. Los estudiantes pertenecían a las asignaturas Técnicas Avanzadas de Aprendizaje On-Line y Plataformas Tecnológicas, impartidas en el Máster Universitario en Educación y Nuevas Tecnologías y en el Máster de Comunicación Digital respectivamente. Por otro lado, la edad media de la muestra fue de 34 años.

Se diseñó una encuesta con el fin de medir las percepciones de los estudiantes sobre el uso del *software* de autenticación facial y su posible impacto en el proceso de enseñanza-aprendizaje. El cuestionario fue dividido en diversos bloques donde cada uno de ellos trató diferentes aspectos, tales como:

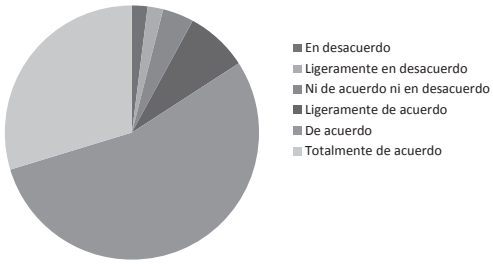
- Bloque 1. Aspectos personales.
- Bloque 2. Apropiación sobre el uso de Smowl en un LMS.
- Bloque 3. Influencia de Smowl en el rendimiento académico del alumnado.
- Bloque 4. Idoneidad del uso de Smowl en las actividades evaluativas de la universidad.
- Bloque 5. Interfaz del *software* y valoración sobre el uso de este sistema en los exámenes finales presenciales.
- Bloque 6. Apropiación del *software* facial dependiendo de qué tipo de herramienta 2.0 de Moodle se utilice.
- Bloque 7. Sentimientos que ha provocado en el alumnado el uso de este *software*.

El análisis que se lleva a cabo en esta investigación recoge diferentes preguntas del cuestionario que hace tener una visión general de todo el experimento. En el cuestionario se utilizó una escala Likert de siete puntos a través de valores numéricos:

- (1) Totalmente en desacuerdo.
- (2) En desacuerdo.
- (3) Ligeramente en desacuerdo.
- (4) Ni de acuerdo ni en desacuerdo.
- (5) Ligeramente de acuerdo.
- (6) De acuerdo.
- (7) Totalmente de acuerdo.

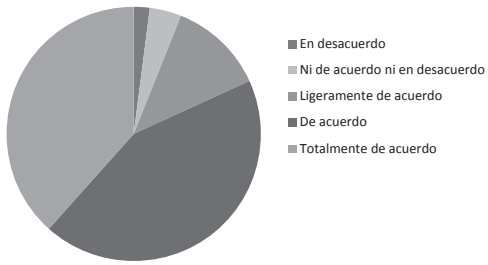
(...) en general, el alumnado parece estar dispuesto a asumir el grado de responsabilidad que conlleva utilizar un *software* de autentificación facial junto a sus actividades didácticas *on-line*

Figura 3. **Después de probar el *software*, ¿cree que es un buen método para identificar personas?**



Media	6,07	Moda	6	Rango	5	Máximo	7
Mediana	6,00	Desviación estándar	0,942	Mínimo	2		

Figura 4. **¿Cree que es apropiado que se utilice el reconocimiento facial en una plataforma virtual de aprendizaje, por ejemplo, Moodle?**



Media	6,15	Moda	6	Rango	5	Máximo	7
Mediana	6,00	Desviación estándar	0,925	Mínimo	2		

Fuente: elaboración propia.

5. RESULTADOS DEL PROYECTO

El proyecto planteó una serie de análisis y resultados en relación a las percepciones que tuvo el alumnado al ser monitorizado por el *software* de autenticación facial Smowl en su aprendizaje *on-line* y cómo podría afectar a su rendimiento académico. Los resultados, que se presentan a continuación, han sido divididos en dos apartados en función del ámbito de estudio que se quería analizar: percepciones del alumnado e influencia de Smowl en el rendimiento académico.

5.1. Percepciones del alumnado

Una vez que el estudiante ha interactuado con la interfaz gráfica del *software* de autenticación facial en sus actividades es cuando posee una opinión objetiva de la herramienta acerca de si es un buen método para la identificación correcta de los estudiantes.

