Artículo Científico / Scientific Paper

UNIVERSIDAD POLITÉCNICA SALESIANA ECUADOR
INGENIUS
Revista de Ciencia y Tecnología
https://doi.org/10.17163/ings.n20.2018.10
pISSN: 1390-650X / eISSN: 1390-860X

Sistema de acceso usando una tarjeta RFiD y verificación de rostro

Access System Using an RFiD Card and Face Verification

José Ignacio Vega-Luna[1,*], Francisco Javier Sánchez-Rangel[1], Gerardo Salgado-Guzmán[1], Mario Alberto Lagos-Acosta[1]

Resumen

En este trabajo se presenta el desarrollo de un prototipo de sistema de acceso a un centro de datos usando como identificación una tarjeta de radio frecuencia o RFiD y verificación del rostro del usuario. El sistema se compone de tres módulos de entrada y un módulo central. El objetivo fue diseñar un sistema para transmitir, desde cada módulo de entrada al módulo central, el identificador único universal de la tarjeta RFiD o UUID y la imagen del rostro del usuario para consultar en una base de datos MySQL y en un directorio de fotografías si el usuario puede acceder al área correspondiente del módulo de entrada. Cada módulo de entrada consta de una tarjeta Raspberry Pi 3 B+, un lector de tarjetas RFiD, una cámara de video y una pantalla de cristal líquido o LCD. El módulo central se compone de los mismos elementos que los módulos de entrada y cuenta con una pantalla táctil usada en la interfaz de usuario en lugar de una pantalla LCD. La comunicación entre los nodos es wifi, logrando una precisión del 99,2 % en la verificación del rostro y un tiempo de respuesta de 180 ms usando 310 fotografías entrenadas.

Palabras clave: cámara de video, MySQL, pantalla táctil, Raspberry Pi 3 B+, verificación de rostro, RFiD.

Abstract

This paper presents the development of an access system to a data center using a RFID card and verification of the user's face. The system consists of three input modules and a central module. The objective was to design a system to transmit, from each input module to the central module, the universal unique identifier of the RFID card or UUID for its acronym in English and the user's face image to consult in a MySQL database and in a directory of photographs if the user can access the corresponding area of the input module. Each input module consists of a Raspberry Pi 3 B+ card, an RFID card reader, a video camera and a liquid crystal display or LCD for its acronym in English. The central module is composed of the same elements as the input modules and has a touch screen used in the user interface instead of an LCD screen. The communication between the nodes is WiFi, achieving a precision of 99.2% in the verification of the face and a response time of 180 ms using 310 trained photographs.

Keywords: Face verification, MySQL, Raspberry Pi 3 B+, RFiD, touchscreen, video camera.

[1,*]Área de Sistemas Digitales, Departamento de Electrónica, Universidad Autónoma Metropolitana-Azcapotzalco Cd. de México, México. Autor para correspondencia ✉: vlji@correo.azc.uam.mx.
https://orcid.org/0000-0002-4226-2936, https://orcid.org/0000-0002-4182-5856,
https://orcid.org/0000-0002-0581-7410, https://orcid.org/0000-0003-0455-007X.

Recibido: 14-05-2018, aprobado tras revisión: 21-06-2018

Forma sugerida de citación: Vega-Luna, J. I.; Sánchez-Rangel, F. J.; Salgado-Guzmán, G. y Lagos-Acosta, M. A. (2018). «Sistema de acceso usando una tarjeta RFiD y verificación de rostro». Ingenius. N.° 20, (julio-diciembre). pp. 108-118. doi: https://doi.org/10.17163/ings.n20.2018.10.

1. Introducción

Los centros de procesamiento de datos (CPD), también llamados centros de datos, son instalaciones que concentran recursos y equipos necesarios para el procesamiento y almacenamiento de información, así como equipos de telecomunicaciones de empresas y organizaciones. En los centros de datos se usan distintos dispositivos para acceder a las instalaciones que incluyen cerraduras electromagnéticas, torniquetes, cámaras de video, detectores de movimiento, tarjetas de identificación, sistemas biométricos y teclados para introducir una clave de acceso, entre otros. Comúnmente, los centros de datos se dividen en secciones llamadas búnkeres y periódicamente son sometidos a auditorías para poder estar certificados. Un punto importante que consideran las auditorías son los procedimientos y técnicas usados en la seguridad y acceso a las instalaciones [1]. En la actualidad existen diferentes soluciones para la identificación de personas para controlar el acceso a los búnkeres de un centro de datos. Algunas soluciones biométricas se basan en el reconocimiento de huella digital, de rostro, de geometría de la mano, de iris, de patrón de retina, de voz y firma de la persona [2].

El presente trabajo considera el requerimiento de una empresa operadora de centro de datos. El objetivo formulado fue contar con un sistema de acceso que use como medio de identificación una tarjeta RFiD y verificación del rostro del usuario para activar el actuador de la puerta de acceso del búnker donde el usuario está intentado acceder. El acceso debe contar con dos niveles de seguridad. Los requerimientos establecidos fueron un sistema confiable, fácil de ubicar y usar. Se requirió el empleo de tarjetas RFiD por ser económicas y fáciles de utilizar. La distancia máxima del búnker más lejano a la oficina de monitoreo son 65 metros y al punto de acceso wifi 35 metros con línea de vista. La solución propuesta consistió de sistema integrado por tres módulos de entrada y un módulo central. El centro de datos cuenta con tres búnkeres en cuya puerta de acceso se instaló un módulo de entrada. El módulo central se instaló en la oficina de monitoreo del centro de datos. Los módulos de entrada se encargan de leer la información almacenada en la tarjeta RFiD, capturar la fotografía del rostro del usuario y transmitir la información de la tarjeta y archivo de la fotografía JPEG al módulo central para su validación, usando tecnología wifi.

No se utilizó un segmento Ethernet para transmitir la información de identificación del usuario a la oficina de monitoreo para no instalar cableado adicional o modificar el existente. Una vez recibida la información, el módulo central consulta en la base de datos de usuarios si el UUID de la tarjeta RFiD está autorizado a entrar al búnker asociado al módulo de entrada, verifica que el rostro del usuario sea el que se encuentra registrado en el directorio de fotografías y registra en la base de datos la fecha y hora de solicitud de entrada. Si se cumplen las dos condiciones anteriores, el módulo central transmite la orden al módulo de entrada para activar el actuador de la puerta correspondiente. Los módulos de entrada y el módulo central se implantaron usando como base una tarjeta Raspberry Pi 3 B+ con sistema operativo Raspbian. La razón principal de usar la tarjeta Raspberry Pi fue porque existe una gran cantidad de aplicaciones y bibliotecas desarrolladas por la comunidad de código abierto de fácil instalación, configuración y uso en Raspbian [3]. En el sistema aquí presentado se implantó como primer mecanismo de seguridad el uso de una tarjeta RFiD y se utilizó el dispositivo NFC/RFiD 532 para la lectura de tarjetas. La tecnología de comunicación de campo cercano, NFC, surgió por la combinación de la tecnología RFiD y las tarjetas inteligentes. Permite la identificación y caracterización de personas u objetos sin contacto físico usando las ondas de radio transmitidas por una etiqueta. La tecnología RFiD permite el intercambio de información entre objetos ubicados cerca uno del otro. La comunicación con NFC es más segura que otras tecnologías ya que el transmisor y receptor están estrechamente acoplados y próximos, con una cercanía máxima de 10 centímetros, sin necesidad de ejecutar una aplicación. Los últimos años han aparecido varios usos de la tecnología NFC con teléfonos móviles, en Internet de las cosas o IoT y en el campo de sensores [4].

