Universidad de Pamplona

Facultad de Ingenierías y Arquitectura

Programa de Ingeniería de Sistemas

Tema:

DISEÑO DE UN PROTOTIPO QUE REALICE CONTROL DE ACCESO EN LOS SERVICIOS Y RECURSOS INSTITUCIONALES DE LA UNIVERSIDAD DE PAMPLONA IMPLEMENTANDO RECONOCIMIENTO BIOMÉTRICO.

Autor:

Oscar Ferney Ardila Contreras

Pamplona, Norte De Santander

Junio 2020

Universidad De Pamplona

Facultad De Ingenierías y Arquitectura

Programa De Ingeniería De Sistemas

Trabajo de grado presentado para optar al título de Ingeniero de Sistemas.

Tema:

DISEÑO DE UN PROTOTIPO QUE REALICE CONTROL DE ACCESO EN LOS SERVICIOS Y RECURSOS INSTITUCIONALES DE LA UNIVERSIDAD DE PAMPLONA IMPLEMENTANDO RECONOCIMIENTO BIOMÉTRICO.

Autor:

Oscar Ferney Ardila Contreras

Director:

Avilio Villamizar Estrada

Magister en gestión de proyectos.

Pamplona, Norte de Santander.

Junio 2020.

Resumen

La autenticación e identificación son la primera etapa por la cual debe atravesar un usuario en el proceso de apertura de conexión a un servicio o una sesión, en las cuales es importante validar que la identidad del usuario sea la misma que está asociada en el sistema de información. Biometría para el reconocimiento de usuarios se basa principalmente en la etapa de identificación buscando características únicas de los seres vivos, posteriormente en la autenticación se utilizan también técnicas de biometría junto con técnicas de autenticación. Hay una gran diferencia entre autenticación contra identificación que es simple, en la identificación el objeto identificador permite comprobar que el usuario exista, en cuanto autenticación es el proceso en el que se puede demostrar que el usuario es quien dice ser.

En el presente documento se plasma el diseño de un prototipo que permita el control de acceso a los servicios institucionales de la Universidad de Pamplona diseñando un prototipo de reconocimiento biométrico, partiendo de la selección bajo un análisis comparativo entre algunas técnicas comunes y confiables de biometría y del mismo modo con técnicas de autenticación, buscando la mayor ventaja en relación costo beneficio para la Universidad de Pamplona. También describe el estudio realizado a la técnica seleccionada con herramientas diferentes y software de código abierto junto con una descripción de ellas. Culminando con el diseño de un prototipo juntando las técnicas seleccionadas junto con las herramientas de software.

Abstract

Authentication and identification are the first stage that a user must go through in the process of opening a connection to a service or a session, in any case it is important to validate that the identity of the user is the same one that is associated in the information. Biometrics for user recognition is mainly based on the identification stage, searching for unique characteristics of living beings. Later on, biometric techniques are also used in conjunction with authentication techniques. There is a great difference between authentication versus identification, which is simple, in identifying the identifier object it allows verifying that the user exists, as authentication is the process in which it can be shown that the user is who he claims to be. This document outlines the design of a prototype that allows access control to the institutional services of the University of Pamplona, implementing biometric recognition, starting from the selection under a comparative analysis between some common and reliable biometric techniques and in the same way with authentication techniques, seeking the greatest cost benefit advantage for the University of Pamplona. We also describe the study of the selected technique with different tools and open source software along with a description of them. Culminating with the design of a prototype combining the selected techniques together with the software tools.

Tabla de contenidos

Tabla de Figuras

1 Descripción del proyecto

1.1 Planteamiento del problema.

Existen diversos métodos de acceso a una plataforma o servicio para realizar autenticación e identificación, los cuales están basados en técnicas biométricas y su funcionalidad principal es automatizar para disminuir el contacto y los “cuellos de botella”, obteniendo así un mejor funcionamiento en relación a tiempos y costos. Estas técnicas biométricas suelen implementarse en modelos de gran escala, donde el control de acceso debido a la cantidad de usuarios hace que sea más complejo de realizarse por lo cual estas técnicas ofrecen un gran beneficio.

La Universidad de Pamplona ofrece múltiples servicios a la comunidad estudiantil, administrativa y docentes, pero una gran parte de los usuarios de estas comunidades no acceden a estos servicios, puesto que los métodos de autentificación e identificación con los que esta cuenta muchas veces son de arduo acceso, debido a que deben acceder al campus virtual por medio de un formulario web para posteriormente dar inicio a el uso de un servicio o acceso a un recurso físico. También teniendo en cuenta el control de asistencia que existe a los usuarios que ingresan a los diferentes recursos de la universidad como laboratorios aulas de clase entre otros, se hace mediante un formato donde el usuario registra sus datos en ocasiones para obtener el acceso.

¿Qué aporte tendría para la Universidad de Pamplona implementar técnicas de reconocimiento biométrico que garanticen la seguridad en el acceso de los servicios o recursos que ofrece la Universidad de Pamplona?

1.2 Justificación

Al realizar el proceso de automatización este proporciona unos beneficios, uno de estos es rendimiento, ya que se obtendrá una reducción de tiempos, además, que cuando se cuenta con un sistema de información de apoyo y una infraestructura ya establecida es factible ofrecer servicios a los usuarios, sin embargo, el acceso a estos servicios muchas veces se reduce a un formulario de acceso web, lo cual en ciertas ocasiones es una forma poco optima y tediosa para el usuario. Acceder a un servicio o recurso ofrecido por la Universidad de Pamplona es una de estas prorrogaciones, incluso un servicio básico como el acceso a recursos físicos para los estudiantes, docentes o administrativos, donde el método de control de asistencia que esta implementado es diligenciar un formato manual lo que se convierte en una tarea poco óptima. Este proyecto busca básicamente que, al iniciar la implementación de biometría se consiga un mejor rendimiento para el usuario y practicidad, puesto que no se necesitaría de los formatos que se emplean para la toma de asistencia en algunos servicios en los recursos de la Universidad de Pamplona.

1.3 Delimitación

- **Objetivo General:**
  - Diseñar un prototipo que realice control de acceso a los servicios y recursos ofrecidos por la Universidad de Pamplona empleando reconocimiento biométrico.
- **Objetivos Específicos**
  - Investigar los aspectos referentes a técnicas de reconocimiento biométrico.
  - Seleccionar bajo un análisis comparativo una de las técnicas más comunes de reconocimiento biométrico buscando la mejor en relación costo beneficio.
  - Seleccionar bajo un análisis comparativo una de las herramientas más comunes de código libre para la construcción del prototipo partiendo de la técnica seleccionada.
  - Diseñar el prototipo para el control de asistencia de los docentes y estudiantes de la Universidad de Pamplona

1.4 Acotaciones

El presente trabajo empleó solamente herramientas de software que sean de código libre (Open Source), el análisis comparativo de las técnicas de biometría se realizó teóricamente es decir basado en investigaciones y artículos, no se implementó ni se validó.

1.5 Metodología

La metodología empleada para el desarrollo de este proyecto es con un enfoque de investigación aplicada, se exploraron y se realizaron un análisis de la forma más adecuada de utilizar con los recursos que ya se cuentan para lograr el cumplimiento de los objetivos de este proyecto.

El proyecto se segmento en (3) fases: La primera fase se basó en explorar, investigar y dar una apertura teórica al tema, se exploraron antecedentes, los tipos de biometría y que tipo de tecnología tiene desplegada en infraestructura la Universidad de Pamplona, posteriormente en la segunda fase con la información recopilada se realizó una toma de decisiones la cual consistió en la selección de un tipo de biometría, además, una comparativa entre las diferentes librerías y tecnologías para obtener como resultado las bases y continuar con la tercera y última fase que básicamente consistió la construcción de un prototipo con base a los elementos teóricos y herramientas seleccionadas en las fases anteriores.

Para este proyecto la recopilación de información se establece partiendo de dos tipos de fuentes de información, información primaria e información secundaria; la información primaria se fundamenta en reuniones realizadas con el equipo encargado del desarrollo, seguridad, administración de bases de datos y algunos administrativos de la Universidad de Pamplona. La información secundaria se estableció de artículos, libros e internet.

2 Marco teórico y estado del arte

2.1 Marco conceptual

- **Biometría:** El concepto biometría viene de las palabras bio (vida) y metría (medida), consiste en técnicas que miden e identifican las características físicas únicas de organismos vivos o patrones de su comportamiento, que permiten identificar los diferentes individuos, como por ejemplo las clásicas huellas digitales. (Cortés Osorio, 2010)

  Partiendo de esta definición se puede encontrar técnicas comunes para el reconocimiento por biometría:

2.1..1 Reconocimiento dactilar:

El reconocimiento biométrico dactilar es uno de los métodos mas implementados con un nivel de confianza alto para identificar usuarios, este éxito se debe a la formación de las crestas que se encuentran en la dermis las cuales forman un patrón que tienen características llamadas minucias cuya probabilidad de repetirse es de “1 entre 64 billones “ (Galton, 1892) existen minucias de bifurcación, básicamente la cresta se divide en dos, y minucias de terminación, donde la cresta termina. El delta o núcleo es un elemento de la huella donde se encuentra una triangualción que esta determiado por las limitantes basilar, nuclear y marginal.

2.1.2 Patrones dactilares:

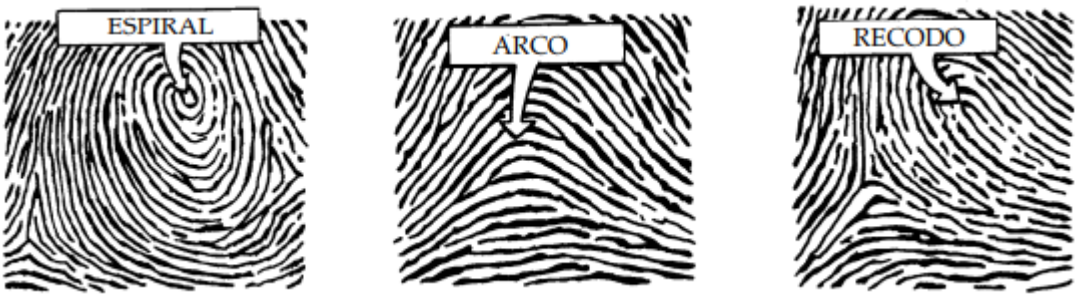


Ilustración 1 Patrones básicos de huellas dactilares fuente: http://lhsgems.org/spanish/FPspanish.pdf

2.1.2.1 Arco y arco entoldado:

En el arco las crestas son bifurcadas y corren de un lado al otro sin la presencia de elementos delta. Por otro lado, en el arco entoldado las crestas tienen típicamente un movimiento que denota más las crestas y hacia arriba.

2.1.2.2 Espiral:

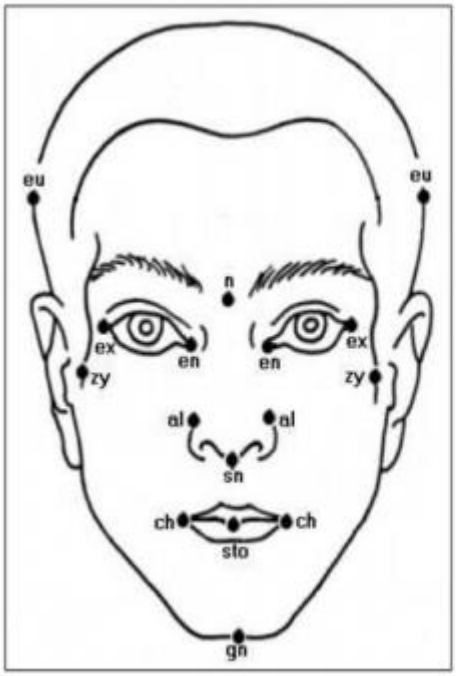
Previo al inicio de cada delta se denota típicamente una ligera curva, básicamente se denota una espiral completa.

2.1.2.3 Recodo o bucle:

Se percibe la presencia de un elemento delta, además las crestas inician en el exterior y en el centro aparecen unas desviaciones que se tornan curvas.

2.1.3 Reconocimiento facial:

Actualmente se está dando el aumento a la implementación del reconocimiento biométrico facial el cual genera un nivel de confianza alto al momento de reconocer usuarios en un caso optimo, esta técnica intenta que mediante el rostro de la persona el sistema pueda identificarlo y autentificarlo. Los sistemas de reconocimiento facial en principio clasifican la morfología de la persona e implementan la medición de puntos específicos, básicamente intentan encontrar un patrón basado en distancias y longitudes descritas en la ilustración 2.