A través de la figura 3 se puede ver cómo la media, mediana y moda se encuentran en el valor seis de la escala Likert de siete puntos (de acuerdo), interpretándose estos datos de forma positiva sobre la idoneidad de la implantación de este software de autenticación facial.

Se constató descriptivamente que, en general, el alumnado parece estar dispuesto a asumir el grado de responsabilidad que conlleva utilizar un *software* de autentificación facial junto a sus actividades didácticas *on-line*. Con una media, mediana y moda con valor seis en la escala Likert (de acuerdo), el alumnado consideró que implantar el *software* facial Smowl en un LMS con el fin de disminuir el fraude de estudiantes que pueden engañar al sistema en sus actividades es muy apropiado (véase figura 4).

La figura 5 es una de las más importantes de la investigación, ya que proporciona valiosa información acerca de si el alumnado cree que es justo el uso de un *software* facial en sus actividades didácticas *on-line* para evitar el fraude académico.

Si se tiene en cuenta el valor con una mayor frecuencia en la distribución de los datos (moda), se observa cómo el valor más destacado en la escala Likert de siete puntos es el siete (totalmente de acuerdo), deduciéndose que la gran mayoría consideran que es justo su uso.

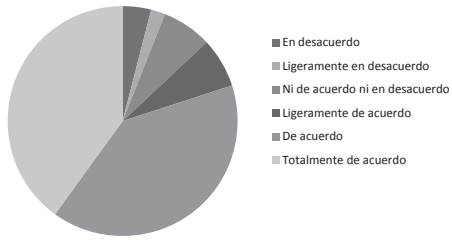
Es posible que cuanto más prestigio tenga una universidad más popular será y, por tanto, el alumnado querrá matricularse en ella. Por ello, es necesario que las universidades que proporcionan enseñanza a distancia cuenten con los mejores métodos que garanticen la correcta identidad de su alumnado. En este aspecto, Smowl podría hacer que mejore el prestigio de aquellas universidades a distancia que implanten este *software* facial.

Se observa a través de la figura 6 cómo la moda se encuentra en el valor siete de la escala Likert, donde el alumnado estaría totalmente de acuerdo en usarlo si con ello su universidad pudiera aumentar su prestigio y, consecuentemente, le resultara más fácil encontrar empleo.

La privacidad es un aspecto legal a tener en cuenta debido a la cantidad masiva de información personal que se comparte a través de internet. Por ello, es necesario conocer las percepciones del alumnado acerca de si creen que el *software* de autenticación facial haría que la perdieran al estar capturando momentos de su privacidad.

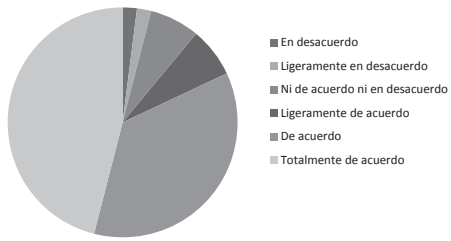
La figura 7 muestra cómo las percepciones de los estudiantes son dispares entre los diferentes valores de la escala Likert. La media se encuentra próxima al valor cuatro (ni de acuerdo, ni en desacuerdo). Es más, si se tiene en cuenta la moda, la mayoría del alumnado cree que no ha perdido su privacidad excesivamente, lo cual también refleja la mediana con valor de cuatro.

Figura 5. **¿Cree que es justo que se controle de forma correcta la identidad del alumnado con el fin de poder localizar a aquellos que pueden hacer trampas?**



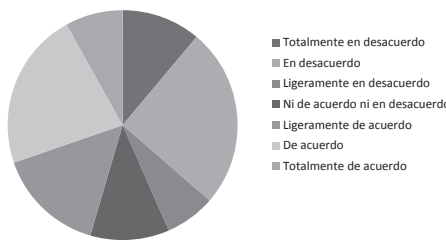
Media	6,00	Moda	7	Rango	5	Máximo	7
Mediana	6,00	Desviación estándar	1,219	Mínimo	2		

Figura 6. **¿Estaría dispuesto a que su universidad incluya un *software* de reconocimiento facial en su plataforma virtual de aprendizaje si con esto se le garantiza que el prestigio de su universidad será mayor y le será más fácil encontrar empleo?**