Aunque inicialmente se estableció usar tarjetas RFiD, se exploraron tecnologías alternas para la identificación de usuarios. Tecnologías como los códigos de respuesta rápida o QR y el sistema iBeacon. Los códigos QR son una mejora a los códigos de barras, almacenan información en matrices de puntos o códigos de barras de forma bidimensional [5]. Cuando un dispositivo móvil lee un código QR ejecuta una aplicación para realizar una acción específica. En el desarrollo de este trabajo pudo usarse una combinación de tecnología RFiD y códigos QR, pero resultaría un sistema un poco más costoso y lento, ya que además de usar un método de impresión del código QR en las tarjetas RFiD, estas no podrían reutilizarse. Por otra parte, iBeacon es un protocolo usado en sistemas de posicionamiento en interiores, o IPS, patentado por Apple Inc. Está basado en transmisores de bajo costo y bajo consumo de energía que indican su presencia a un dispositivo con sistema operativo iOS y a algunos dispositivos con sistema operativo Android [6]. Existen proveedores de transmisores, llamados *beacons*, compatibles con iBeacon. Los *beacons* usan transmisores de tecnología Bluetooth de bajo consumo de energía o BLE por sus siglas, o Bluetooth 4.0, los cuales transmiten su UUID a dispositivos electrónicos móviles, permitiendo que un teléfono móvil o tableta ejecute una acción o aplicación basada en la ubicación del *beacon* al recibir la identificación, o dar seguimiento a clientes o usuarios

de beacons. El sistema iBeacon se utiliza en comercio móvil, donde una aplicación, ejecutándose en un teléfono móvil, puede encontrar la ubicación de un producto asociado a un *beacon* dentro de una tienda o un *beacon* puede enviar ofertas o promociones al teléfono móvil. En otras aplicaciones los beacons transmiten al teléfono móvil información de tiendas y restaurantes cercanos, así como tiempos de espera o distribución de mensajes de puntos de interés de acuerdo con el lugar donde se encuentre el teléfono. La tecnología iBeacon difiere de otras, como NFC/RFiD, en que la transmisión realizada por el *beacon* es en un solo sentido y necesita que se ejecute una aplicación en iOS o Android. Pudo haber sido una opción usar iBeacon en el desarrollo de este trabajo, lo cual implicaría usar un *beacon* como identificador del usuario y un dispositivo con iOS en cada punto de acceso al centro de datos, lo que aumentaría la complejidad en el uso, instalación y costo del sistema [7].

Con la explosión de servicios basados en la Internet, o Internet de las cosas, la tecnología RFiD continúa usándose en distintos desarrollos y aplicaciones de identificación, incluyendo cadena de suministros [8], cuidado de la salud, localización de objetos, automatización de hogares, sistemas de seguridad y entrega de productos en restaurantes [9]. Se han realizado trabajos de sistemas de acceso a instalaciones basados en Arduino, tarjetas RFiD y bases de datos MySQL. La diferencia con respecto al aquí presentado es que se usa una tarjeta Raspberry de tecnología más reciente y menor costo que Arduino [10]. Adicionalmente, los trabajos que se han desarrollado usan comunicación Ethernet a la base de datos y en este trabajo se usó tecnología inalámbrica wifi cuya implantación es no intrusiva a las instalaciones del centro de datos [11]. De manera similar, se han realizado trabajos de sistemas de acceso a hogares, oficinas, e incluso a vehículos, que usan teléfonos inteligentes para emular tarjetas NFC y lectores NFC PN532 [12] como el utilizado en este trabajo. En estos sistemas el usuario debe portar un teléfono inteligente para identificarse, lo cual no es factible ni es una opción en los centros de datos debido al costo y que en ocasiones los usuarios son visitantes. Se han llevado a cabo también diversos trabajos que utilizan códigos QR o una combinación de estos con tarjetas RFiD para controlar el acceso a instalaciones, para sistemas de localización y navegación [13] y para identificación de productos [14] e imágenes médicas. Inclusive, se han realizado sistemas de acceso a centros de datos combinando códigos QR y marcas de agua [15]. El uso de códigos QR proporciona un nivel de seguridad más alto que las tarjetas RFiD, pero el costo de implantación y operación de estos sistemas es elevado, ya que una vez usada una tarjeta con un código QR no puede utilizarse para otro usuario y el *hardware* de impresión y lectura de códigos QR es de más alto precio que un lector NFC. Otros trabajos realizados recientemente para identificación, localización y control de acceso integran tecnologías iBeacon y wifi [16] o Bluetooth LE. Estos sistemas tienen la limitante de usar dispositivos con sistema operativo iOS o Android, lo cual hace que sean de mayor costo que al desarrollado en este trabajo.

Como segundo mecanismo de seguridad se utiliza la verificación del rostro de la persona. El reconocimiento facial empezó a usarse en los años 60. Era un proceso semiautomático en el que un operador identificaba los rasgos de la persona en dos o más fotografías y calculaba las distancias a puntos de referencia para compararlas entre sí. Los avances tecnológicos de la computación en los últimos años han creado una explosión de algoritmos, técnicas y aplicaciones no intrusivas de reconocimiento facial automatizado que se ejecutan en una computadora para identificar una persona en una imagen digital. Tomando la imagen de una persona no conocida debe encontrarse un perfil con el mismo rostro en un conjunto de imágenes conocidas, también llamadas imágenes de entrenamiento. Esto se realiza con uno de dos propósitos: 1) Verificación o autenticación de rostros, comparando una imagen del rostro de una persona con otra imagen. La aplicación confirma o niega la identidad del rostro, el objetivo es asegurar que la persona es quien dice ser y 2) Identificación o reconocimiento de rostros, comparando la imagen de un rostro no conocido con las imágenes de rostros conocidos almacenados en una base de datos para determinar su identidad. El reconocimiento facial es un área que integra las siguientes tecnologías: procesamiento de imágenes, visión por computadora, reconocimiento de patrones, redes neuronales y aprendizaje de máquinas [17]. El procedimiento usado por los sistemas de reconocimiento facial consiste de manera general de cinco fases:

- Fase de registro, se captura la imagen del rostro de la persona a identificar usando una cámara fotográfica o una cámara de video.