DESCRIPCION
Eurion → eu
Cigion → zy
Nasion → n
Gnation → gn
Subnasal → sn
Alar → al
Cheilion → ch
Estomion → en
Endocanto → ex
Labiale Superius → ls
Labiale Inferius → li

Ilustración 2 Puntos característicos del complejo facial para una vista frontal. (Farkas., 1994)

2.1.4 Reconocimiento por iris:

"Es el método más fiable, ya que, posee alrededor de 266 puntos particulares y

exclusivos de cada persona, mientras que el resto de los sistemas cuentan alrededor de 13 a 60 características distintas. Cada ojo es único y permanece estable con el paso del tiempo y en diferentes ambientes de clima.” (Neocheck, 2016), se considera esta técnica muy fiable y eficiente para identificar a un usuario por su gran velocidad de identificación puesto que los patrones son muy estables.

2.1.5 Autenticación:

La autenticación debe certificar que la identidad del usuario mediante los datos suministrados sea la que se encuentra relacionada en el sistema de información, este proceso se puede realizar bajo varias técnicas.

2.1.6 Identificación:

Debe responder a la petición de si el usuario existe en el sistema bajo una comparación de estos, los datos personales deben coincidir con los datos que están en la base de datos.

2.1.7 Autenticación e identificación de usuarios basada en contraseñas:

Es un mecanismo ampliamente extendido, soportado por prácticamente todos los sistemas operativos del mercado. Sin embargo, se debe tener en cuenta que su seguridad depende de una elección segura de la contraseña y de su correcta conservación por parte del usuario, siendo el factor humano uno de los principales puntos débiles de la seguridad informática. (Álvaro Gómez Vieltes, 2006)

2.1.8 Tratamiento de imágenes:

Para identificar usuarios sin importar la técnica biométrica, se debe realizar un tratamiento

de la imagen para posteriormente aplicarle diferentes métodos de reconocimiento de patrones esto se realiza mediante herramientas para identificar a los usuarios, es importante encontrar un buen plano de imagen y tener una buena data, los filtros aplicados a la imagen dependen directamente de la técnica biométrica.

2.1.9 Reconocimiento de patrones:

El término de reconocimiento de patrones se refiere a un procesamiento de información que tiene una gran importancia práctica que da solución a un amplio rango de problemas. Algunos de estos problemas son resueltos por los humanos sin mucho esfuerzo. Sin embargo, en muchos casos, la solución a estos problemas, usando computadoras, se vuelve extremadamente dificultosa (Bishop, 1995)

2.1.10 Control de acceso:

"El control de acceso se trata sobre los sistemas que protegen a los objetos de valor y también sobre las decisiones tomadas por las personas que determinan quien recibe alguna clase de acceso. Los sistemas de control de acceso se ponen en marcha para garantizar que sólo las personas autorizadas tengan acceso a la información, y que para que la información se mantenga intacta y disponible cuando sea necesario. " (Peltier, 2014)

2.1.11 Lector de huellas digitales:

Es un dispositivo que tiene la capacidad de leer, almacenar en algunos e identificar huellas dactilares, con el fin de brindar seguridad. El funcionamiento de este dispositivo se basa en detectar el relieve que existen en los dedos empleando sensores eléctricos o luz, este dispositivo capta la imagen, la envía a un punto de control o una computadora para realizar

su identificación, el proceso puede variar. El lector de huellas es muy común encontrarlo en diferentes dispositivos móviles, chapas de puertas, carros, entre otros.

2.1.12 Cámara IP:

Una cámara IP es un dispositivo que fue diseñado con la especialidad de poder transmitir en directo señales de audio y video en internet o en una red local, permitiendo acceder mediante un IP definido. Muchas de estas cámaras cuentan con protocolos para el acceso a las señales, además, algunas permiten almacenar información de forma local sin contar con algún otro dispositivo externo, lo que lo convierte en un gran beneficio para algunas aplicaciones.

2.1.13 Protocolo RSTP:

Rapid Spanning Tree Protocol (RSTP), controla él envió de datos garantizando que se haga de forma correcta, este protocolo "se trabaja normalmente al hacer STREAMING es muy sensible a la sincronía temporal (o a la falta de ella). Así pues, se podría considerar que el RTSP actúa como si de una especie de mando a distancia de red para servidores multimedia se tratase." (Costilla, 2008)

2.1.14 Inteligencia artificial:

"En términos simples, inteligencia artificial (IA) se refiere a sistemas o máquinas que imitan la inteligencia humana para realizar tareas y pueden mejorar iterativamente a partir de la información que recopilan." (Oracle, 2017). El campo de la inteligencia artificial es bastante amplio que se subdivide en varios subcampos como lo son MACHINE LEARNING y DEEP LEARNING.

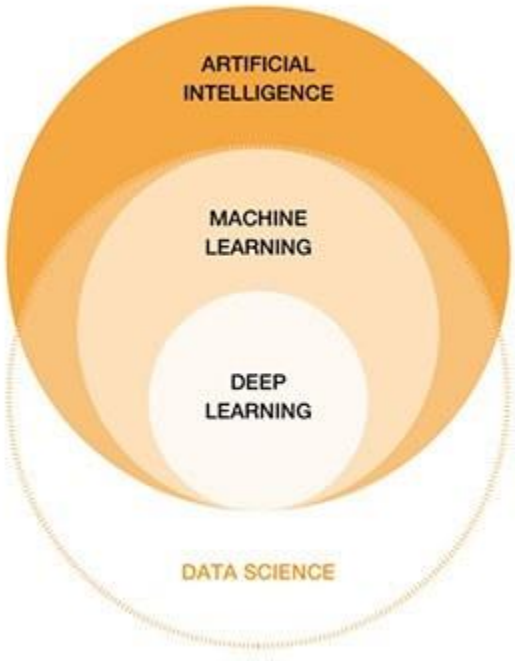


Ilustración 3 Sub campos de la inteligencia artificial. (Oracle)

2.1.15 Bases de datos:

Actualmente es una de las herramientas más usadas para almacenar información de un sistema, debido a que cuenta con una amplia gama de posibles aplicaciones. “Base de Datos un conjunto de datos estructurado y almacenado de forma sistemática con objeto de facilitar su posterior utilización. Una base de datos puede, por tanto, constituirse con cualquier tipo de datos, incluyendo los de tipo puramente espacial (geometrías, etc.)” (github, s.f.)

2.1.16 Código abierto:

También conocido como Open Source, “diseñado de manera que sea accesible al

público: todos pueden ver, modificar y distribuir el código de la forma que consideren conveniente. El software open source se desarrolla de manera descentralizada y colaborativa, así que depende de la revisión entre compañeros y la producción de la comunidad. Además, suele ser más económico, flexible y duradero que sus alternativas propietarias, ya que las encargadas de su desarrollo son las comunidades y no un solo autor o una sola empresa." (RedHat, s.f.) . Existe una diferencia entre código libre y software libre, suelen ser lo mismo en la mayor parte de los casos con excepciones. En algunos casos se basan principalmente en el acuerdo de licencias de uso y distribución.

2.1.17 Software Libre:

"El movimiento del software libre defiende la libertad de los usuarios de ordenadores, en un movimiento en pro de la libertad y la justicia" (GNU, 2008). En sus principios esta el poder copiar, ejecutar y distribuir programas informáticos bajo un acuerdo que de libertad y sin asumir ningún recargo monetario por este.

2.1.18 Arquitectura de software:

El concepto básico de arquitectura de software son los patrones, lineamientos y procedimientos mediante los cuales se basa un equipo de trabajo para desarrollar un programa, además, uno de los principales objetivos es crear un modelo para que el desarrollo sea fácilmente escalable entre las diferentes arquitecturas establecidas. La arquitectura puede estar definida en una serie de etapas:

- Requerimientos: En esta etapa básicamente se procede a definir los requerimientos funcionales del sistema, esto con el fin de poder definir el

manejo de la información, importante para optar por una arquitectura fácilmente escalable.

- Diseño: En esta etapa se buscan las tecnologías más adecuadas según los requerimientos definidos en la primera etapa, se busca que la arquitectura sea fácilmente adaptable al modelo del sistema o software a construir y se definen las funciones y responsabilidades de los componentes con los que va contar este.

La arquitectura de software es un pilar muy importante al momento de realizar un sistema, es por esto que no se debe seleccionar la que se encuentre de moda, se busca el mejor beneficio más no una arquitectura potente.

2.1.19 API

Application Programming Interface, es una interfaz que se puede componer de protocolos, procedimiento y funciones que generalmente es usada para la interconexión de dos sistemas con el fin de intercambiar datos, además, simplifican el desarrollo de aplicaciones puesto que no se necesita de qué forma se encuentran implementadas.

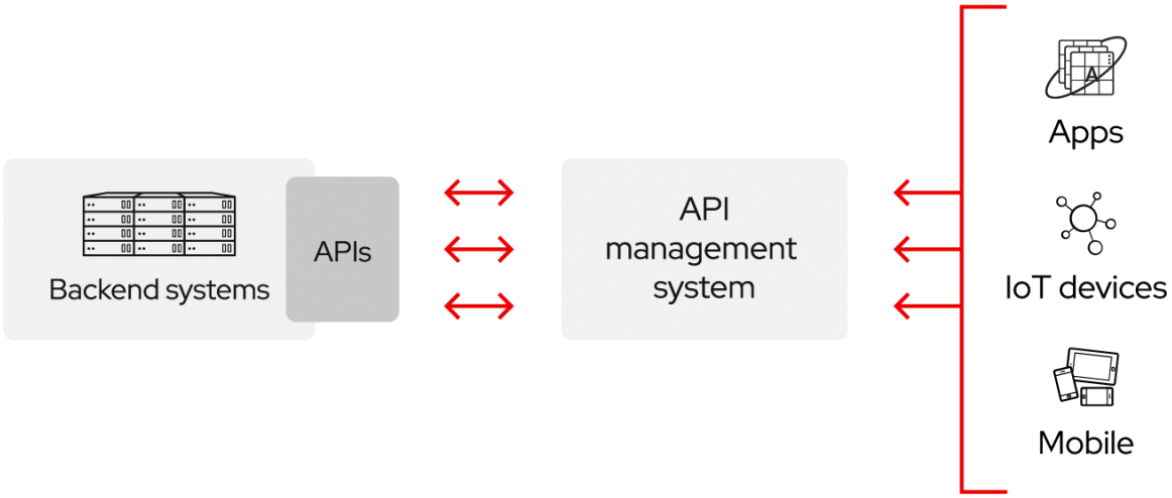


Ilustración 4. Arquitectura API (Red Hat)

2.1.20 FLASK

Es un 'micro' Framework que fue creado para la construcción de un sitio web de una forma dinámica y sencilla, este se encuentra escrito en Python. Flask está en disponibilidad de Open Source.

2.2 Herramientas para reconocimiento biométrico

Existen diversos tipos de herramientas para realizar reconocimiento biométrico, a continuación, se enuncian las más comunes.

- **Sensor de huellas para reconocimiento biométrico dactilar.**

Existen varios tipos de sensores que realizan reconocimiento biométrico dactilar, los más comunes son sensores ópticos, escáner y sensores de estado sólido, cada uno presenta sus

ventajas y desventajas que representan en magnitudes amplias cuando llega el momento de realizar la construcción de un prototipo funcional.

Este tipo de herramienta generalmente tiene un patrón de aceptación bastante excelente en cuanto a la forma que determina la identidad de un individuo, debido a que el sensor usa las huellas, estas, difícilmente repetibles.

- **Sensores ópticos para reconocimiento biométrico facial.**

  La finalidad de este es más general, se basa en imágenes para detectar un patrón, lo cual lo hace variante, debido a que los cambios en la piel, cara y cabeza conforme avanza la edad del individuo van siendo significativamente altos, esto reduciendo la cantidad de coincidencias encontradas para lograr una buena aceptación. No obstante, con ir actualizando los datos base para partir a una coincidencia, solucionaría el inconveniente.

  Este sensor debe contar con buen hardware para que en el momento que se lleve a cabo la toma de una imagen o video, este quede con alta calidad que lo cual repercute en el momento de realizar una comparativa esto pueda arrojar una coincidencia más alta.

- **Sensores láser para reconocimiento biométrico mediante iris.**

  Este tipo de sensor emplea el uso de láser para realizar el trabajo de toma del patrón, lo cual conlleva a que su implementación sea más costosa, generalmente la lectura mediante iris se vuelve incomoda. La implementación de este sensor puede llevar a un nivel más alto de seguridad, pero, no es un método general, debido a la toma de datos para la creación de patrones.