Media	6,12	Moda	7	Rango	5	Máximo	7
Mediana	6,00	Desviación estándar	1,122	Mínimo	2		

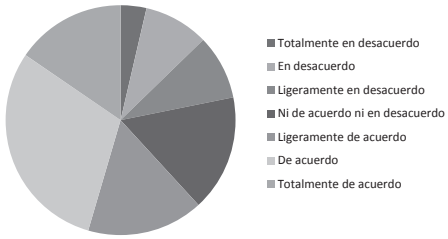
Figura 7. **¿Cree que perdería la privacidad si Smowl estuviera analizando sus fotografías mientras hace sus actividades didácticas *on-line*?**



Media	3,94	Moda	2	Rango	6	Máximo	7
Mediana	4,00	Desviación estándar	1,930	Mínimo	1		

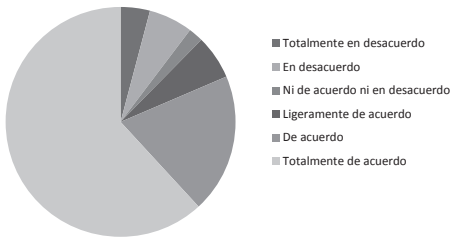
Fuente: elaboración propia.

Figura 8. **¿Se sentiría cómodo si Smowl estuviera analizando sus fotografías mientras realiza sus actividades didácticas *on-line*?**



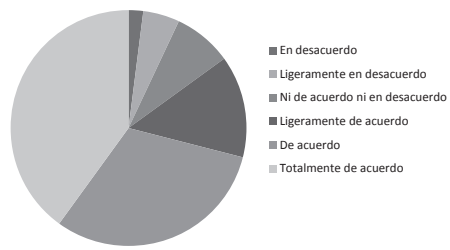
Media	4,90	Moda	6	Rango	6	Máximo	7
Mediana	5,00	Desviación estándar	1,716	Mínimo	1		

Figura 9. **¿Le gustaría que esta tecnología avance para que los exámenes presenciales actuales se puedan sustituir por exámenes *on-line* con un reconocimiento facial seguro?**



Media	6,19	Moda	7	Rango	6	Máximo	7
Mediana	7,00	Desviación estándar	1,490	Mínimo	1		

Figura 10. **¿Cree apropiado que la Udima invierta esfuerzos en la innovación tecnológica que supone la inclusión del reconocimiento facial en los entornos virtuales de aprendizaje?**



Media	6,03	Moda	7	Rango	5	Máximo	7
Mediana	6,00	Desviación estándar	1,154	Mínimo	2		

Fuente: elaboración propia.

Uno de los aspectos que podría hacer síntesis de forma general a los diferentes cuadros de sensaciones que el alumnado podría percibir al interactuar con Smowl es la de sentirse cómodo, provocando que su aprendizaje no se viera alterado y no afectara a su rendimiento académico.

La mayoría de los valores tienden a desplazarse hacia los valores más altos de la escala Likert. Por ejemplo, la moda posee un valor seis (de acuerdo), donde la mayoría del alumnado cree haberse sentido cómodo con el uso del *software* (véase figura 8).

Hoy en día, es necesario realizar un examen final presencial que permita verificar la identidad correcta del estudiante a la hora de evaluar los conocimientos adquiridos en una asignatura. Los resultados concluyeron que el alumnado estaría dispuesto a ser monitorizado por un sistema de autenticación facial que permitiera la realización de estos exámenes sin la necesidad de desplazarse físicamente y, por consiguiente, que todo el proceso evaluativo quedase en línea. Con una media de seis y una mediana y moda de siete en la escala Likert, el alumnado se muestra totalmente de acuerdo a que se siga investigando esta tecnología para conseguir este avance (véase figura 9).

Como conclusión general que englobe el proceso de investigación sobre las percepciones del alumnado se encuentra la innovación tecnológica por seguir mejorando el proceso de enseñanza-aprendizaje en la Udima.

Se puede ver reflejado en la figura 10 que el alumnado aprecia el esfuerzo que lleva a cabo la universidad para mejorar la innovación tecnológica de un *software* biométrico en las actividades didácticas del alumnado con el fin de mejorar el valor de los títulos ofertados.