- Fase de procesamiento de la imagen, se lleva a cabo la alineación del rostro basándose en algunas propiedades geométricas y se obtiene una imagen independiente de la iluminación y gama de colores de la imagen original.

- Fase de extracción de información biométrica, se obtienen las características faciales como un patrón biométrico.

- Fase de comparación, el patrón biométrico se compara el patrón de rostros almacenados en la base de datos. Es una comparación 1:N donde se determina el porcentaje de similitud de la persona a identificar respecto a las fotografías almacenadas en la base de datos.

- Fase de toma de decisiones, utilizando una matriz de similitudes, se identifica a la persona que resultó con mayor porcentaje de similitud de la base de datos usando un rango establecido.

Recientemente el uso de sistemas de reconocimiento facial ha experimentado un auge en diferentes tipos de aplicaciones, utilizándose para autenticar a los propietarios de dispositivos móviles, en la detección de conductores con sueño o cansados, en la trata de personas, en el análisis de riesgos y en situaciones en lugares de alta concentración de personas [18]. Microsoft aplica reconocimiento facial para acceder a una computadora con Windows [19], mientras que Apple está intentando contar con un mecanismo en el que los usuarios de iOS puedan compartir automáticamente fotos con amigos etiquetados. Facebook y Google se han enfrascado en una guerra en el diseño y uso de algoritmos de reconocimiento facial para etiquetar amigos y encontrar fotos de una persona. Pretenden lograr el algoritmo perfecto, reconociendo rostros mucho mejor que el ser humano. Google presentó en 2015 el sistema de reconocimiento facial denominado FaceNet, con una precisión del 99,63 %, reconociendo fotos en Google+ [20]. Este sistema usa aprendizaje de máquina generando un mapa en un espacio euclidiano compacto a partir de la imagen de un rostro humano, donde las distancias corresponden directamente a la medida de similitud del rostro. Con este espacio, las tareas de verificación y reconocimiento de una imagen, se pueden realizar fácilmente usando técnicas estándares como la de vectores de FaceNet embeddings. El sistema FaceNet usa una red neuronal convolucional profunda entrenada con más de 260 millones de imágenes de rostros. Los autores de FaceNet indican que han desarrollado el estado del arte de los métodos de reconocimiento facial usando solo 128 bytes para cada rostro y más de 13 000 imágenes de rostros de la Internet para verificar si dos imágenes son la misma persona, mientras que el sistema de reconocimiento YouTube Faces logra el 95,12 %. La tecnología usada por Facebook para reconocimiento facial se llama DeepFace, fue desarrollada por la compañía israelí face.com y liberada en 2013 [21]. Los creadores de DeepFace indican que pueden lograr una precisión del 97,25 % al comparar dos rostros.

En años recientes el reconocimiento facial se ha estado utilizando en sistemas de acceso en centros de datos. Se pueden lograr sistemas confiables y con porcentaje de precisión aceptable sin usar algoritmos tan sofisticados como los desarrollados por compañías como Google y Facebook que, además, son algoritmos patentados y propietarios. Existen bastantes algoritmos de código abierto que pueden utilizarse en el sistema operativo de una computadora pequeña, de bajo costo y poderosa como la tarjeta Raspberry Pi 3 B+. Uno de estos algoritmos es el de histograma de gradientes orientados o HOG, denominado algoritmo HOG [22]. Este algoritmo se desarrolló en 2005, es de los más avanzados y continuamente se mejora para optimizarlo y lograr mayor precisión. Un HOG es un descriptor de características usado en visión por computadora y procesamiento de imágenes para la detección de objetos. Este cuenta las ocurrencias de orientación de gradientes en partes definidas de una imagen. Los descriptores pueden utilizarse como datos de entrada o características para un algoritmo de aprendizaje de máquina. Existen bibliotecas de código abierto que implantan las fases de un sistema de reconocimiento facial con el algoritmo HOG y aprendizaje profundo de máquina, las cuales son fáciles de instalar y utilizar reduciendo significativamente el código del programa [23]. Una de estas bibliotecas es Face_Recognition y es la que se utilizó en este trabajo para verificar el rostro de usuarios. Esta biblioteca usa una red neuronal entrenada y está basada en dlib, la herramienta estado de arte en reconocimiento de rostros construida con aprendizaje profundo. Los autores de Face_Recognition indican que su precisión es del 99,38 % y proporciona varias funciones con las cuales se pueden realizar algunas acciones como encontrar rostros en una fotografía, determinar la ubicación de los puntos de referencia de un rostro, manipular las características faciales de un rostro, codificar biométricamente un rostro, comparar dos rostros codificados, reconocer rostros en video de tiempo real y reconocer rostros localizados en una fotografía usando un directorio de fotografías de personas obteniendo el nombre de cada persona. Para poder usar la biblioteca Face_Recognition deben instalarse las siguientes herramientas en Raspian: biblioteca de Python para picamera (python3-picamera), dlib v19.6 y OpenCV.

Por otro lado, se ha realizado una gran variedad de sistemas de acceso a centros de datos a través de dispositivos biométricos. Algunos de estos sistemas llevan a cabo reconocimiento facial usando una computadora de escritorio para implantar el proceso de reconocimiento [24] y comunicación alámbrica entre la computadora y la cámara de video [25] o cámara web son eficientes, pero su costo y tamaño es mayor al aquí desarrollado. Otros sistemas de este tipo se basan en la lectura del iris del ojo [26] usando un lector instalado en la puerta de acceso o por medio del teléfono inteligente del usuario. Estos sistemas son más seguros que los de tarjetas RFiD, códigos QR, lectura de huellas digitales o reconocimiento facial 2D, pero el costo del lector es mucho más alto.

2. Materiales y métodos

La metodología utilizada en el diseño de este sistema consistió dividirlo en dos componentes: los módulos de entrada y el módulo central. Posteriormente, se implantó el sistema eligiendo los elementos adecuados

y de menor costo de acuerdo con los requerimientos establecidos. El diagrama de bloques funcional del sistema se muestra en la Figura 1.