2.3 Estado del arte

- **Internacional:**

Autenticación Web de Estudiantes Mediante Reconocimiento Biométrico

"En este trabajo se hace un análisis de las tecnologías de reconocimiento biométrico basado en dinámica de tecleo para la autenticación de estudiantes en entornos web. A diferencia de la autenticación basada en algo que tenemos (tarjetas) o algo que sabemos (passwords), el reconocimiento biométrico hace uso de características propias de los individuos (algo que somos) para verificar sus identidades. En este trabajo se estudian las características de estos sistemas, así como su idoneidad para su aplicación en entornos docentes. Se incluye también un experimento práctico en el que se analiza el patrón biométrico de 64 alumnos. El experimento permite analizar el rendimiento de dos sistemas de reconocimiento a través de la dinámica de tecleo de los alumnos a lo largo de 3 exámenes elaborados durante un semestre. Los resultados muestran una tasa de reconocimiento superior al 90% lo cual anima a seguir investigando esta línea para su implantación en entornos reales." (Aythami Morales, 2015)**.** Este informe presenta información importante en la cual el autor del libro tomo como referencia para realizar un primer acercamiento a la arquitectura física a emplear, además, este trabajo obtuvo resultados por arriba de 90% de posibilidades de acierto.

Sistema de Control de Acceso al Personal Mediante Reconocimiento Facial.

"La investigación "Sistema de Control de Acceso al Personal Mediante Reconocimiento Facial" pretende mejorar eficientemente el ingreso los empleados y generar

un reporte en una base de datos para tomar decisiones de manera correcta. Para la fase de reconocimiento se aplicó la técnica de Análisis de Componentes Principales (PCA), debido a que reduce la dimensionalidad de las imágenes eliminando la información que no es necesaria, para luego descomponer de manera precisa la estructura facial en componentes ortogonales conocidos como Eigenfaces. Para la experimentación se utilizó una base de datos (MySQL) de imágenes normalizadas. Con esta técnica se logra mejorar el porcentaje de aciertos en el reconocimiento facial, ya que permite trabajar con un conjunto grande de imágenes para el entrenamiento." (Juan Pablo Pallo, 2016). En este informe se lograron resultados altamente satisfactorios que motivaron al autor del libro a buscar herramientas que realicen diferentes tipos de comparativas, además, este trabajo menciona las problemáticas que puede tener el sistema cuando el usuario cuenta con gorras, lentes, bufandas y otros elementos de uso personal.

- **Nacional:**

Diseño e implementación de un prototipo para el control de acceso en la sede de ingeniería de la universidad distrital francisco José de caldas mediante el uso de torniquetes controlados por carnet con tecnología NFC y lector biométrico de huella dactilar. "Día a día las empresas e instituciones buscan soluciones prácticas que ayuden a tener un control permanente en sus instalaciones, es por ello que la industria ha venido desarrollando sistemas de control que proporciona acceso total o parcial al personal en áreas específicas dentro de las instalaciones. En la actualidad se ha incrementado la necesidad de elevar el nivel de seguridad de ingreso en búsqueda de brindar tranquilidad a quienes hacen

parte de una comunidad especifica; en respuesta a dicha necesidad, el mercado ofrece diversas soluciones especializadas, con el uso de métodos y herramientas que cumplan con los requerimientos para mejorar la seguridad. En este ámbito, los centros educativos han buscado la forma de regular y controlar el acceso de estudiantes y funcionarios en cada una de las áreas dentro de las instalaciones, garantizando así la protección frente a posibles intrusos que puedan poner en riesgo la seguridad de las instalaciones y de sus individuos. Hoy en día existe gran variedad de tecnologías que permiten validar información para realizar el control de acceso, entre las cuales encontramos, tarjetas de banda magnética, tarjetas de chip (Smart Card), tarjetas de proximidad RFID, tarjetas de proximidad NFC y lectores biométricos, algunas con una validación más confiable y segura que otras. De dichas tecnologías sobresalen por su confiabilidad y baja vulnerabilidad las tarjetas NFC y dentro de los lectores biométricos el correspondiente a huella dactilar. Últimamente se han creado distintos protocolos y estándares de conexión que dan la posibilidad de realizar el envío y recepción de información entre dispositivos, dentro de estos estándares de validación se encuentra el NFC, que se encarga de generar un método de comunicación inalámbrica, de corto alcance y alta frecuencia permitiendo el intercambio de datos entre dispositivos. También existe un avance considerable en cuanto a la identificación por medio de huella dactilar, biométricos que cuentan con algoritmos de rápido reconocimiento y que dan una lectura con mayor exactitud. Todo lo anterior se puede llevar al entorno que presenta la Universidad Distrital Francisco José de Caldas frente al ingreso de sus funcionarios y estudiantes. La forma en que actualmente se controla el acceso de personal a la institución es

poco confiable ya que se realiza de manera manual al presentar el carnet o recibo de pago que identifica a la persona como miembro de la Universidad a un guarda de seguridad quien es el encargado de validar la información y permitir o no, el acceso a las instalaciones de la misma. Al observar este sistema anticuado y con estándares de validación bajos nace el proyecto planteado y es aquí donde se encuentra su objetivo con la inclusión de las tecnologías NFC y lectores biométricos de huella dactilar. Al incluir estas nuevas tecnologías se integraría un sistema que permite la validación de la información con un mayor nivel de seguridad en un tiempo mucho menor lo cual va a 11 evitar congestiones tanto a la entrada como a la salida y va mejorar el control de acceso a las instalaciones de la Universidad Distrital Francisco José de Caldas, mejorando principalmente el tiempo y la seguridad. Para lograr la ejecución del proyecto se realizó un prototipo basado en un sistema compuesto por 2 lectores MIFARE y un controlador con tecnología NFC, todo lo anterior integrado a un Torniquete Gunnebo que cuenta con control de entrada-salida, que junto con el software ZKAccess crean un sistema que aporta un mayor nivel de seguridad y un flujo constante de personal. Ya que los recursos del proyecto fueron limitados, no fue posible realizar la instalación del lector biométrico de huella dactilar pero el sistema queda abierto para su futura instalación.” (Alvaro Javier Balsero Menseses, 2016). Uno de los elementos que el autor del libro considero importantes de este trabajo, fue el uso de dos técnicas como método de acceso a un sistema, además, la integración de la infraestructura con el prototipo y, también, menciona la importancia de existencia de información porque es con esta que el prototipo funcionará.

Sistema de reconocimiento facial para control de acceso a viviendas. “Este trabajo de grado presentó el desarrollo de un sistema de reconocimiento facial el cual permitirá el control de acceso a una casa. Debido a la alta inseguridad que se evidencia en la ciudad, y los constantes robos en las viviendas, es imperativo crear alternativas que afronten este aspecto, ya que esta problemática afecta el estado de confort y seguridad en el hogar perjudicando en gran medida la salud de los ciudadanos sea física o mentalmente; por este hecho, se vio la necesidad de crear una solución que disminuya estos porcentajes de hurto utilizando un sistema de identificación biométrica facial, permitiendo que el acceso a nuestros hogares no depende de objetos que puedan perderse o caer en manos ajenas. Durante el desarrollo del trabajo de grado se realizó la recopilación de información, análisis de requerimientos, tanto de un control de acceso como de los dispositivos que se utilizaron, y por último la implementación del control de acceso en el hogar y los aspectos a tener en cuenta para un funcionamiento ideal del sistema otorgando sus respectivas pruebas de funcionamiento y la eficacia del sistema al reconocer a una persona en diferentes expresiones faciales. Con este sistema no solo se pretende brindar seguridad y confort al usuario si no incentivar el uso de herramientas tecnológicas como el reconocimiento facial, y dispositivos que están en el mercado, para implementar un control de acceso a viviendas seguro y de un bajo costo.” (David Leonardo Castaño Saavedra, 2019). Mediante este trabajo el autor del libro establece la importancia de utilizar algoritmos que sean ya implementados por entes u organizaciones, puesto que el consumo de procesamiento fue un aspecto importante para el trabajo mencionado anteriormente.

- **Regional:**

En Pamplona Norte de Santander el autor del libro encontró, **Prototipo de sistema de control de acceso y monitoreo automatizado para el laboratorio de redes y electrónica del ISER de pamplona.** "La integración de diferentes disciplinas del área de la ingeniería como la programación, las redes de comunicaciones y la electrónica han permitido el desarrollo de aplicaciones que garantizan el bienestar y el confort de las personas en diferentes ámbitos de la vida como el hogar, el sitio de trabajo o de estudio, lo que actualmente se conoce como domótica e inmótica. Algunos de los desarrollos que han tomado mayor relevancia en los últimos años y que se abordan en este proyecto son los sistemas de seguridad de espacios físicos y el control del acceso a los mismos utilizando biométrica (huella, iris, entre otros), técnicas de comunicación inalámbrica (RFID o bluetooth) o mediante protocolos de comunicación e identificación. El propósito de este proyecto fue desarrollar un prototipo que permitiera controlar el acceso al laboratorio de redes y electrónica del ISER mediante un sistema biométrico soportado en una tarjeta Arduino uno y el establecimiento de comunicación bluetooth mediante una APP. Igualmente se desarrolló el sistema de monitoreo del aula en cuanto a variables ambientales como humedad, temperatura y el estado de seguridad locativa como estado de ventanas y puertas entre otros." **(Alexander Rojas Manrique, 2018)**, Este modelo permite al autor tener una guía de implementación puesto que tiene un estudio y una guía de creación del prototipo, también un aspecto importante sobre este trabajo se centra en la arquitectura empleada para la construcción de este, que brinda sistemas por salón de implementación.

3 Análisis preliminar.

El siguiente capítulo al cual el escritor del libro lo segmentó describiendo los principales aspectos que hacen referencia al reconocimiento biométrico. Se enfatizó con aspectos generales de estas, con el fin de contar con una base sólida que aporte a la toma de decisiones.

3.1 Principales técnicas de reconocimiento biométrico.

"El reconocimiento biométrico, definido como la técnica que posibilita la identificación automática de individuos basándose en sus características físicas o de comportamiento, está ganando gran aceptación como método para determinar la identidad de cada persona y ya se está utilizando en multitud de aplicaciones tanto comerciales como públicos gubernamentales, en ámbitos tanto civiles como forenses (es decir, relacionadas con lo policial y lo legal)." (Ortega-Garcia, J. & Alonso-Fernandez, Fernando & Coomonte-Belmonte, 2008).

El análisis preliminar se centra en un análisis a las técnicas a tratar, buscando puntos de referencia más importantes de cada una de ellas con esto facilitando la toma de decisiones. Para cada técnica se pueden responder las siguientes preguntas: ¿Cuáles son sus fundamentos?, ¿Cómo es su implementación?, ¿Cómo es su funcionamiento?, ¿Cuáles son sus ventas y sus desventajas?

- **Reconocimiento dactilar.**

Esta técnica es una de las más comunes, se puede conseguir en los dispositivos móviles, en los vehículos, en los cajeros, en acceso a casas. Es una técnica de alta precisión, sus bases

teóricas se referencian en la forma que está constituida la piel de un individuo, esto fue atribuido a “J. C. A. Mayer, médico y anatomista alemán, escribió el libro titulado Anatomical Copper-plates with Appropiate Explanations, que contenía los planos detallados de los patrones de las crestas de fricción en piel. Mayer escribió, aunque la disposición de las crestas de la piel nunca se duplica en dos personas, las similitudes son más cercanas entre algunos individuos. En otros, las diferencias están marcadas, pero a pesar de las peculiaridades de la disposición, todos tienen una cierta semejanza” (Departamento de Justicia de los Estados Unidos, 2002).

Los patrones que se consiguen en las manos, más específico en los dedos, tienen bifurcaciones que son las encargadas de dar la unicidad entre individuos, estas son difícilmente repetibles , según galton estimo que la posibilidad de repetirse es de “1 entre 64 billones “ (Galton, 1892), esto lo hace una tecnica de reconocimiento de una escala de aceptabilidad bastante alta.

Ilustración 5. Huella dactilar. (Departamento de Justicia de los Estados Unidos, 2002)

Esta técnica tiene diferentes algoritmos que se encargan de realizar su clasificación, estos cuantifican defectos y para ello tienen parámetros, uno de estos es la Tasa de Falsa Aceptación (FAR sus siglas en inglés) y Tasa de Falso Rechazo (FRR por sus siglas en inglés), entonces, de estos errores la más aceptada es FAR, puesto que con esta se miden errores de lectura, entonces según sea implementado el sistema de recolección hasta cierto tiempo podrá volver a intentarlo. Si FRR es tomado en consideración puede tener vulnerabilidades de seguridad puesto que son tazas altas de rechazo, significando esto que no es el usuario valido para el acceso, lo que conlleva a que usuarios no autorizados puedan acceder.

El funcionamiento de esta técnica tiene varias herramientas tecnológicas que se emplean para el reconocimiento. El escritor del libro selecciono que las más comunes son: Sensores Ópticos, sensores de Estado Sólido y Sensores de Ultrasonido.

