REDES NEURONALES ARTIFICIALES PARA EL CONTROL DE ACCESO BASADO EN RECONOCIMIENTO FACIAL

NEURAL NETWORKS FOR ACCESS CONTROL BASED ON FACE RECOGNITION USING

José Ibarra-Estévez[1]

Kimberly Paredes[2]

Recibido: 27 de septiembre de 2017
Aceptado: 31 de enero de 2018

[1] Escuela de Ingeniería, Pontificia Universidad Católica del Ecuador Sede Ibarra. Ibarra, Ecuador. (*jibarra@pucesi.edu.ec).

[2] Escuela de Ingeniería, Pontificia Universidad Católica del Ecuador Sede Ibarra. Ibarra, Ecuador.

REDES NEURONALES ARTIFICIALES PARA EL CONTROL DE ACCESO BASADO EN RECONOCIMIENTO FACIAL

NEURAL NETWORKS FOR ACCESS CONTROL BASED ON FACE RECOGNITION USING

José Ibarra-Estévez, Kimberly Paredes

Palabras clave: Redes Neuronales Artificiales, Inteligencia Artificial, Sistemas de Control de Acceso, Reconocimiento Facial.

Keywords: Artificial Neural Networks, Artificial Intelligence, Access Control Systems, Face Recognition.

Resumen

En este trabajo se presenta el desarrollo de un sistema basado en redes neuronales artificiales para el reconocimiento rápido de rostros y su utilización en el control de acceso. El reconocimiento facial es un tema de gran interés por su impacto y posibles aplicaciones en temas de carácter laboral, control de ingreso a espacios, seguridad ciudadana, activación y funcionamiento de equipos, entre otros. El control de acceso es una de las medidas que puede contribuir a garantizar la seguridad del personal dentro de una organización o en entornos domésticos, por lo cual es importante el uso de herramientas tecnológicas que ayuden al apropiado reconocimiento facial y automatizar los procesos de con-

trol de acceso. La inteligencia artificial ha demostrado su utilidad y aplicación en diversas áreas del quehacer cotidiano y particularmente las redes neuronales artificiales por su capacidad de aprendizaje y generalización es una técnica novedosa y con potencialidades para su uso en el reconocimiento facial. En el sistema desarrollado se utilizan las redes neuronales artificiales para el reconocimiento facial de forma rápida a través de la extracción de características tomadas de la imagen del rostro. La implementación del sistema incluye el desarrollo usando herramientas de *hardware* libre para la automatización del sistema de control de acceso. El sistema desarrollado fue implantado en una empresa en la ciudad de Ibarra, Ecuador, obteniéndose resultados favorables y que permiten el registro y control de acceso a los empleados y visitantes.

Abstract

This paper describes the development of a system based on artificial neural networks for fast faces recognition and their use in access control system. Facial recognition is a topic of great interest for its impact and possible applications related to employment issues, control space entry, safety, equipment activation and operation, among others. Access control is one of the activities that can help ensure the safety of personnel within an organization or in home environments, so it is important to use technological tools to assist the appropriate facial recognition and automate control access processes. Artificial intelligence has proved its usefulness and application in various areas of everyday life and particularly artificial neural networks for their learning ability and generalization is a novel and with potential for use in facial recognition technology. In the developed system, artificial neural networks are used for fast face recognition through the extraction of features taken from the facial image. The implementation of the system includes the development using free hardware tools for automation of the access control system. The developed system was implemented in a company in the city of Ibarra, Ecuador, obtaining favorable results and allowing the registration and control of access to employees and visitors.

Introducción

El reconocimiento facial (Serratosa, 2012) es un tema de gran interés por su impacto y posibles aplicaciones en temas de carácter laboral, control de acceso, seguridad ciudadana, entre otros.

Los sistemas biométricos permiten identificar a una persona mediante distintas partes del cuerpo humano (mano, ojos, rostro, dedo), claves de acceso o tarjeta, pero en varias ocasiones tanto las claves como las tarjetas son vulnerables a ultrajes o clonaciones respectivamente, a diferencia de los sistemas que se basan en biometría, que son considerados como uno de los sistemas más confiables (Motato Toro & Loaiza Correa, 2009).

El control de acceso (Li & Jain, 2004) es una de las medidas que puede contribuir a garantizar la seguridad del personal dentro de una organización empresarial, por lo cual se plantea desarrollar una aplicación de control de acceso basado en tecnologías de reconocimiento facial usando sistemas inteligentes particularmente las redes neuronales artificiales.

En la investigación realizada por Romero (2016) se realizaron pruebas mediante la utilización de imágenes obtenidas desde Internet e imágenes adquiridas con la cámara web y se concluye que los resultados alcanzados demostraron que la solución computacional es bastante robusta en cuanto a rotación lateral del rostro, así como también a distintos tipos de color de piel, siempre y cuando se cuente con niveles de iluminación adecuada.

En lo concerniente a sistemas biométricos son identificados principalmente por el área de reconocimiento facial, reconocimiento del iris del ojo y reconocimiento dactilar, teniendo en común el proceso de funcionamiento, que consiste en tres fases: mismos que tienen en común entrenamiento, almacenamiento y finalmente una de prueba, respectivamente (Espinosa Duró, 2001).

La inteligencia artificial ha demostrado su utilidad y aplicación en diversas áreas del quehacer cotidiano (Aguilar & Rivas, 2001) y particularmente las redes neuronales artificiales (Hagan, Demouth, Beale & De Jesús, 2014) por su capacidad de aprendizaje y generalización es una técnica novedosa y con potencialidades para su uso asociado con el reconocimiento facial. En este trabajo se pretende utilizar las redes neuronales artificiales para dicho reconocimiento facial y la adquisición de destrezas en el desarrollo de aplicaciones con esta técnica inteligente.