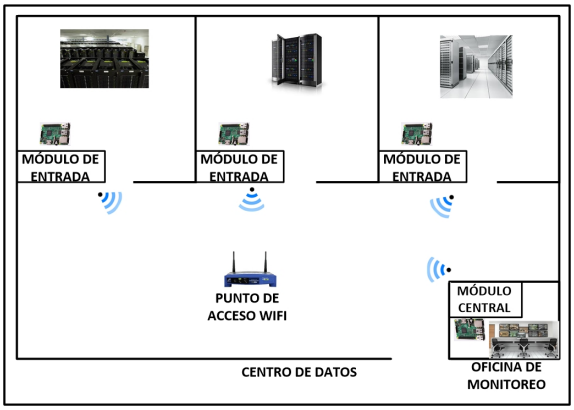

Figura 1. Diagrama de bloques funcional del sistema de acceso.

2.1. Los módulos de entrada

Se construyeron tres módulos de entrada, todos con la misma arquitectura como la mostrada en la Figura 2. Las funciones principales de estos módulos son las siguientes: explorar continuamente si se encuentra una tarjeta bajo el alcance del lector RFiD y leer el UUID, capturar la imagen del rostro de la persona que intenta acceder, transmitir al módulo central la información leída de la tarjeta y la fotografía de la persona en un archivo JPEG y esperar del módulo central la respuesta para permitir o negar el acceso al usuario. Cada módulo de entrada está compuesto por una tarjeta Raspberry Pi 3 B+, un lector de tarjetas RFiD, una cámara de video, una pantalla LCD 2x16 y una interfaz de salida.

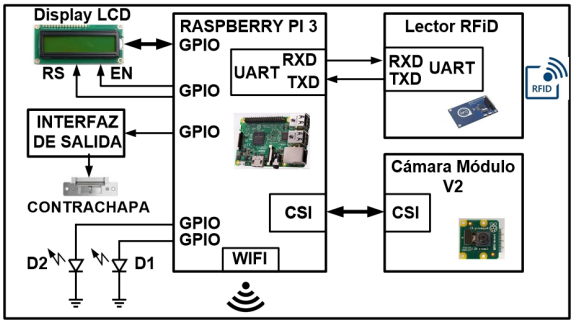

Figura 2. Diagrama de bloques de los módulos de entrada.

La tarjeta Raspberry Pi 3 B+ usada en este módulo cuenta con los siguientes recursos *hardware*: 1 GB de memoria RAM, 40 terminales GPIO, interfaz serie para cámara, o CSI, puerto DSI para pantalla táctil, puerto Ethernet Gigabit, ranura para memoria SD y una interfaz wifi. El lector de tarjetas RFiD usado es el dispositivo NFC/RFiD PN532. Este lector es de los más usados en aplicaciones que usan tecnología NFC, tarjetas y etiquetas RFiD de 13.56 MHz, ya que su principal circuito integrado está embebido en muchos teléfonos inteligentes. Puede escribir tarjetas y etiquetas RFiD tipo 1 a 4 e integra una antena cuyo alcance son 10 centímetros.

Existe una gran cantidad de herramientas de código abierto para realizar aplicaciones con el NFC/RFiD PN532. Una de estas herramientas es la biblioteca libnfc. Tanto en los módulos de entrada como en el módulo central, el lector RFiD se conectó al puerto UART de la Raspberry Pi y se descargó en ella la versión 1.7.0 de la biblioteca libnfc. Antes de instalar y configurar libnfc se deshabilitó, en el núcleo del sistema operativo de la Raspberry Pi, el UART como puerto de consola usando la herramienta paspi-config y editando el archivo /boot/config.txt. A continuación, se instaló y construyó la biblioteca libnfc usando los siguientes comandos: sudo make clean y sudo make install all, los cuales crearon los drivers, archivos de documentación, binarios y ejecutables correspondientes. Los módulos de entrada contienen también un módulo de cámara para Raspberry V2 conectado a la interfaz CSI de la Raspberry Pi 3 B+. Este módulo de cámara, cuenta con un sensor de alta resolución Sony IMX219 de 8 megapixeles. Permite capturar fotografías con una resolución máxima de 3238 x 2464 y video de alta definición.

Existen bibliotecas de código abierto para usar la cámara y manipular fotos y video que pueden invocarse desde Raspbian o desde un programa en Python. La cámara puede controlarse usando el comando raspinstall, sin embargo, en este trabajo se utilizó la biblioteca python-picamera de Python en caso de que posteriormente, en el sistema, sea necesario modificar las características de captura de fotografías o video. La cámara de los módulos de entrada se habilitó a través de la herramienta raspi-config de Raspbian y posteriormente se instaló la biblioteca python-picamera utilizando el comando: sudo apt-get install python3-picamera. Una vez realizado lo anterior, se pudo usar la función camera.capture(‘archivo.jpg’) para capturar una imagen en un archivo JPEG. El programa que se ejecuta en los nodos de captura se realizó en Phyton 3.6 y realiza las siguientes acciones: configura temporizadores, el puerto UART, la interfaz wifi, terminales GPIO y dispositivos periféricos, lector RFiD, cámara de video y pantalla LCD, muestra en la pantalla LCD el mensaje que indica al usuario colocar la tarjeta RFiD en el lector y a continuación entra en un ciclo continuo donde explora cada 0.5 segundos el lector RFiD ejecutando la función nfc-pool_8c.

La comunicación entre los módulos de entrada y el de control se llevó a cabo usando intercambio de mensajes con *sockets* bajo el esquema cliente-servidor, los módulos de entrada son los clientes y el de control es el servidor. Cuando el lector detecta una tarjeta,

muestra un mensaje en la pantalla LCD solicitando al usuario se coloque al frente de la cámara de video y captura en un archivo JPEG la imagen del rostro de la persona. Posteriormente, el programa transmite al módulo central, a través de un *socket*, el UUID de la tarjeta RFiD y el archivo JPEG. Una vez realizado lo anterior, el programa espera en el socket la respuesta del módulo central. Si la respuesta indica que el usuario está autorizado a entrar, el módulo de entrada activa el actuador de la puerta de acceso, a través de la interfaz conectada a una terminal GPIO de la tarjeta Raspberry y enciende un led verde (D1), conectado a otra terminal GPIO, durante 3 segundos. Si el usuario no está autorizado, enciende un led rojo (D2) intermitentemente durante 5 segundos. En la Figura 3 se indica el diagrama de flujo del programa.