5.2. Influencia de Smowl en el rendimiento académico en el alumnado

El proyecto de investigación analizó si el uso del *software* de autenticación facial en las actividades académicas de los alumnos podría influir en su rendimiento académico debido a que estos podrían tener sentimientos de vergüenza o pérdida de privacidad. Consecuentemente, esto podría ocasionar una variación en los resultados académicos de los estudiantes, y que estos tuvieran un cambio significativo en sus calificaciones. Se estableció como hipótesis nula que no existían diferencias significativas entre el grupo de estudiantes que fue monitorizado por Smowl y el que no lo fue.

Con el fin de comprobarlo, se trabajó con dos grupos homogéneos:

- Grupo control, que no fue monitorizado por el *software* facial en sus actividades didácticas *on-line*.
- Grupo experimental, que fue monitorizado.

La muestra consistió en 35 estudiantes para cada grupo en los «Controles tipo test» y, por otro lado, 25 estudiantes por cada grupo para las actividades «Glosarios». La distribución de los datos muestra los valores centrales de ambos grupos teniendo en cuenta la media, mediana, moda y desviación estándar (véase tabla 1).

Se aprecia en la tabla 1 un aparente aumento de las calificaciones numéricas para el grupo experimental, pero este aumento puede ser no significativo. Con el fin de comprobar si este aumento es significativo estadísticamente, se llevó a cabo la prueba de normalidad Kolmogorov-Smirnov. Este test dio como resultado normalidad para las actividades tipo «Glosarios» y no normalidad para las actividades «Controles tipo test». Por lo tanto, se utilizó la prueba paramétrica (T-Student) para los «Glosarios» y la prueba no paramétrica (U de Mann-Whitney) para los «Controles tipo test».

Tabla 1. **Datos descriptivos del experimento**

	Controles tipo test		Glosarios	
Descriptivos	**Control**	**Experimental**	**Control**	**Experimental**
Media	8,95	9,31	7,67	8,42
Mediana	9,17	9,59	8,00	8,70
Moda	9	10	9	10
Desviación estándar	1,773	0,863	1,699	1,501

Fuente: elaboración propia.

Tabla 2. **Pruebas estadísticas para el rendimiento académico del alumnado**

Controles tipo test (Mann-Whitney U Test)			Glosarios (T-Student)					
(sig.)	Test estadístico	Decisión	(sig.)	T	Diferencia error estándar	95 % de intervalo de confianza de la diferencia		Decisión
						Inferior	Superior	
0.629	573.000	Conserva la hipótesis nula	0.107	– 1.641	0.453	– 1.656	0.168	Conserva la hipótesis nula

Fuente: elaboración propia.

Teniendo en cuenta los resultados obtenidos en la tabla 2, se constató que los promedios que se obtuvieron entre el grupo control y experimental en ambos tipos de actividades no tuvieron diferencias significativas a nivel de significación 0.05. Dicho de otro modo, el rendimiento académico de los estudiantes que fueron monitorizados por el *software* de autenticación facial en sus actividades didácticas no es significativamente distinto de los que no lo fueron.

Por lo tanto, la conclusión que arrojan estos resultados es que un mecanismo de autenticación facial en las actividades *on-line* que el alumnado realiza a través de glosarios y controles de tipo test no influye estadísticamente en su rendimiento académico.

Los resultados obtenidos en este estudio han demostrado que el uso de un *software* de autentificación facial se posiciona como una herramienta idónea que ayude en la medida de lo posible a identificar de forma correcta al alumnado respecto de aquellos que puedan engañar al sistema

6. CONCLUSIONES Y TRABAJO FUTURO

En una sociedad rápidamente cambiante, las TIC se han masificado y potenciado, especialmente las plataformas virtuales, lo que hace que un mecanismo de autenticación facial pueda fortalecer aún más la seguridad de identificar de forma correcta al alumnado.

Hay que tener en cuenta también los nuevos caminos que puedan complementar este trabajo, teniendo en cuenta las posibles limitaciones que el uso de un *software* biométrico puede tener en un LMS.

Con el fin de seguir investigando sobre esta línea de trabajo, sería idóneo realizar un nuevo proyecto sobre cómo realizar exámenes finales virtuales con la ayuda de un *software* biométrico, para que así el alumnado no tenga que desplazarse (en muchas ocasiones a otra ciudad en la que reside) de forma obligatoria hasta la sede de la universidad donde pueda examinarse.