Los sensores Ópticos, son de los más implementados por la simplicidad de su funcionamiento, además, de que es uno de los más antiguos, el funcionamiento de este radica en que genera un haz de luz en varias direcciones mediante un LED, lo que hace iluminar las crestas de la huella y dejando más opacos los surcos, dejando claro el patrón que es capturado por un dispositivo de carga acoplada (CDC por sus siglas en ingles).

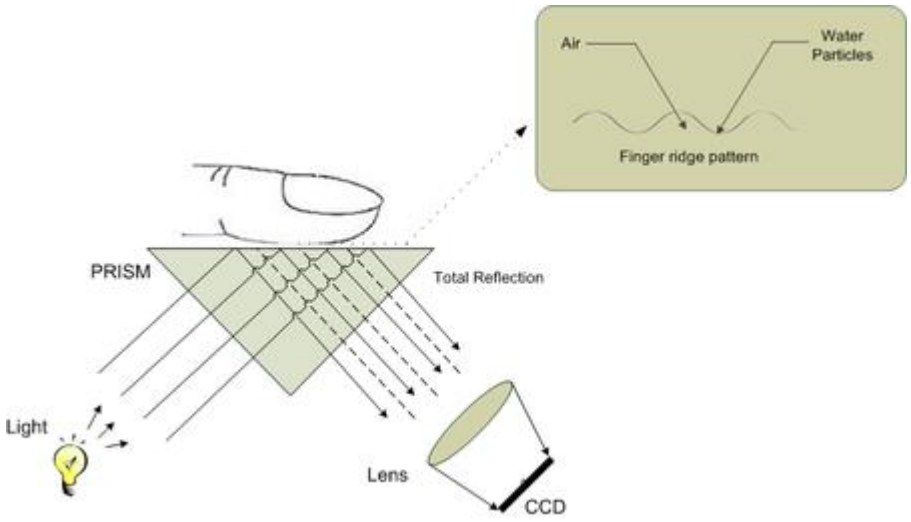


Ilustración 6. Funcionamiento de sensor óptico. (xataka)

Los sensores de estado sólido, se encargan de convertir la información física en estados de señales eléctricas, esto es una particularidad que la diferencia de los sensores ópticos, ya que este no necesita de un dispositivo de carga acoplada CDC, para la captura de la huella. El funcionamiento de estos sensores, se basa en la toma de voltaje mediante micro capacitores que están distribuidos e integrados en un chip, la medida captada es la que determina la imagen de la huella dactilar. Una de las principales desventajas de este sensor es que la piel seca o muy húmeda no arroja mediciones estables.

Los sensores de ultrasonido, emplean un transmisor para que reproduzca señales acústicas, las cuales generan eco, es decir, la señal impacta la huella dactilar y esta es captada por un componente receptor, entonces las variaciones se van a representar en las crestas o surcos, así determinando un patrón. Este sensor presenta dificultades cuando el individuo tiene las huellas húmedas y sucias, haciendo el FRA más grande.

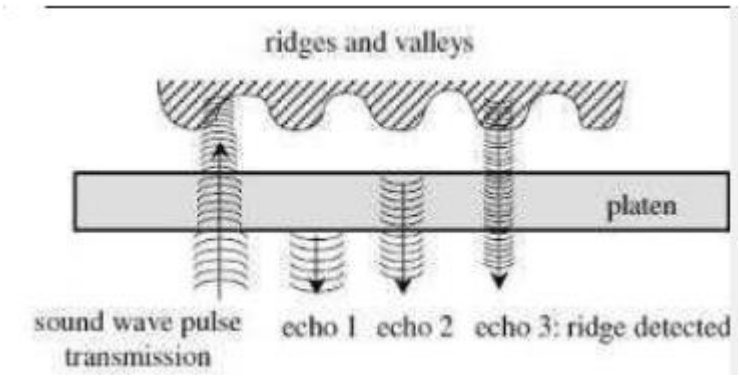


Ilustración 7.Funcionamiento de sensor Ultrasonido (Rubio Báez & Parreño Silva, 2011)

- **Reconocimiento Facial.**

El reconocimiento facial es una técnica basada en identificación sin contacto y además que suele ser empleada en diversos medios y sistemas debido a que su implementación es mediante dispositivos utilizados para capturar imágenes o videos, los cuales se encuentran presentes en diversos componentes facilitando así su implementación. Este tipo de técnica también arroja buenos patrones de aceptación. Existen diversas formas de realizar reconocimiento facial, el escritor segmento las más comunes optando por: Reconocimiento fácil mediante distancias, Reconocimiento Facial por aprendizaje.

Reconocimiento por distancias se basa mayormente en dos dimensiones (2D), este hace una conjunción de hardware y software para examinar las características que tiene un individuo en el rostro. Esta cuenta una colección de imágenes las cuales ayuda a determinar un patrón de resultado, esta colección el autor del libro la denomino data. Para un correcto funcionamiento la data debe contar con estándares que demuestren que la imagen está en

óptimas condiciones, puesto que es de allí donde parten los algoritmos, esto puede ser una gran desventaja en comparación con otras técnicas. No obstante, reconocimiento por distancias, genera una gran aceptabilidad al momento de calcular el patrón de identificación.

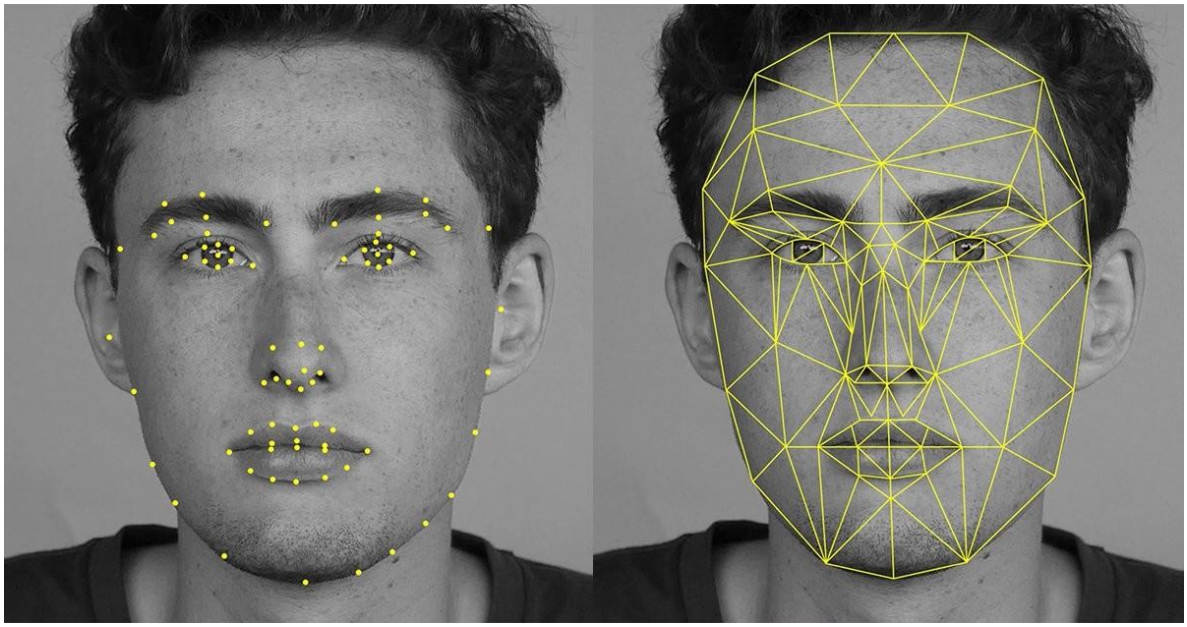


Ilustración 8. Funcionamiento reconocimiento facial por distancias. (xataka)

El reconocimiento fácil mediante aprendizaje, se fundamenta en redes neuronales, las cuales se alimentan hacia adelante multicapas o básicamente perceptrones multicapa. Tiene componentes principales básicos de una red neuronal, una capa de entrada, una o n capas intermedias ocultas y una capa de salida.

- **Arquitectura.**

Para el escritor del libro fue muy importante establecer una arquitectura estable que se adapte a las necesidades que debe asumir el desarrollo del presente proyecto. Uno de los

principales retos para dar progreso a todos los objetivos del proyecto, se basó en el tipo de arquitectura que se empleará para tener como base al momento de construir el prototipo, es decir, como se va comunicar este y cuáles van a ser los parámetros para que se construya un prototipo de fácil despliegue y a un costo bajo.

La Universidad de Pamplona actualmente cuenta con una red que permite la conexión a internet, esta se encuentra desplegada en los tres campus de esta alma mater (Campus principal, sede la casona, sede virgen del rosario) para que estos tengan una comunicación estable entre sí. Esta estructura de red establece conexiones directas desde el campus principal hasta los servidores de esta alma mater, no obstante, tiene restricciones de seguridad ampliando la viabilidad de esta estructura ya preestablecida para ser tomada en consideración como estructura de comunicación para el desarrollo del proyecto.

El modelo OSI “es el modelo de red descriptivo propuesto por la Organización Internacional para la Estandarización (ISO) en el año 1977 y aprobado en el año 1984. Es una normativa formada por siete capas que define las diferentes fases por las que deben pasar los datos para viajar de un dispositivo a otro sobre una red de comunicaciones.” (Solano, s.f.)

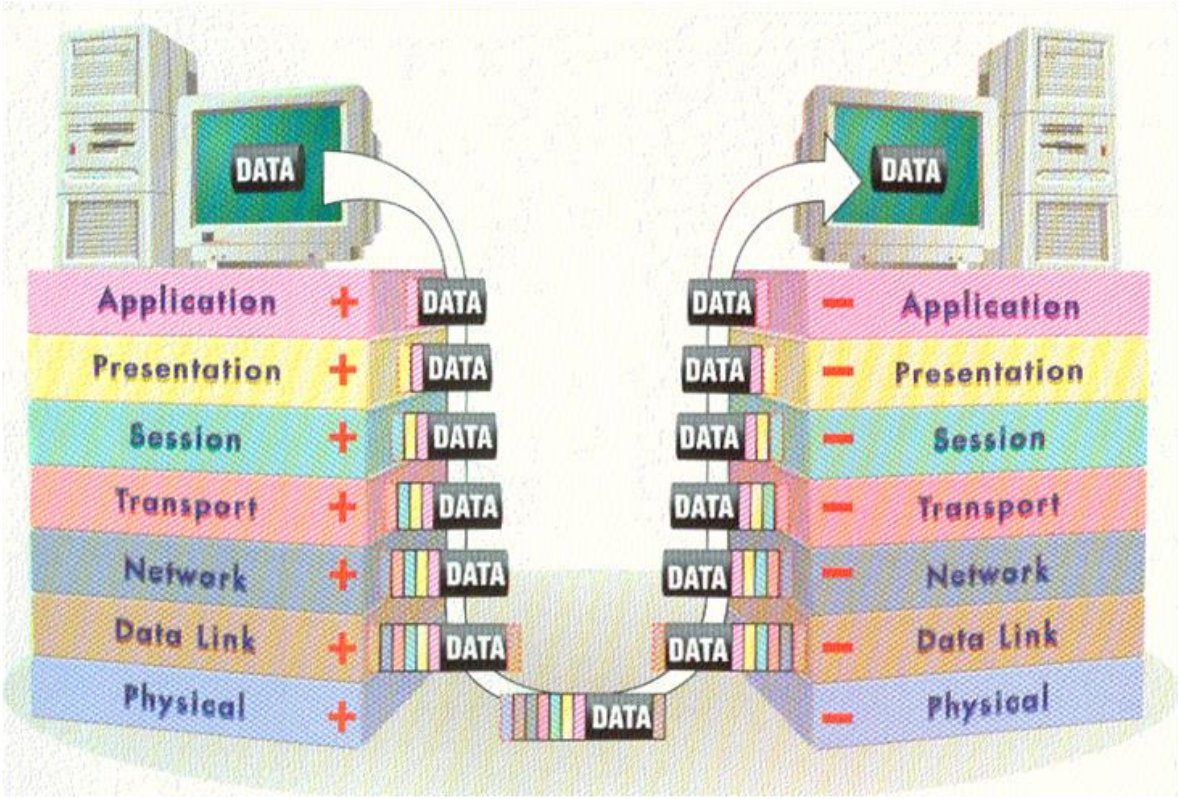


Ilustración 9. MODELO OSI (Jose Solano, DIS).

Si bien es cierto, algunas arquitecturas locales son fácilmente desplegables puesto que la estructura interna no depende de comunicación directa entre dos dispositivos lo cual es ventajoso siempre y cuando no se necesite mantener una comunicación directa entre sí, dando a esto un aligeramiento al momento del manejo de la información en asuntos de seguridad. No obstante, existen despliegues de alto nivel donde si se precisa que la comunicación entre dos dispositivos cumpla con parámetros y lineamientos de funcionamiento como lo serian al momento de realizar una validación. Ahora bien, en el momento de realizar una validación, se envía información la cual debe estar en protocolos de comunicación segura, puesto que estos datos son altamente susceptibles a el intento de hurto de información.