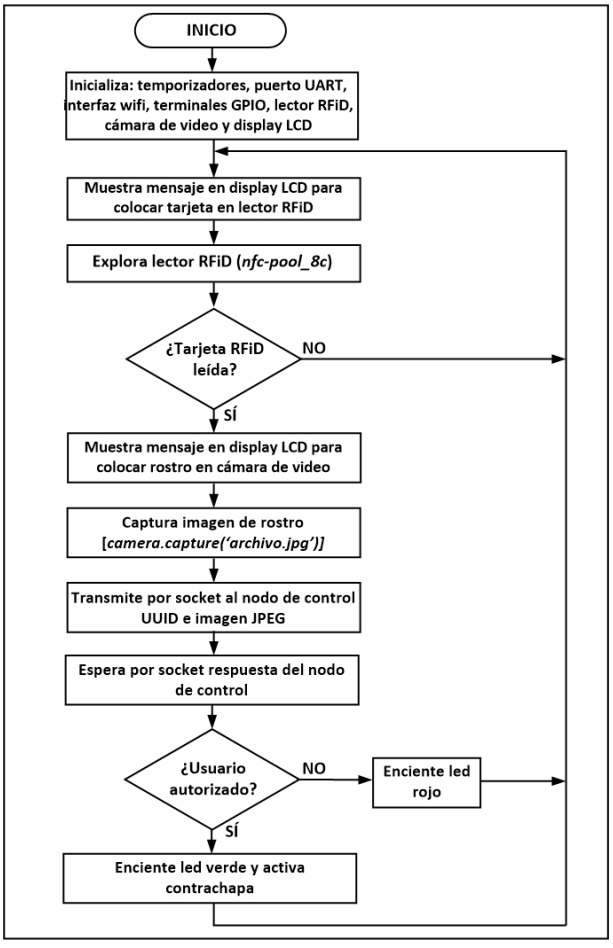

Figura 3. Diagrama de flujo del programa de los módulos de entrada.

Para poder usar *sockets* desde Python debe instalarse la biblioteca correspondiente ejecutando el comando siguiente: sudo apt-get install socket. La interfaz de salida que controla el actuador de la puerta de entrada se conectó a una terminal GPIO de la tarjeta Raspberry como se muestra en la Figura 4.

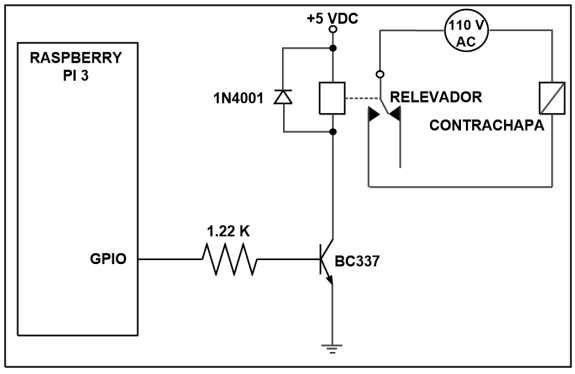

Figura 4. Interfaz de salida del actuador de la puerta de entrada.

2.2. El módulo central

El módulo central está constituido por los siguientes componentes: una tarjeta Raspberry Pi 3 B+, un lector de tarjetas RFiD, una cámara de video y una pantalla táctil Pi+TFT de 3,5". En la Figura 5 se indica el diagrama de bloques de la arquitectura del módulo central.

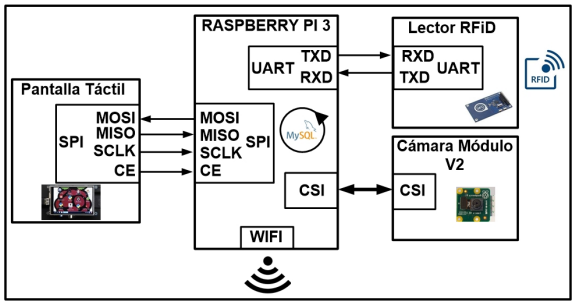

Figura 5. Diagrama de bloques del módulo central.

La programación del módulo central se realizó en Phyton 3.6 y se divide en tres partes: el programa principal, la rutina de comunicación con los módulos de entrada y la rutina de la interfaz de usuario. El programa principal configura temporizadores, el puerto UART, la interfaz wifi y dispositivos periféricos, lector RFiD, cámara de video y pantalla táctil e invoca las dos rutinas del sistema, como se indica en el diagrama de flujo de la Figura 6.

En este módulo se creó una base de datos, manejada con MySQL, que almacena la información de usuarios autorizados a acceder a los búnkeres y un directorio con las fotografías del rostro de los usuarios anteriores.

La rutina de comunicación con los módulos de entrada ejecuta un programa en segundo plano que realiza las siguientes funciones: 1) Crea un *socket* a través del cual recibe desde los módulos de entrada el UUID y el archivo JPEG. 2) Accede la base de datos MySQL para determinar si el usuario está autorizado

a entrar al área correspondiente. 3) Invoca la rutina que verifica que el rostro del usuario se encuentre en el directorio de fotografías. 4) Actualiza el registro del usuario en la base de datos MySQL con fecha y hora de entrada. 5) Transmite el mensaje al módulo de entrada para activar el actuador de la puerta o negar la entrada. 6) Actualiza la bitácora de registro de intentos de acceso almacenando en ella el archivo JPEG.

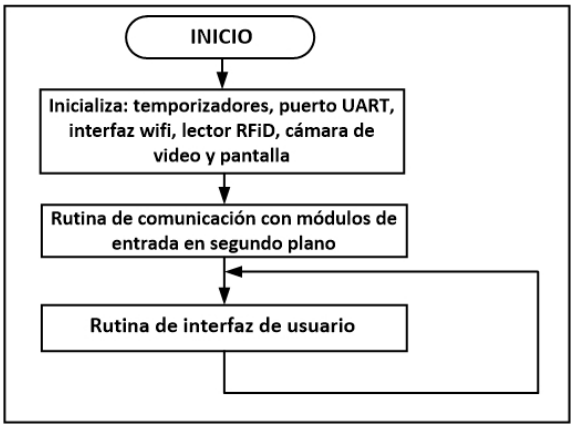

Figura 6. Diagrama de flujo del programa principal del módulo central.

En la Figura 7 se indica en el diagrama de flujo de esta rutina. Tanto la base de datos como el directorio de fotografías codificadas y entrenadas residen en la tarjeta SD de 16 GB de la Raspberry Pi. En la base de datos se creó una tabla que contiene los registros de usuarios. Cada registro almacena el UUID de la tarjeta RFiD asignada, número de puertas a las que tiene acceso, nombre, compañía y correo electrónico del usuario. Para crear la base de datos y tabla de usuarios se llevaron a cabo las siguientes tareas:

1. Instalación del servidor y cliente de MySQL, así como el API de Python para acceder MySQL.
2. Creación de la base de datos ejecutando los siguientes comandos: mysql -u root -p, mysql> CREATE DATABASE RFID_DB; CREATE TABLE users_tbl (id INT NOT NULL PRIMARY KEY AUTO_INCREMENT, UUID VARCHAR(20), puertas VARCHAR(20), nombre VARCHAR(20), apellidos VARCHAR(30), company VARCHAR(20), email VARCHAR(30)).