En este trabajo se ha expuesto que la identificación correcta de los estudiantes que realizan sus estudios en la modalidad a distancia es un proceso difícil y complejo. No obstante, este trabajo ha presentado la autenticación facial como herramienta para ayudar a mejorar el proceso anterior. Los resultados obtenidos en este estudio han demostrado que el uso de un *software* de autentificación facial se posiciona como una herramienta idónea que ayude en la medida de lo posible a identificar de forma correcta al alumnado respecto de aquellos que puedan engañar al sistema. Aunque el método presentado no evita por completo el engaño del estudiante, este tipo de herramientas ofrece una ayuda adicional a la identificación correcta del alumnado durante las sesiones de enseñanza-aprendizaje.

7. REFERENCIAS BIBLIOGRÁFICAS

Dehnavi, M. K. y Fard, N. P. [2011]: «Presenting a multimodal biometric model for tracking the students in virtual classes», *Procedia-Social and Behavioral Sciences*, 15, págs. 3.456-3.462.

Etzioni, A. [2008]: *The limits of privacy*, EE. UU.: Basic Books.

Fayyoumi, A. y Zarrad, A. [2014]: «Novel Solution Based on Face Recognition to Address Identity Theft and Cheating in Online Examination Systems», *Advances in Internet of Things*, 4, págs. 5-12.

García-Hernández, J. y Paredes, R. [2005]: «Biometric identification using palm print local features», *Biometrics on the Internet*, 11.

González-Agulla, E., Alba-Castro, J. L., Argones-Rúa, E. y Anido-Rifón, L. [2010]: «Realistic measurement of student attendance in LMS using biometrics», en *Proc. of the Int. Symposium on Engineering Education and Educational Technologies (EEET'09)* y *Systemics, Cibernetics and Informatics*, 8 (5), págs. 40-42.

Henríquez, G. F. A. [2014]: «Sistema de autenticación biométrica por reconocimiento de rostro», *Anuario de Investigación 2014*, pág. 119.

Jain, A. K., Flynn, P. J. y Ross, A. A. (eds.) [2008]: *Handbook of biometrics*, Springer.

Kalikova, J., Koukol, M. y Krcal, J. [2015, mayo]: «User authentication system for testing students in computer sciences subjects», *The 4th International Symposium on Next-Generation Electronics (ISNE 2015)*, IEEE, págs.1-4.

Labayen, M., Vea, R., Flórez, J., Guillén-Gámez, F. D. y García-Magariño, I. [2014]: «Smowl: a tool for continuous student validation based on face recognition for on-line learning», *Edulearn14 Proceedings*, págs. 5.354-5.359. International Association of Technology, Education and Development.

Lockwood, F. (ed.) [2013]: *Open and distance learning today*, Londres y Nueva York, NY: Routledge Taylor and Francis Group.

Noguera, C. G. [2012]: *Autenticación por reconocimiento facial para aplicaciones web, utilizando software libre*. Tesis doctoral (Universidad Pontificia Bolivariana).

Sayed, M. y Jradi, F. [2014]: «Biometrics: effectiveness and applications within the blended learning environment», *Computer Engineering and Intelligent Systems*, 5 (5), págs. 1-8.

Smowl [2015]: Website of Smowl Tech. Disponible en: http://smowltech.com/en. [Consulta: 5 de diciembre de 2015].

Soler, C. E., Prados, F., García, J. P. y Soler, J. [2009]: «La competencia "El trabajo colaborativo": una oportunidad para incorporar las TIC en la didáctica universitaria. Descripción de la experiencia con la plataforma ACME (UdG)», *UOC Papers: Revista sobre la Sociedad del Conocimiento*, 8.

Subban, R. y Mankame, D. P. [2014]: «Human face recognition biometric techniques: analysis and review», *Recent Advances in Intelligent Informatics*, Suiza: Springer International Publishing, págs. 455-463.

Valencia Arras, A. K. [2014]: *Competencias en TIC, rendimiento académico y satisfacción de los estudiantes de maestría en administración en la modalidad presencial y virtual de la Facultad de Contaduría y Administración de la Universidad Autónoma de Chihuahua, por género* (tesis doctoral). Universidad de Salamanca.