Partiendo del modelo OSI y con la infraestructura de red que cuenta la Universidad de Pamplona para dar acceso a conexión de internet, las capas en las cuales se puede revisar los protocolos que son seleccionables son: Nivel de Transporte, Nivel de Sesión, Nivel de Presentación y Nivel de aplicación.

Las capas de Nivel de Transporte, Nivel de Sesión, Nivel de Presentación, se encuentran agrupadas en la capa de Nivel de transporte en el modelo TCP/IP, no obstante, no todos los autores clasifican de esta manera. Para este libro el autor agrupara estos niveles en el Nivel de transporte. El nivel de transporte "se establece una conexión lógica entre el host transmisor y el host receptor. Los protocolos de transporte segmentan los datos en el host origen para que las capas inferiores realicen el envío y una vez que estos llegan a su destino, son ensamblados para recuperar el mensaje original, brindando de esta manera un transporte de extremo a extremo." (Gonzalo Hernández Hernández, s.f.)

En lo que corresponde al Nivel de transporte, los protocolos encargados de realizar el transporte de los datos son dos TCP y UDP, consolidando una breve descripción de TCP, es el Protocolo de Control de la Transmisión (Transmission Control Protocol por sus siglas en inglés) este es un estándar el cual está encargado de mantener una conexión donde se realizan los intercambios de mensajes de forma estable realizando el control de errores, este también se encarga de decidir cómo se dividen los paquetes de envió, realiza control de flujo y además maneja la retransmisión de los datos perdidos.

El Protocolo de Datagrama de Usuario (User Datagram Portocol por sus siglas en inglés) UDP, este también es un estándar y se encuentra en la capa de nivel de transporte, está basado en el envío de información sin establecer una conexión previa entre dos puntos de conexión o más, no cuenta con control de flujo, tampoco cuenta con control de errores, convirtiéndolo en un protocolo de difusión masiva.

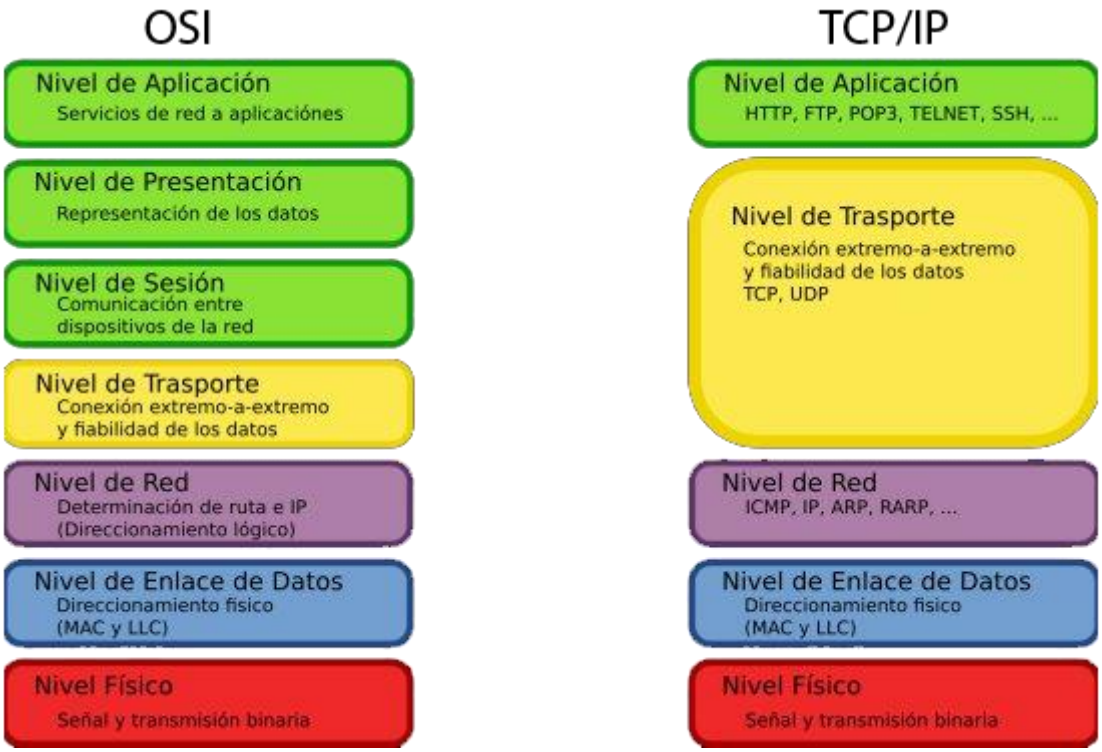


Ilustración 10. Modelo OSI contra TCP/IP. (Universidad Autónoma del Estado de Hidalgo)

- **Características del usuario.**

En el alcance del proyecto se definió a groso modo donde se implementaría, no obstante, no se han mencionado las características con las cuales cuentan los usuarios. En primer lugar, el usuario final tendrá género masculino o femenino, también contará con conocimientos básicos en informática y estará inscrito y cursando una carrera ofertada por la Universidad de Pamplona.

- **Coste base para reconocimiento facial.**

El costo de este va ligado principalmente a qué tipo de tecnología se va implementar, puesto que existen diversidad de tipos de cámaras. En primer lugar, existen cámaras CCTV que se caracterizan principalmente por ser diseñadas para seguridad, esta no está alimentada directamente por comunicación IP, su conexión va a un punto de inicio (Grabador) que este posteriormente lanza conexión a internet. También existen las cámaras IP funcionan mediante las redes locales (LAN), su implementación es barata porque no necesariamente necesitan de un punto central (Grabador) para funcionar, estas permiten estar conectadas a internet. Cabe aclarar que se buscó el costo base de cada una de las diferentes cámaras en páginas de venta por internet únicamente para tenerlas como referencia, puesto que no sería el mismo costo en el que la Universidad de Pamplona las compraría por el tipo de contratación al ser una entidad pública. Por otra parte, las cámaras debían tener las especificaciones sugeridas por el equipo de desarrollo del CIADTI, que fueron cámaras PTZ-mini y que tengan buena resolución.

Costo de una cámara CCTV (febrero-18-20202)

Estas imágenes fueron importantes para tener un punto de referencia de variación del coste. Se tomaron dos tiendas de venta online, una nacional y otra internacional.

MercadoLibre:

Cámara Cctv Tetrahíbrida Full Hd, Tipo Domo | Cctv-1120
por Steren

$ 114.900

36x $ 3.192

Envío gratis

Amazon:

Patrocinado

XVIM 1080P HD Cámara CCTV interior al aire libre resistente a la intemperie Cámara de seguridad para el hogar 24 LEDs IR de 85 pies de visión nocturna, puede ajustar el modo de soporte...

★★★★☆ 9

COP65,670 ~~COP69,535~~

Con envíos a Colombia

- **Coste base para reconocimiento dactilar.**

El costo de este va ligado principalmente a qué debía contar con un medio que permita la comunicación directa con el servidor o punto de acceso, esto hace que el dispositivo tenga

un coste más alto de implementación. Para esto el autor del libro en conjunto con el equipo de desarrollo del CIADTI, optaron que se realizara el estudio con Arduino como punto de comunicación. Cabe aclarar que se buscó el costo base de cada uno de los diferentes sensores de lectura para huella digital, Arduino y componentes extras en páginas de venta por internet únicamente para tenerlas como referencia, puesto que no sería el mismo costo en el que la Universidad de Pamplona las compraría por el tipo de contratación al ser una entidad pública. Estas imágenes fueron importantes para tener un punto de referencia de variación del coste. Se tomaron dos tiendas de venta online, una nacional y otra internacional.

Costo de un sensor óptico de huella digital (febrero-18-20202)

MercadoLibre:

Lector Optico Huella Digital Biometrico Arduino

$ 60.000

Hasta 12x $ 5.000 sin interés

Envío gratis

Amazon:

Lector de huellas dactilares óptico Módulo de bloqueo de puerta Control de acceso de la luz roja para Arduino Mega2560 UNO R3 Geekstory

★★★½☆ 23

COP 72,616

Costo Arduino y componentes. (febrero-18-20202)

MercadoLibre:

Arduino Uno R3 Con Cable Usb

$ 26.000

Hasta 12x $ 2.167 sin interés

Bogotá D.C.

Modulo Ethernet Shield:

Ethernet Shield W5100 Arduino

$ 23.000

Hasta 12x $ 1.917 sin interés

Bogotá D.C.

Amazon:

Programming Arduino: Getting Started with Sketches, Second Edition (Tab)
por Simon Monk | 9 junio 2016
519
Pasta blanda
Kindle
COP34,290 COP57,662

Modulo Ethernet Shield:

DEVMO Ethernet Shield LAN W5100 para Arduino Board UNO R3 ATMega 328 MEGA 1280 2560
3
COP53,779
Con envíos a Colombia

4 Definición base.

Como resultado del capítulo 3, se obtiene las bases fundamentales para realizar la toma de decisiones sobre qué tipo de biometría se debe seleccionar para llevar a cabo el diseño del prototipo. Este capítulo describe como el autor seleccionó el tipo de biometría realizando un análisis costo beneficio para generar un mayor beneficio a la Universidad de Pamplona, además, la comparativa de herramientas que realizan la implementación de la técnica a la arquitectura.

La arquitectura física de comunicación se definió nuevamente en una reunión con el equipo administrativo del CIADTI, las bases fundamentales fue implementar la estructura cableada de red que tiene desplegada actualmente la Universidad de Pamplona, siendo esta la que permitiría el acceso directo desde el punto de toma de datos, sin importar el tipo de biometría, permitiendo así realizar adaptaciones modulares en futuros proyectos.

4.1 Selección tipo de biometría.

Para la selección de esta, inicialmente se realizó una exploración de las diferentes técnicas que se adaptaban a la intención del prototipo, la cual es que sea fácil de implementar y de usar en cuestión de practicidad para el usuario (docente o estudiante) con el fin de no generar cuellos de botella, además, la decisión se basó en la técnica que cumpliera con los siguientes parámetros: Facilidad de acceso, Facilidad de implementación, Costos bajos,

recomendaciones de otros autores y completitud de la herramienta. Dando como resultado la técnica de reconocimiento Facial.

- **Principios para realizar la comparativa.**

Como primera instancia se descartaron algunos tipos de biometría, que, si bien demuestran buenos resultados al momento de identificar o autentificar un usuario, resultaban ser cuello de botella al implementar, por ejemplo, partiendo de biometría mediante reconocimiento de iris, esta es una técnica de alto coste monetario, de difícil implementación y de poca practicidad, puesto que el autor del libro considera que se presentarían filas en la identificación debido a la composición y estructura del dispositivo que está encargado de realizar la detección, además, este dispositivo se hace difícil su adquisición en forma masiva. Otros tipos de biometría que para su implementación requiera tecnología de alto coste o de difícil adquisición también está descartada.

El autor seleccionó para realizar la comparativa dos técnicas: Biometría mediante reconocimiento de iris y Biometría mediante reconocimiento facial.

- **Identificar las ventajas y desventajas de cada tipo.**

Para realizar la comparativa se partió de escritores que ya hubieran realizado estudios a estas técnicas, bajo estos el autor decide plasmar las ventajas y desventajas partiendo estos junto a otros criterios, dando como resultado las siguientes tablas:

Biometría por reconocimiento dactilar.

Ventajas	Desventajas
• El reconocimiento dactilar es uno de los más empleados en el mundo, debido a su eficacia al momento de hacer coincidencia. • La tecnología a emplear es de bajo coste. • Es difícilmente falsificable. • Es de fácil implementación	• Reconocimiento dactilar se encuentra sujeto fallos cuando el usuario presenta cortaduras, sudor o piel seca. • Los cuellos de botella no se eliminan por completo. • Realiza contacto directo, lo cual permite la transmisión de gérmenes o bacterias.

Biometría por reconocimiento facial.

Ventajas	Desventajas
• El reconocimiento del rostro puede ser implementado de forma pasiva. • La implementación se adapta muy bien al modelo de control de asistencia. • La adquisición de la imagen es más fácil. • No requiere de contacto lo cual genera que sea una técnica de biometría higiénica. • La tecnología es fácilmente conseguible. • Su implementación está pensada en interiores, por su fácil operación.	• Este sujeto a fallos cuando el usuario presenta elementos que no permitan una toma clara del rostro • La toma de imágenes debe ser de buena calidad. • Depende del algoritmo, es decir la forma como el algoritmo realice el reconocimiento.