Una vez creada la base de datos, se realizó el programa en Python para acceder la misma. Python usa un objeto o estructura de datos, llamada cursor, para acceder los datos de la tabla. Este objeto permite realizar operaciones de creación, lectura, actualización y remoción de registros en la base de datos. El programa ejecuta de manera general las siguientes acciones:

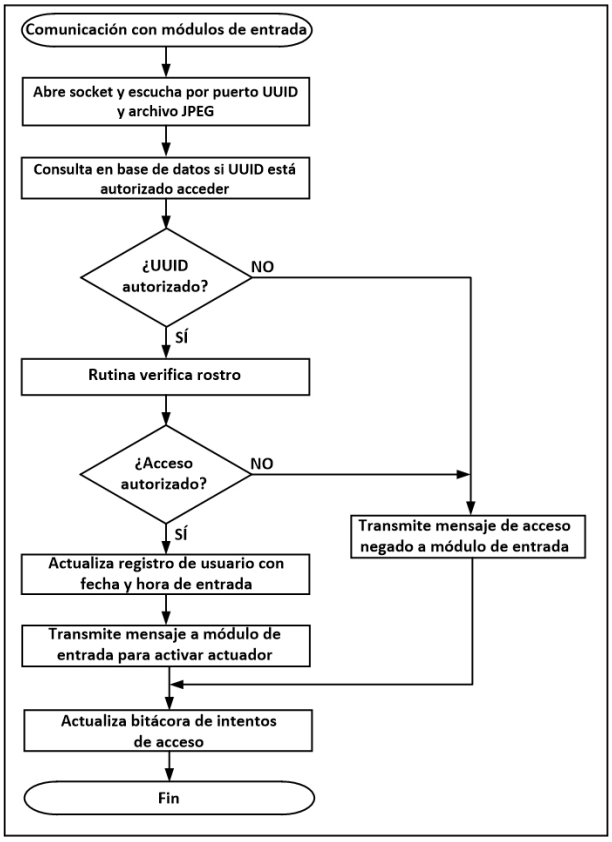

Figura 7. Diagrama de flujo de la comunicación con los módulos de entrada.

1. Importa el API de Python para MySQL: import MySQLdb.
2. Realiza la conexión a la base de datos: db=MySQLdb.connect("localhost", "root", "password", "RFID_DB").
3. Define el objeto cursor: cursor=db.cursor().
4. Espera la opción seleccionada por el usuario en la interfaz gráfica.
5. Dependiendo de la opción, define uno de los siguientes query's de SQL: cursor.execute ("INSERT INTO users-tbl"), cursor.execute ("SELECT * FROM users_tbl"), cursor.execute ("UPDATE users_tbl SET") o cursor.execute ("DELETE FROM users_tbl WHERE")
6. Ejecuta el query: db.commit().

En el directorio de fotografías, el nombre de cada archivo corresponde al nombre del usuario registrado en la base de datos MySQL. La rutina que verifica si el rostro del usuario se encuentra en el directorio de fotografías realiza las siguientes acciones: carga en un *buffer* la imagen del rostro recibida de un módulo de entrada utilizando la función face_recognition.load_image_file, codifica y aprende a reconocer la imagen almacenada en el *buffer* usando

la función face_recognition.face_encodings y entra a un ciclo donde compara la imagen codificada del *buffer* con cada imagen del directorio de fotografías codificadas, el ciclo termina cuando encuentra igualdad entre las dos imágenes analizadas o cuando exploró el directorio completo sin encontrar igualdad. La comparación se realiza a través de la función face_recognition.compare_faces, la cual obtiene, en caso de ser exitosa, el nombre del usuario de la fotografía. Si el nombre obtenido es igual al nombre leído del registro del usuario en la base de datos, retorna a la rutina que la invocó autorizando el acceso al usuario, como se muestra en el diagrama de flujo de la Figura 8. Se consideró que la imagen recibida del módulo de entrada solo contiene un rostro, de lo contrario tendría que usarse la función face_recognition.face_locations para encontrar los rostros en la imagen y codificarlos individualmente.

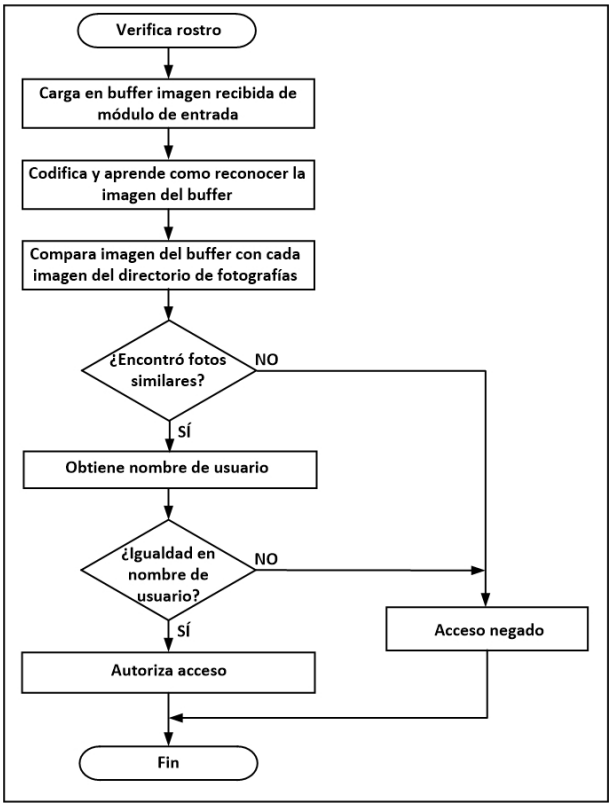

Figura 8. Diagrama de flujo de la rutina de verificación de rostro.

La rutina que implanta la interfaz gráfica de usuario, permite acceder y administrar la base de datos usando la pantalla táctil. La pantalla utilizada en el módulo central es el dispositivo Pi+TFT de 3,5" el cual tiene una resolución de 480 x 320 y se conectó al puerto SPI de la tarjeta Raspberry Pi. En la interfaz de usuario, el administrador puede realizar las siguientes operaciones: altas, bajas y cambios de usuarios, así como mostrar los usuarios registrados y la bitácora de registro de intentos de acceso. El lector de tarjetas RFiD y la cámara del módulo de validación se usan al dar de alta o realizar cambios en el registro de un usuario. La interfaz de usuario se realizó usando pygame. La herramienta pygame es un conjunto de bibliotecas que pueden usarse en un programa de Python para la implantación de videojuegos, programas multimedia e interfaces gráficas de usuario, ya que permite mostrar texto, imágenes y sonidos en una pantalla táctil y controlar la posición del cursor. Esta herramienta se instala por defecto con la versión de Raspbian para Raspberry Pi. La dirección IP de la interfaz wifi de cada módulo de entrada es fija y es usada por el módulo central para determinar el número de puerta en la que está intentando el usuario acceder.