Estas ventajas y desventajas son tomadas de referencia de los autores Jorge Rafael Valvert Gamboa (Métodos y técnicas de reconocimiento de rostros en imágenes digitales bidimensionales, 2006), Salvatierra Tumbaco Gabriel (Desarrollo de un sistema de control

de asistencia estudiantil mediante reconocimiento facial, 2018/) y de algunos sitios web únicamente como criterios.

- **Relación coste beneficio.**

Con las ventajas y desventajas definidas, se plasmaron algunas métricas de medición extra, además, algunas fueron tomadas en consideración por el autor y otras fueron propuestas por el equipo de desarrollo del CIADTI.

Para dar inicio a la comparativa se definen los siguientes criterios y sus pesos, los cuales son tomados a consideración de reuniones y por parte del autor, para la matriz de relación costo beneficio cualitativa:

1. Costo base de implementación, para este criterio el autor se basó en el coste de los componentes que se enunciaron en el capítulo anterior, para definir el valor de cada alternativa.
2. Probabilidad de aciertos, este criterio es uno de los más importantes, el autor tomó como referente otros autores e información oficial para realizar la medición.
3. Facilidad de integración con la arquitectura física, para este criterio el autor le da la máxima importancia, puesto que este criterio puede alterar altamente los costos.
4. Usabilidad, este criterio se le da un peso asignado por reunión con alguno de los miembros del equipo de desarrollo del CIADTI.

5. Higiene de su uso, este aspecto tendrá un peso medio puesto que algunos tipos de biometría podrían involucrar el transporte de enfermedades o gérmenes.
6. Durabilidad, los valores asignados a este criterio fueron establecidos en reunión con el equipo de desarrollo del CIADTI.
7. Existencia de información, este criterio es altamente considerado por el autor, puesto que la inexistencia de datos (imágenes, información codificada) puede ser un punto de fluctuación al momento de implementar.

Factor		Alternativas	
Descripción	Peso	Reconocimiento dactilar	Reconocimiento facial
Costo base de implementación	7	6	6
Probabilidad de aciertos	8	9	8
Facilidad de integración con la arquitectura física	10	5	8
Usabilidad	6	8	6
Higiene de su uso	8	5	9
Durabilidad	6	9	9
Existencia de información	7	0	6
		306	390
		58,84615385	75

Para el criterio de existencia de información su valor fue 0 puesto que no existe información alguna de los estudiantes de la universidad de pamplona de huellas dactilares. Además, no toda la información existente de fotografías de los estudiantes está bien actualizada.

Para el criterio de Probabilidad de aciertos el autor se basó en la siguiente información.

“NEC Corporation líder en la integración de tecnologías de red y TI, anunció el pasado 3 de octubre que su tecnología de reconocimiento facial logró la mayor precisión de coincidencia en la Prueba de Reconocimiento de Rostro (FRVT) 2018, la cual fue realizada por el Instituto Nacional de Estándares y Tecnología (NIST) de EE. UU., con una tasa de error del 0,5% al registrar a 12 millones de personas.” (NEC, 2018), considerando que NEC es una empresa con más de 30 años probando a las agencias gubernamentales. Este es una taza de error muy baja teniendo en cuenta que el sistema se despliega en áreas comerciales.

Otro referente para la toma de esta decisión, fueron las pruebas realizadas por Daniel Castro y Juan Pablo Pallo en su estudio denominado, Sistema de Control de Acceso al Personal Mediante Reconocimiento Facial. En este mencionan que obtuvieron resultados de acierto de un 93.33 % en base a 30 personas, dando el contraste de algoritmos altamente entrenados y creados para el desarrollo de reconocimiento facial como el empleado por NEC, contra algoritmos más jóvenes.

Ahora bien, en sistemas de reconocimiento dactilar suelen existir inclusive Hardware que realiza la identificación de forma automática, por lo cual el autor del libro se basó en los siguientes escritos, “Los sistemas de reconocimiento de huellas suelen ser muy seguros y

rápidos, especialmente cuando hay que identificar un individuo entre muchos (por ejemplo 1 entre 1000). Esto se debe fundamentalmente a que las características biométricas de las huellas son precisas y no varían o lo hacen muy poco" (imesd, s.f.), IMESD, es una empresa encargada de realizar control de presencia y acceso a trabajadores de algunas empresas. En el estudio realizado por Manuel Ocaña Diez de la Torre cuyo título es ALGORITMOS DE MATCHING ENTRE HUELLAS DACTILARES, realiza el estudio de precisión usando algoritmos FVC para la coincidencia, obtiene un 95% de precisión. Para este tipo de técnica de reconocimiento biométrico se ve el contraste un poco más bajo del uso de algoritmos comerciales contra algoritmos más jóvenes.

En base a esta relación costo beneficio cualitativa, el autor del libro seleccionó como técnica biométrica reconocimiento facial.

4.2 Selección tipo de herramienta.

Partiendo de la selección del tipo de biometría, el autor realizo una búsqueda de los algoritmos, bibliotecas, frameworks, más comunes, reviso cada uno de los siguientes para realizar la comparativa.

- **Open Face**

Este algoritmo está basado en FaceNet, un proyecto que está a cargo por parte de los investigadores de Google siendo este el máximo referente en cuestión de reconocimiento

facial, Open Face le han realizado pruebas con 6000 imágenes y ha generado resultados de precisión de un 87% (genbeta, s.f.) en algunos segundos. Además, la implementación de este código tiene alta complejidad.

- **Face Recognition**

Esta biblioteca cuenta con distintas herramientas, las cuales se emplean para realizar el reconocimiento facial, puede hacer reconocimiento de caras e identificación empleando aprendizaje profundo mediante dlib, esta biblioteca cuenta con una precisión de 99.38% (Geitgey, s.f.), con reconocimiento en tiempo real, además con fácil integración e implementación, también tiene distribución de núcleos y tolerancia a errores, una biblioteca bastante completa.

- **TensorFlow**

Esta biblioteca está dirigida al aprendizaje automático, esta fue desarrollada por Google, también implementa dlib para el aprendizaje profundo y emplea módulos de FaceNet, también de Google, “nuestro sistema logra una nueva precisión de registro de 99,63%.” (Florian Schroff, 2015), este algoritmo emplea diferentes tipos de aprendizaje profundo.

Para la selección del tipo de herramienta el autor se basó en los porcentajes de coincidencia que menciona cada librería y la compatibilidad que presenta con el sistema operativo que cuenta actualmente el CIADTI, si bien es cierto que TensorFlow ofrece un

porcentaje más alto, su instalación presentó problemas de compatibilidad con la arquitectura seleccionada y el sistema operativo destinado. Para la selección se realizó una reunión con el equipo de desarrollo del CIADTI, en esta se plasmaron las compatibilidades de las herramientas y la que generaba mejor resultado teórico, dando como resultado Face Recognition puesto que no presento ningún inconveniente con la compatibilidad y además que cuenta con un nivel alto de coincidencia.

- Pruebas realizadas a Face Recognition.

Para las pruebas realizadas del algoritmo son funcionales, puesto que se enfatizó en ver el funcionamiento de la herramienta, estas se les realizaron a los compañeros Hugo Alexander Parada Orjuela y Mario Alejandro Rangel Guerrero, y que bajo su consentimiento aceptaron y autorizaron el uso de las siguientes imágenes.

Imágenes que el algoritmo usa como base para realizar la coincidencia.

Ilustración 11. Foto base Mario Alejandro Rangel

Ilustración 12 Foto base Hugo Alexander Parada Orjuela.

Se tomaron las siguientes imágenes para buscar coincidencias.

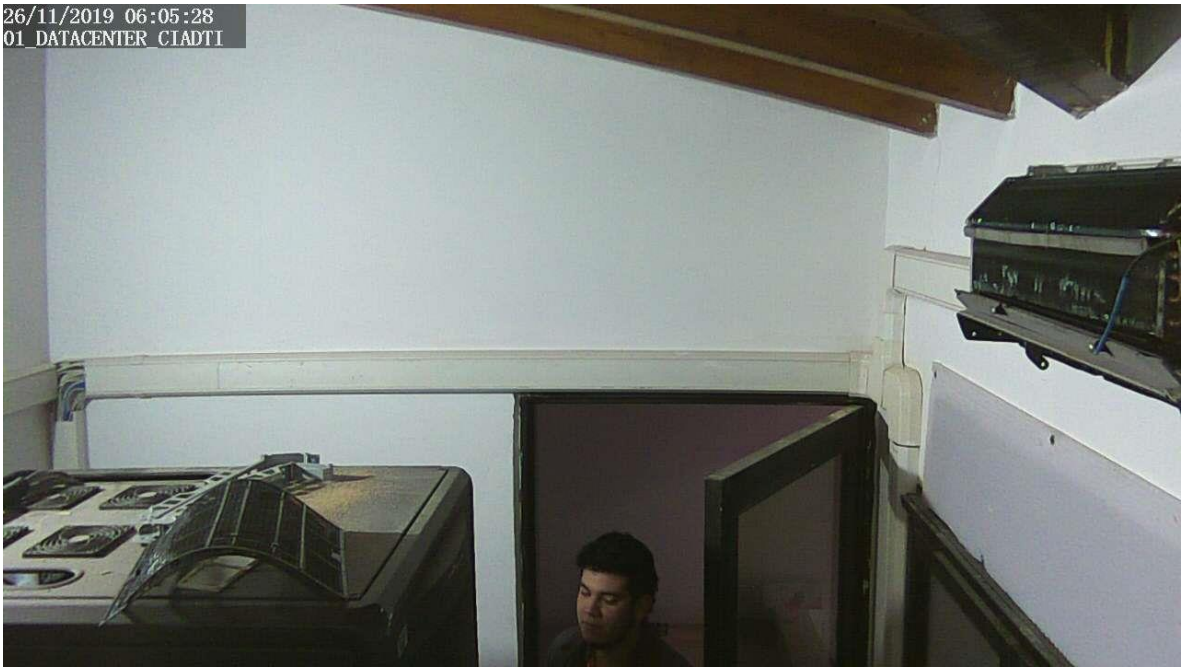


Ilustración 13 Foto desconocida para el algoritmo de Mario.

Ilustración 14 Foto desconocida para el algoritmo de Hugo.

El tipo de prueba al ser de tipo funcional es una de tipo caja negra, por consecuente se busca probar la funcionalidad del algoritmo. Al finalizar las pruebas se obtuvo como resultado la coincidencia en ambas imágenes, cabe aclarar que, si bien es cierto que el algoritmo es capaz de obtener coincidencias de una forma bastante aceptable, también pueden existir variación puesto que está ligado a la posición de la cara de las personas.

Ilustración 15 Foto coincidencia de Mario.

Ilustración 16 Foto coincidencia de Hugo.

5 Diseño

En el capítulo 4 se consolido el tipo de biometría junto con la herramienta, además, en el capítulo 3 también se estableció el tipo infraestructura de comunicación. No obstante, la integración de todos estos compendios no está aún materializada. En este capítulo se detalla la forma en que el autor del libro realizó la integración, describiéndolo en algunos segmentos.

5.1 Arquitectura de comunicación.

La arquitectura de comunicación que se empleó para el diseño del prototipo es mediante API, la cual tiene la capacidad de transmitir y recibir información de forma sencilla y eficaz, puesto que esta arquitectura se adecua muy bien a la proyección que el autor del libro tiene. A groso modo una descripción para las API es “Son como las funcionalidades que aporta un cierto servicio software facilitando que pueda ser utilizado por otro software para mejorar sus resultados.” (Sheila Plaza Estévez, Nerea Ramírez Lamela, Carmen Acosta Morales). El beneficio que obtiene el prototipo al emplear este tipo de arquitectura, es que tiene un fácil despliegue y una fácil integración, puesto que la intención de este tipo de arquitectura es poderse comunicar entre sistemas, entonces, puede ser fácilmente integrándolo con la plataforma que se requiera. Para el diseño del prototipo, el autor del libro empleó el uso de Python como lenguaje base.

- **Servidor HTTP**

El servidor seleccionado fue FLASK, este es un framework minimalista que cuenta con la capacidad de crear sitios web rápidamente, no obstante, el autor del libro recomienda emplear servidores mucho más sofisticados.

El servidor estará encargado de dar respuesta a las peticiones según el método POST o GET en este caso, no obstante, existen más métodos de peticiones. El servidor estará encargado de generar una respuesta con un código HTTP, este código se encuentra encargado de llevar información alusiva a la respuesta de una petición realizada, además, de cuerpo de respuesta.

- **APIS**

  La comunicación se estableció mediante el uso de JSON, siendo este un formato de texto sencillo para el intercambio de datos, como estructura de transferencia. Se emplearon dos métodos de acceso, mediante POST y GET, los cuales se describen así:

  - POST:

  Nombre: Reconocimiento.

  Este API está encargada de validar que el usuario mediante reconocimiento facial coincida con el de la base de datos mediante el documento.

  - El protocolo es HTTP.
  - La estructura de los datos al enviar es:

    {“codigo” : “123456789”}

  - El punto de acceso:

    Localhost/api/v1/reconocimiento

  - Los datos de respuesta son:

Código HTTP: 200 {“rsp”: “Usuario valido.”}

Código HTTP: 400 {“rsp”: “Datos erroneos.”}

Código HTTP: 403 {“rsp”: “Usuario no autorizado.”}

- GET:

  Nombre: Reconocimiento.

Este API está encargada de validar que usuarios mediante reconocimiento facial estén presentes en una imagen captada por el servidor.

- El protocolo es HTTP.
- El punto de acceso:

  Localhost/api/v1/reconocimiento

- Los datos de respuesta son:

  Código HTTP: 200 {“data”: [123, 1234, 123456]}

  Código HTTP: 204 {“rps”: “No se encontró ningún usuario.”}

- **Toma de imágenes.**

  Ahora bien, el acceso mediante APIS facilita las solicitudes, pero antes de proseguir con el cómo integrar, se definió el procedimiento para responder a la pregunta ¿Cómo acceder a la toma de imágenes sin la necesidad de un intermedio?, el autor del libro bajo una investigación amplia, encontró la existencia del protocolo RSTP, este “define diferentes tipos de conexión y diferentes conjuntos de requisitos, para intentar conseguir siempre un envío de flujo de datos a través de redes IP lo más eficiente posible. Además, establece y controla uno o más flujos sincronizados de datos como audio y video. A tal

fin se definió el uso de sesiones, mediante identificador único, en este protocolo" (David Mateos Costilla, Samuel Reaño Montoro , 2008).

- **Integración de arquitectura de comunicación.**

  En este punto el autor definió el diseño del modelo de la arquitectura de comunicación, para realizar un proceso automático con los procedimientos anteriores, no obstante, el acceso a la base de datos aún no está plasmado. El acceso a la base de datos se implementa mediante una estructura monolítica "de forma muy resumida, puede decirse que la arquitectura monolítica es aquella en la que el software se estructura de forma que todos los aspectos funcionales del mismo quedan acoplados y sujetos en un mismo programa." (viewnext s.a, 2018), la cual realiza acceso a la base de datos y solicita según el método del API, la información. Ahora bien, el momento de ejecución o de solicitud el autor lo establece incorporando el llamado desde el CRONTAB, "Crontab es un fichero de texto que guarda una lista de comandos a ejecutar en el tiempo especificado por el usuario. Crontab verificará la fecha y hora a la que se debe ejecutar el comando y los permisos de ejecución. Esta es la manera más sencilla de administrar tareas de cron en sistemas multiusuario ya sea como un usuario normal o como root." (Isabel Mª Cano Jordán), el cual ejecutara los llamados GET, según las tareas programadas.

El siguiente diagrama hace una representación de la arquitectura física propuesta por el autor de forma local.

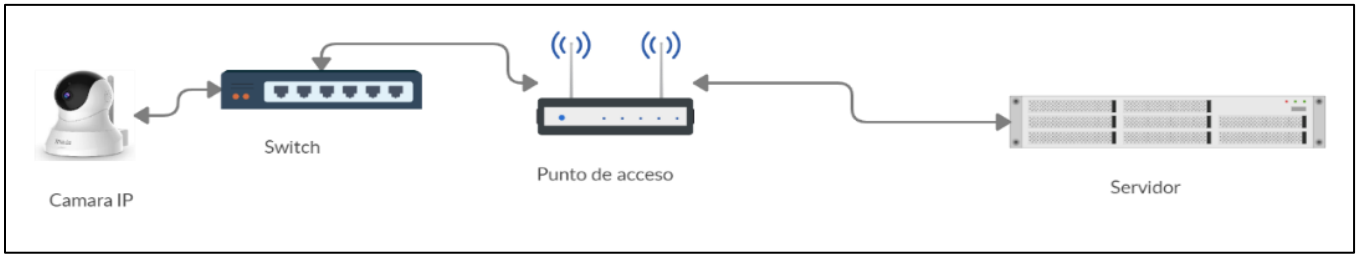


Ilustración 17. Arquitectura de red local.

El siguiente diagrama hace una representación de la arquitectura API propuesta por el autor.

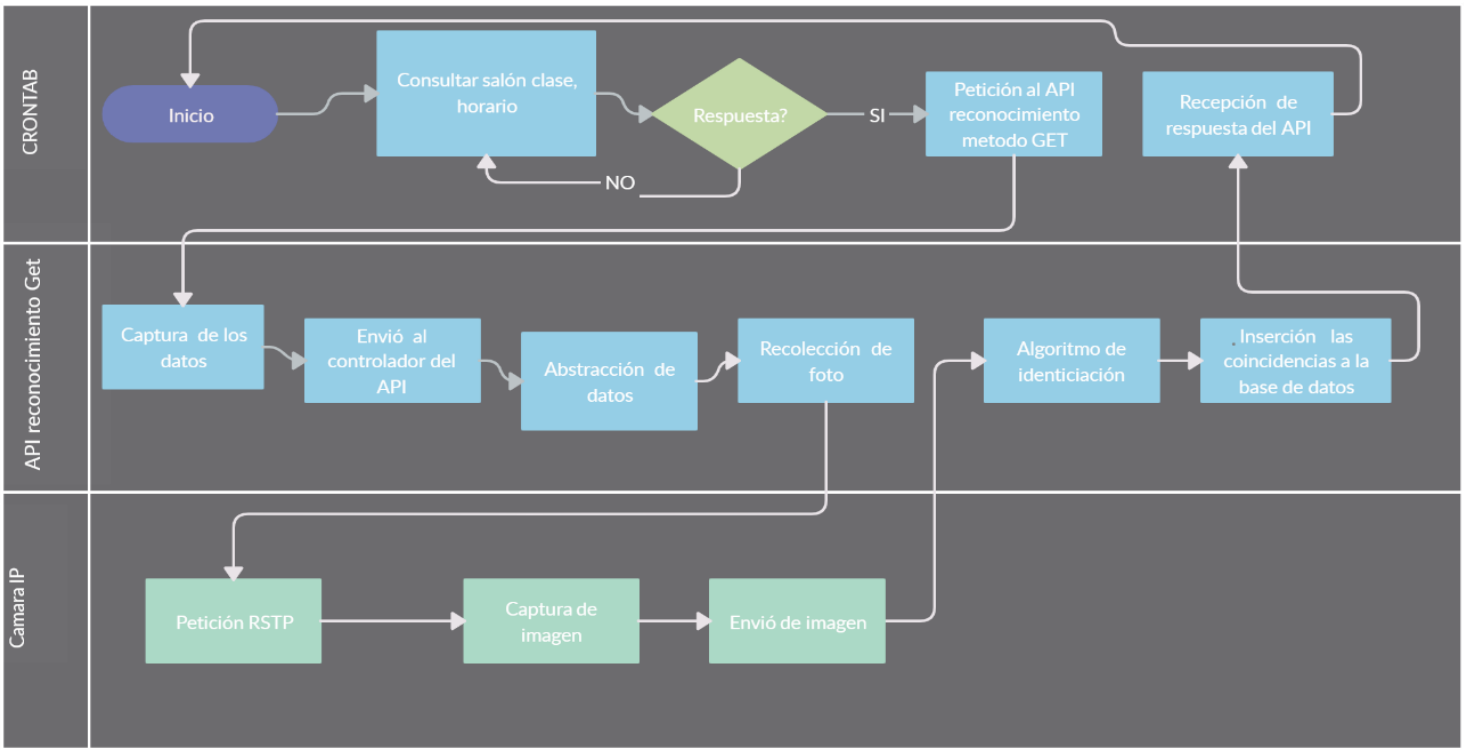


Ilustración 18. Representación API reconocimiento, método GET.

- **Descripción de las acciones.**

- Consultar salón, clase, horario.

  En este procedimiento el sistema realiza una petición a la base de datos buscando según la hora actual, que clase está en curso, en el bloque FJ salón 103, obteniendo como resultado el código del salón, código de la materia.

- Captura de los datos.

  Recolecta los datos desde el llamado al API, los estructura para su posterior análisis o procesamiento.

- Envió al controlador del API.

  Envía la información al controlador correspondiente, partiendo del tipo de petición.

- Abstracción de datos.

  En este procedimiento descarta información poco relevante, buscando con los parámetros de ingreso (salón, clase, horario) los usuarios que coincidan con este. En este procedimiento también se tiene muy en cuenta que la información que se obtiene de la base de datos sea el código del estudiante y la ruta donde está la data de imágenes a comparar como datos más relevantes.

- Recolección de foto

  Gracias a que algunas cámaras IP cuentan con el protocolo RSTP, para este procedimiento se realiza una petición mediante este, la cámara a la cual enviar esta petición es recibida como parámetro de ingreso con la información del salón. Por otro

lado, se pueden realizar peticiones Http a una cámara enviándole parámetros, por ejemplo:

cgi-bin/CGIProxy.fcgi?cmd=INSTRUCCIÓN

Mediante esta petición la cámara recibe comandos, los cuales están definidos por cada fabricante junto con su funcionalidad.

- Captura de imagen y Envió de imagen.

  Estos son procedimientos internos de la cámara, pero generan como resultado una imagen de la cámara, la cual es enviada al servidor que ejecuto la petición.

- Algoritmo de identificación.

  Este recibe como información de entrada, la imagen del salón de clases, las direcciones de las imágenes de cada estudiante junto con su código, realiza la ejecución del algoritmo y genera una respuesta dando como resultado un JSON de coincidencias.

- Inserción de las coincidencias a la base de datos.

  Para este procedimiento se realiza una validación determinando si existieron o no coincidencias en el paso anterior, de existir coincidencias realiza la inserción a la base de datos, para generar una respuesta satisfactoria, de lo contrario, se envía una respuesta negativa.

- Recepción de respuesta del API.

Este es el último paso, en este caso el algoritmo revisa la respuesta por parte del API, si la respuesta fue satisfactoria da por terminado el procedimiento, si el algoritmo no encontró coincidencias reinicia el proceso.

- **Modelo de bases de datos.**

El autor propone el siguiente modelo de bases de datos como ejemplo de la base de datos que podría emplearse.

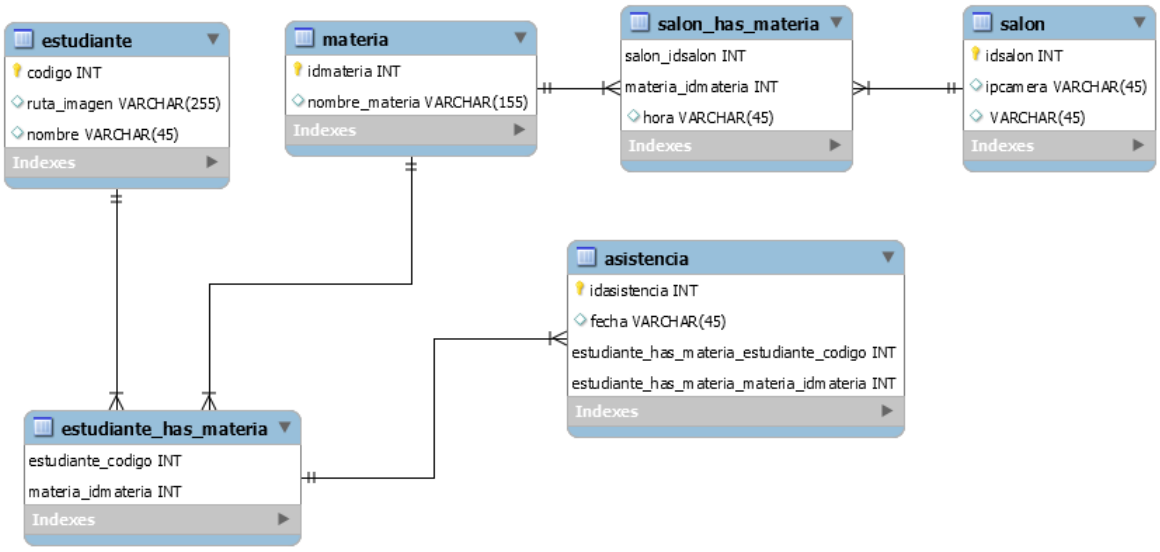


Ilustración 19. Modelo de base de datos.

Este modelo es una pequeña adaptación, puesto que el modelo real que implementa la Universidad de Pamplona no es de acceso al público por políticas internas de esta alma mater, entonces el autor realizo una pequeña adaptación de la estructura que debería contener un modelo en caso de ser necesaria la replicación.