3. Resultados y discusión

Se realizaron cuatro grupos de pruebas. El primer grupo tuvo como objetivo medir el alcance del lector RFiD de los módulos de entrada. Colocando 50 tarjetas en el lector de los módulos se determinó que el alcance son 14 centímetros, un poco más de lo indicado en las especificaciones del fabricante. El segundo grupo de pruebas tuvo como objetivo almacenar las fotografías de 50 usuarios en el directorio del módulo de central y entrenar la red neuronal. El tamaño promedio de cada fotografía fue 110 KB. El tercer grupo de pruebas tuvo como objetivo determinar la precisión del sistema de verificación del rostro de usuarios registrados en la base de datos. Este grupo de pruebas se llevó a cabo en varias fases. En la primera, el directorio de fotografías entrenadas almacenó 50 rostros y en cada una de las siguientes se adicionaron 20 fotografías hasta tener 310. En cada fase se realizó la verificación de 40 rostros diferentes. Con algunos rostros el reconocimiento no fue exitoso a pesar de estar registrados en el módulo central. La cantidad de reconocimientos no exitosos trajo como consecuencia que en la primera fase la precisión fuera del 96,3 %, la cual fue aumentando conforme creció el número de fotografías entrenadas hasta llegar al 99,2 % como se muestra en la gráfica de la Figura 9.

El cuarto grupo de pruebas tuvo como objetivo medir el tiempo de respuesta del sistema. Para realizar estas pruebas en cada una de las fases del grupo de pruebas anterior, se registró en un archivo en el módulo de entrada la hora de captura del rostro de una persona registrada en la base de datos y la hora al recibir respuesta del módulo central una vez verificada la persona autorizada. El tiempo de respuesta en la primera fase fue 132 ms en promedio y aumentó hasta 180 ms en la última fase, casi imperceptible para el usuario como se indica en la gráfica de la Figura 10. Las fotografías del directorio del módulo central fueron tomadas con suficiente iluminación ambiental, de frente, sin anteojos, poses u objeto que impidan ver

claramente el rostro. Es recomendable que al dar de alta nuevos usuarios se capturasen varias fotografías del rostro usando diferentes poses con lo cual el sistema podría ser más tolerante y mejorar tanto la precisión como el tiempo de respuesta. La implantación de este trabajo no requirió instalar cableado adicional para transmisión de datos ni modificar el existente, el módulo central se instala en una oficina de control del centro de datos, esto lo hace más práctico a los comercialmente disponibles que usan comunicación alambrada. El costo del sistema es $350,00 USD, más bajo que los comercialmente existentes cuyo costo es $1700,00 USD en promedio.

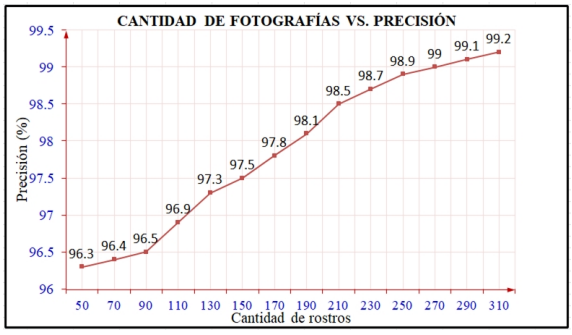

Figura 9. Precisión del sistema con diferentes cantidades de rostros entrenados.

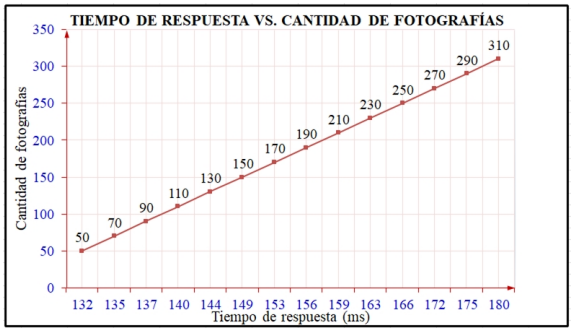

Figura 10. Tiempo de respuesta del sistema

4. Conclusiones

El resultado de este trabajo fue un sistema de acceso con doble mecanismo de seguridad más robusto que los disponibles comercialmente que usan solo un mecanismo, fue construido usando componentes de reciente tecnología y bajo costo y *software* de código abierto y la comunicación es a través de wifi, la cual no impacta en las instalaciones del centro de datos, llevando a cabo una aplicación práctica que cumple con los requisitos establecidos. El alcance de lectura de tarjetas RFiD logrado fue 14 centímetros. En la verificación del rostro se logró una precisión del 99,2 % y un tiempo de respuesta de 180 ms usando 310 fotografías entrenadas.

Trabajos futuros

Con el porcentaje de precisión y tiempo de respuesta logrados, el centro de datos solicitó realizar una segunda versión que incorpore las siguientes funcionalidades: 1) Incorporar un servidor *web* al módulo central y una pantalla táctil en los módulos de entrada de forma tal que el administrador pueda acceder la base de datos de usuarios y directorio de fotografías desde cualquier módulo de entrada y 2) Incorporar un lector de huellas digitales en todos los módulos para contar con un nivel adicional de seguridad. Estas funcionalidades son factibles de realizar con la arquitectura actual de los módulos del sistema.

Agradecimientos

Se agradece el apoyo proporcionado por el Departamento de Electrónica de la Universidad Autónoma Metropolitana-Azcapotzalco.

Referencias

[1] M. V. M. Lima, R. M. F. Lima, and F. A. A. Lins, "A multi-perspective methodology for evaluating the security maturity of data centers," in *2017 IEEE International Conference on Systems, Man, and Cybernetics (SMC)*, Oct 2017. DOI: https://doi.org/10.1109/SMC.2017.8122775, pp. 1196–1201.

[2] M. Levy and J. O. Hallstrom, "A new approach to data center infrastructure monitoring and management (dcimm)," in *2017 IEEE 7th Annual Computing and Communication Workshop and Conference (CCWC)*, Jan 2017. textscdoi: https://doi.org/10.1109/CCWC.2017.7868412, pp. 1–6.

[3] I. B. Mustaffa and S. F. B. M. Khairul, "Identification of fruit size and maturity through fruit images using opencv-python and rasberry pi," in *2017 International Conference on Robotics, Automation and Sciences (ICORAS)*, Nov 2017. DOI: https://doi.org/10.1109/ICORAS.2017.8308068, pp. 1–3.

[4] J. Mihal'ov and M. Hulič, "Nfc/rfid technology using raspberry pi as platform used in smart home project," in *2017 IEEE 14th International Scientific Conference on Informatics*, Nov 2017. DOI: https://doi.org/10.1109/INFORMATICS.2017.8327257, pp. 259–264.