5.2 Algoritmo de reconocimiento.

En el capítulo anterior se realizó la selección del algoritmo face recognition, una biblioteca que se basa internamente en aprendizaje profundo para realizar la detección de coincidencia con un rostro. Esta biblioteca se junta con OPENCV, “es una biblioteca de software de aprendizaje por computadora y visión por computadora de código abierto. OpenCV se creó para proporcionar una infraestructura común para aplicaciones de visión por computadora y para acelerar el uso de la percepción de máquinas en los productos comerciales. Al ser un producto con licencia BSD, OpenCV facilita a las empresas utilizar y modificar el código.” (OpenCV, s.f.), además el autor del libro recomienda el uso de PYTHON y la implementación en Linux, puesto que presenta menos inconvenientes de compatibilidad.

- **Procedimiento de instalación**

Inicialmente se debe contar con unos requisitos para su instalación, el autor del libro recomienda el uso de CENTOS en su distribución 7 y contar en el sistema con los siguientes requisitos.

- PIP 3, que es un instalador de paquetes de Python.
- CMAKE, “es una familia de herramientas multiplataforma de código abierto diseñada para crear, probar y empaquetar software.” (cmake, s.f.)
- DLIB, “es un kit de herramientas moderno de C ++ que contiene algoritmos de aprendizaje automático y herramientas para crear software complejo en C ++ para resolver problemas del mundo real.” (DLIB, s.f.)

Estos requisitos básicos preinstalados minimizan el riesgo de fallo de incompatibilidad. Para realizar el proceso de instalación automático se emplea el siguiente comando.

```
pip3 install face_recognition
```

Con esto se añade la biblioteca al sistema para que este quede en ambiente, lo cual significa que este se puede acceder desde cualquier parte del sistema sin tener que referenciarlo, no obstante, las versiones pueden generar problemas de compatibilidad, por lo cual la recomendación del autor es tener todo en su última versión.

- **Funcionamiento básico.**

Esta biblioteca está fuertemente centrada en el reconocimiento de rostros, para realizar la descripción del funcionamiento, partiendo de la arquitectura de comunicación definida anteriormente, primeramente, el algoritmo recibe como datos de entrada los códigos de los estudiantes conocidos y la ruta de la imagen de cada uno de ellos, consiguiente a esto realiza un ciclo para codificar las imágenes, de la siguiente forma realizó la codificación de las imágenes.

```
face_recognition.face_encodings(estudiante)[0]
```

Posterior a esto se realiza el cargue de la foto tomada en la cámara IP. Para realzar la toma de la cámara desde el servidor en el procedimiento de Recolección se realiza mediante el siguiente URL,

```
URL=http://IP/cgi-bin/CGIProxy.fcgi?cmd=snapPicture2&usr=USUARIO&pwd=CLAVE
```

Esta imagen se codificó siguiendo el mismo funcionamiento de codificación del algoritmo, posteriormente, se debe conseguir la ubicación de los rostros de la imagen tomada por la cámara IP, esto se realizó así,

```
face_locations = face_recognition.face_locations(unknown_image)
```

Ahora se realiza un ciclo para coincidir por comparación de existencias generada, de no coincidirse realiza una validación mediante distancias. Si el algoritmo encuentra coincidencias guarda la posición de coincidencia, para posteriormente guardar el estudiante en un array con el documento. Las dos formas de encontrar coincidencias son las siguientes.

```
matches = face_recognition.compare_faces(known_face_encodings, face_encoding)
face_distances = face_recognition.face_distance(known_face_encodings, face_encoding)
```

Esta sería una explicación a groso modo del funcionamiento de la biblioteca FACE RECOGNITION, el autor del libro recomienda revisar la documentación y ejemplos de uso del algoritmo, en sus repositorios oficiales.

- **Prueba.**

El prototipo se ejecutó realizando un llamado al API mediante POST, enviando el documento 123456789 que estaba ligado a la siguiente imagen. Cabe resaltar que estas imágenes fueron tomadas bajo autorización de Mario Alejandro Rangel.

Ilustración 20. Foto base de Mario Rangel ligado al documento 123456789.

La imagen esta guardada en la misma ruta de ejecución del proyecto, esta imagen se toma del mismo carnet que genera la Universidad de Pamplona, se hace el cambio de código para proteger los datos personales del mismo.

La imagen que capto el servidor fue la siguiente.

Ilustración 21.Imagen captada por el servidor de Mario Rangel.

Se realizó la ejecución del algoritmo, dando como resultado la coincidencia de este, el autor del libro efectuó modificaciones sobre el algoritmo para que generara una imagen con la coincidencia encontrada y el código, dando como resultado,

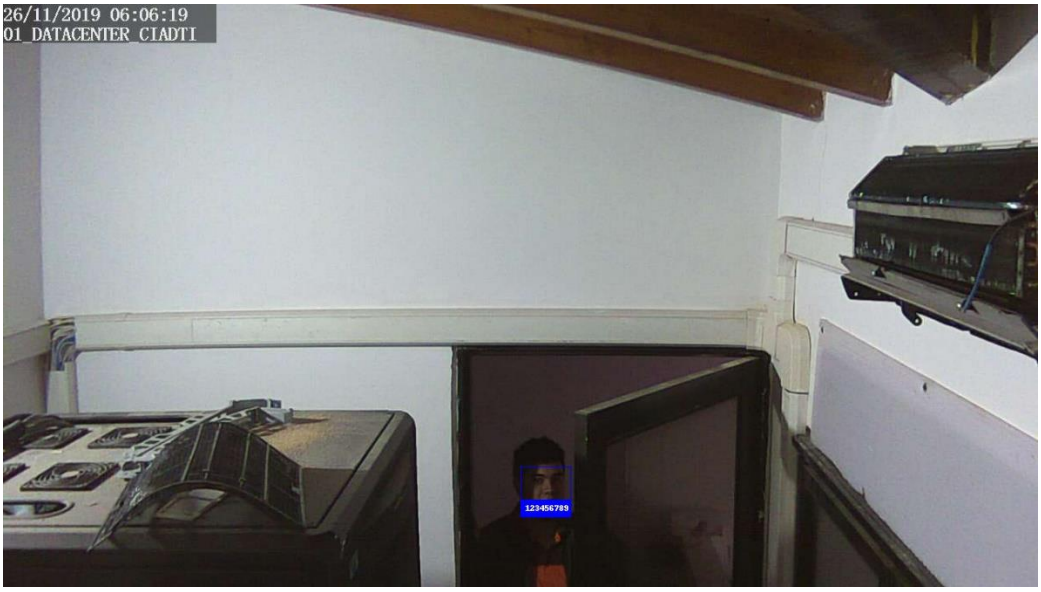


Ilustración 22.Imagen generada por el algoritmo.

Esta prueba es una simulación realizada del funcionamiento correcto del prototipo, el autor realizó diferentes pruebas, al final selecciono la que fuera más difícil de identificar bajo su criterio.

6 Conclusiones

- Con base en los aspectos referentes a biometría plasmados en este documento se pudo establecer la selección de un tipo de biometría compatible con la arquitectura física que presenta la Universidad de Pamplona.
- El estudio de las herramientas de reconocimiento facial determinó a la biblioteca de Face Recognition, puesto que esta biblioteca representaba más facilidad de integración con los sistemas actuales del CIADTI.
- Se diseñó un prototipo capaz de integrarse de forma sencilla con el sistema que cuenta actualmente la Universidad de Pamplona e inclusive con la arquitectura de comunicación física existente en las tres sedes de esta alma mater.
- El uso de las API facilita en gran parte el proceso de desarrollo, puesto que permite la integración de dos sistemas de una forma sencilla, además, ofrecen un buen rendimiento.

7 Recomendaciones y trabajos futuros

- Como trabajo futuro se pretende implementar y validar el prototipo diseñado.
- Emplear la combinación entre varios tipos de algoritmos buscando así tener más coincidencias, esto con el fin de hacer un prototipo que se base en múltiples maneras de hacer coincidencia. No obstante tener en consideración el reusó del servidor.
- Cambiar el protocolo RSTP por un protocolo más actualizado, u otra forma de transmisión de STREAMING.

8 Bibliografía.

alexander rojas manrique, s. e. (2018). *prototipo de sistema de control de acceso y monitoreo automatizado para el laboratorio de redes y electrónica del iser de pamplona.* pamplona, colombia.

alvaro javier balsero meneses, c. g. (2016). *diseño e implementación de un prototipo para el control de acceso en la sede de ingeniería de la universidad distrital francisco josé de caldas mediante el uso de torniquetes controlados por carnet con tecnologia nfc y lector biométrico de huella dactilar.* bogotá d.c.

aythami morales, j. f. (2015). *autenticación web de estudiantes mediante reconocimiento biométrico.* madrid, españa.

bishop, c. m. (1995). neural networks for pattern recognition. *oxford: oxford university press.*

casanova, i. m. (s.f.). *el planificador de tareas de linux* .

cmake. (s.f.). *cmake*. obtenido de cmake: https://cmake.org/

costilla, d. m. (2008). *semanticscholar*. obtenido de https://pdfs.semanticscholar.org/e60c/29d0f0f94a52ed9b101cb09e4ee1f45e0114.pdf

david leonardo castaño saavedra, j. d. (2019). *sistema de reconocimiento facial para control de acceso a.* bogotá d.c.

david mateos costilla, samuel reaño montoro . (2008). *streaming de audio/video. protocolo rtsp* .

departamento de justicia de los estados unidos. (2002). *el libro de referencia de las huellas dactilares.*

dlib. (s.f.). *dlib*. obtenido de dlib: http://dlib.net/

farkas., l. (1994). *antropometría normal y patológica en cabeza y cara. cirugía plástica, reconstructiva y estetica.*

florian schroff, d. k. (2015). *facenet: a unified embedding for face recognition and clustering.*

galton, f. (1892). *huellas dactilares.*

gary b. huang, m. r.-m. (s.f.). *rostros etiquetados en la naturaleza: una base de datos para estudiar el reconocimiento facial en entornos sin restricciones.* obtenido de http://vis-www.cs.umass.edu/lfw/

geitgey, a. (s.f.). obtenido de https://github.com/ageitgey/face_recognition

genbeta. (s.f.). *openface, un nuevo software de reconocimiento facial, de código abierto*. obtenido de genbeta: https://www.genbeta.com/actualidad/openface-un-nuevo-software-de-reconocimiento-facial-de-codigo-abierto

github. (s.f.). *github*. obtenido de https://volaya.github.io/libro-sig/chapters/bases_datos.html

gnu. (2008). obtenido de gnu: https://www.gnu.org/philosophy/open-source-misses-the-point.es.html

gonzalo hernández hernández. (s.f.). *universidad autónoma del estado de hidalgo*. obtenido de https://www.uaeh.edu.mx/scige/boletin/huejutla/n10/r1.html

imesd. (s.f.). *reconocimiento facial vs huellas dactilares*. obtenido de imesd: https://imesd.es/es/blog/reconocimiento-facial-vs-huellas-dactilares/

isabel mª cano jordán, j. g. (s.f.). *el planificador de tareas de linux.*

juan pablo pallo, d. c. (2016). *sistema de control de acceso al personal mediante reconocimiento facial*. ambato, ecuador.

nec. (2018). *la tecnología de reconocimiento facial de nec ocupa el primer lugar en las pruebas de precisión nist.* tokio.

neocheck. (2016). *nneocheck*. obtenido de nneocheck: https://www.neocheck.es/sistemas-de-seguridad-biometricos/

opencv. (s.f.). *opencv*. obtenido de opencv: https://opencv.org/about/

oracle. (2017). *oracle*. obtenido de https://www.oracle.com/co/artificial-intelligence/what-is-artificial-intelligence.html

ortega-garcia, j. & alonso-fernandez, fernando & coomonte-belmonte. (2008). *seguridad biométrica.*

peltier, t. r. (2014). *information security fundamentals* (vol. 2). ee.uu: taylor & frances group.

redhat. (s.f.). *redhat*. obtenido de https://www.redhat.com/es/topics/open-source/what-is-open-source

sheila plaza estévez, nerea ramírez lamela, carmen acosta morales. (s.f.). *accesibilidad, api de servicios web orientados a.*

solano, j. (s.f.). *dis*. obtenido de http://dis.um.es/~lopezquesada/documentos/ies_1213/lmsgi/curso/xhtml/xhtml22/index.html#:~:text=el%20modelo%20osi%20establece%20una,lo%20que%20hacen%20las%20dem%c3%a1s.

viewnext s.a. (2018). *viewnext*. obtenido de https://www.viewnext.com/arquitectura-de-microservicios-vs-arquitectura-monolitica/#:~:text=de%20forma%20muy%20resumida%2c%20puede,sujetos%20en%20un%20mismo%20programa.