[5] N. Goel, A. Sharma, and S. Goswami, "A way to secure a qr code: Sqr," in *2017 International Conference on Computing, Communication and Automation (ICCCA)*, May 2017. DOI:

https://doi.org/10.1109/CCAA.2017.8229850, pp. 494–497.

[6] S. Menon, A. George, N. Mathew, V. Vivek, and J. John, "Smart workplace – using ibeacon," in *2017 International Conference on Networks Advances in Computational Technologies (NetACT)*, July 2017. DOI: https://doi.org/10.1109/NETACT.2017.8076803, pp. 396–400.

[7] X. Li, D. Xu, X. Wang, and R. Muhammad, "Design and implementation of indoor positioning system based on ibeacon," in *2016 International Conference on Audio, Language and Image Processing (ICALIP)*, July 2016. DOI: https://doi.org/10.1109/ICALIP.2016.7846648, pp. 126–130.

[8] M. Chamekh, S. E. Asmi, M. Hamdi, and T. H. Kim, "Context aware middleware for rfid based pharmaceutical supply chain," in *2017 13th International Wireless Communications and Mobile Computing Conference (IWCMC)*, June 2017. DOI: https://doi.org/10.1109/IWCMC.2017.7986576, pp. 1915–1920.

[9] K. B. Eric and W. H. Ya, "Iot based smart restaurant system using rfid," in *4th International Conference on Smart and Sustainable City (ICSSC 2017)*, June 2017. DOI: https://doi.org/10.1049/cp.2017.0123, pp. 1–6.

[10] M. Andriansyah, M. Subali, I. Purwanto, S. A. Irianto, and R. A. Pramono, "e-ktp as the basis of home security system using arduino uno," in *2017 4th International Conference on Computer Applications and Information Processing Technology (CAIPT)*, Aug 2017. DOI: https://doi.org/10.1109/CAIPT.2017.8320693, pp. 1–5.

[11] S. Nath, P. Banerjee, R. N. Biswas, S. K. Mitra, and M. K. Naskar, "Arduino based door unlocking system with real time control," in *2016 2nd International Conference on Contemporary Computing and Informatics (IC3I)*, Dec 2016. DOI: https://doi.org/10.1109/IC3I.2016.7917989, pp. 358–362.

[12] J. Cui, D. She, J. Ma, Q. Wu, and J. Liu, "A new logistics distribution scheme based on nfc," in *2015 International Conference on Network and Information Systems for Computers*, Jan 2015. DOI: https://doi.org/10.1109/ICNISC.2015.48, pp. 492–495.

[13] W. Xiao-Long, W. Chun-Fu, L. Guo-Dong, and C. Qing-Xie, "A robot navigation method based on rfid and qr code in the warehouse," in *2017 Chinese Automation Congress (CAC)*, Oct 2017. DOI: https://doi.org/10.1109/CAC.2017.8244199, pp. 7837–7840.

[14] H. Keni, M. Earle, and M. Min, "Product authentication using hash chains and printed qr codes," in *2017 14th IEEE Annual Consumer Communications Networking Conference (CCNC)*, Jan 2017. DOI: https://doi.org/10.1109/CCNC.2017.7983126, pp. 319–324.

[15] P. Pramkeaw, T. Ganokratanaa, and S. Phatchuay, "Integration of watermarking and qr code for authentication of data center," in *2016 12th International Conference on Signal-Image Technology Internet-Based Systems (SITIS)*, Nov 2016. DOI: https://doi.org/10.1109/SITIS.2016.111, pp. 669–672.

[16] H. Zou, Z. Chen, H. Jiang, L. Xie, and C. Spanos, "Accurate indoor localization and tracking using mobile phone inertial sensors, wifi and ibeacon," in *2017 IEEE International Symposium on Inertial Sensors and Systems (INERTIAL)*, March 2017. DOI: https://doi.org/10.1109/ISISS.2017.7935650, pp. 1–4.

[17] Z. Yu, F. Liu, R. Liao, Y. Wang, H. Feng, and X. Zhu, "Improvement of face recognition algorithm based on neural network," in *2018 10th International Conference on Measuring Technology and Mechatronics Automation (ICMTMA)*, Feb 2018. DOI: https://doi.org/10.1109/ICMTMA.2018.00062, pp. 229–234.

[18] N. Mokoena, H. D. Tsague, and A. Helberg, "2d methods for pose invariant face recognition," in *2016 International Conference on Computational Science and Computational Intelligence (CSCI)*, Dec 2016. DOI: https://doi.org/10.1109/CSCI.2016.0163, pp. 841–846.

[19] D. Goldman. (2015) Microsoft will let you unlock windows 10 with your face. CNN tech. [Online]. Available: https://goo.gl/tgo8pM

[20] F. Schroff, D. Kalenichenko, and J. Philbin, "Facenet: A unified embedding for face recognition and clustering," in *2015 IEEE Conference on Computer Vision and Pattern Recognition (CVPR)*, June 2015. DOI: https://doi.org/10.1109/CVPR.2015.7298682, pp. 815–823.

[21] S. Srisuk and S. Ongkittikul, "Robust face recognition based on weighted deepface," in *2017 International Electrical Engineering Congress (iEECON)*, March 2017. DOI: https://doi.org/10.1109/IEECON.2017.8075885, pp. 1–4.

[22] M. Wiglasz and L. Sekanina, "Evolutionary approximation of gradient orientation module in hog-based human detection system," in *2017 IEEE Global Conference on Signal and Information Processing (GlobalSIP)*, Nov 2017. DOI: https://doi.org/10.1109/GlobalSIP.2017.8309171, pp. 1300–1304.

[23] J. Zeng, X. Zhao, C. Qin, and Z. Lin, "Single sample per person face recognition based on deep convolutional neural network," in *2017 3rd IEEE International Conference on Computer and Communications (ICCC)*, Dec 2017. DOI: https://doi.org/10.1109/CompComm.2017.8322819, pp. 1647–1651.

[24] X. Chen, L. Qing, X. He, J. Su, and Y. Peng, "From eyes to face synthesis: a new approach for human-centered smart surveillance," *IEEE Access*, vol. 6, pp. 14 567–14 575, 2018. DOI: https://doi.org/10.1109/ACCESS.2018.2803787.

[25] A. H. M. Amin, N. M. Ahmad, and A. M. M. Ali, "Decentralized face recognition scheme for distributed video surveillance in iot-cloud infrastructure," in *2016 IEEE Region 10 Symposium (TENSYMP)*, May 2016. DOI: https://doi.org/10.1109/TENCONSpring.2016.7519389, pp. 119–124.

[26] Ş. Karahan and Y. S. Akgül, "Eye detection by using deep learning," in *2016 24th Signal Processing and Communication Application Conference (SIU)*, May 2016. DOI: https://doi.org/10.1109/SIU.2016.7496197, pp. 2145–2148.