Marco Teórico

El reconocimiento facial es un área que forma parte del reconocimiento de patrones. En los últimos años ha cobrado un gran interés especialmente por la amplia gama de aplicaciones que tiene en distintos campos tales como seguridad, vigilancia, tarjetas inteligentes, entre otros.

A continuación, se describirán las metodologías actualmente utilizadas para el reconocimiento facial (Blázquez, 2013), citando algunas técnicas representativas de cada una de estas. Sin embargo, es importante mencionar que si bien en los últimos años se ha logrado un gran avance en el área de reconocimiento facial desarrollando técnicas más robustas que buscan solucionar problemas como cambios en iluminación, rotaciones, oclusiones, entre otros; todavía no se puede hablar de métodos para reconocimiento facial que resulten altamente confiables y tolerantes a diferentes condiciones o circunstancias de manera que asemejen el proceso de reconocimiento que lleva a cabo un ser humano. Por lo tanto, algunas metodologías presentan mejores resultados bajo unas condiciones y otras bajo condiciones diferentes, lo que permite indicar que la selección de una u otra metodología y de las técnicas empleadas, están basadas en los requerimientos específicos de la aplicación para la que se realiza la tarea de reconocimiento.

Metodologías para Reconocimiento facial a partir de imágenes estáticas

Métodos basados en características geométricas

Estos métodos están orientados a la construcción de modelos del rostro humano a partir de características geométricas (características invariantes) que permitan establecer diferencias faciales entre un rostro y otro. Los modelos pueden ir desde un conjunto de medidas antropométricas faciales tales como distancia ínterocular, separación entre ojos y nariz, separación entre boca y nariz, tamaño de la boca, tamaño de los ojos, alto o ancho del área del rostro, entre otras medidas; hasta modelos más complejos como diagramas elásticos compuestos por nodos en puntos definidos en el rostro (ojos, nariz, contornos, entre otros). Como se puede notar uno de los pasos esenciales en estos métodos es la detección de características locales (ojos, boca, nariz, entre otras), debido a que son la base para construir el modelo del rostro. Para llevar a cabo la detección de estas características, cada una es considerada como un nuevo patrón (con sus propias particularidades). Una de las me-

todologías más comúnmente utilizadas con este fin es la de correspondencia.

Una vez construido el modelo del rostro, métodos estadísticos o redes neuronales, generalmente son empleados para determinar la identidad de la persona a base del modelo creado y sus componentes.

Los métodos basados en características geométricas suelen ser menos afectados por cambios de iluminación en las imágenes lo que constituye una ventaja, sin embargo, presentan menor tolerancia a cambios de expresión facial y la construcción de los modelos puede ser difícil y costosa a nivel computacional.

Métodos holísticos o basados en la imagen

Son métodos conceptualmente relacionados con el uso de plantillas, tratan de identificar los rostros usando representaciones globales. Es decir, consideran a la imagen del rostro como un todo por lo tanto no trata de analizar su contenido, sino que extraen características relevantes de la región completa.

Una vez que han sido extraídas las características del área del rostro, al igual que en los métodos basados en características geométricas se pueden utilizar métodos estadísticos o redes neuronales para llevar a cabo el reconocimiento en sí. Este tipo de métodos son utilizados habitualmente en imágenes de baja resolución.

Métodos híbridos

Combinan aspectos de los métodos anteriores. Si se considera que los métodos holísticos y los basados en características geométricas tienen ventajas y desventajas con respecto al otro, el combinarlos se pueden lograr mejores resultados.

En este trabajo se utilizará uno de los métodos basados en características geométricas y a partir de allí se usará una red neuronal artificial para el reconocimiento facial.

Procedimiento Experimental

En este trabajo se utilizará uno de los métodos basados en características geométricas

Para la construcción del prototipo; se realizó una investigación sobre los fundamentos teóricos tanto de redes neuronales artificiales, reconocimiento facial, control de acceso, herramientas computacionales disponibles. La metodología usada está basada en la metodo-

logía para el desarrollo de sistemas inteligentes e Ingeniería de Software (Aguilar & Rivas, 2001).

En lo referente a los materiales y equipos utilizados se puede mencionar:

- Webcam Microsoft LifeCam Studio 1080p HD, la cual es encargada de obtener video al momento de hacer el reconocimiento facial.
- Notebook HP, el cual es el encargado de alojar el sistema DaxaControlAcces.
- Arduino mega 2560, el cual es el encargado de guardar la programación que interactúa con la cerradura eléctrica.
- Módulo de relés de 4 canales para Arduino, el cual es el encargado de conmutar cargas de corriente alterna conectada a la red eléctrica.
- Cerradura eléctrica viro de 12v, la cual es la encargada de aperturar la puerta.
- Transformador, el cual es el encargado de convertir una entrada de 110V a 12V que es lo que recibe la cerradura eléctrica.
- Fuente de poder, el cual es el encargado de recibir 110V y enviar 5V, con la finalidad que no exista sobrecarga de voltaje.
- Cortapico el cual es el encargado de proporcionar 6 tomas eléctricas.

Diseño y desarrollo del Sistema de reconocimiento facial basado en redes neuronales

En primera instancia se obtienen los patrones del rostro de los usuarios con los cuales se construiran las redes neuronales, los patrones con los que se trabaja son cuatro: ancho del rostro, alto del rostro, ancho y alto de los orígenes de la imagen.

Para obtener estos parámetros se lo realiza a través de una *webcam*, con la cual se obtiene durante un determinado tiempo las variaciones de patrones del rostro de un usuario, mediante la librería OpenCV (OpenCV 2018), y la existencia de un proceso de procesamiento de las imágenes de entrada y reconstrucción de las mismas.

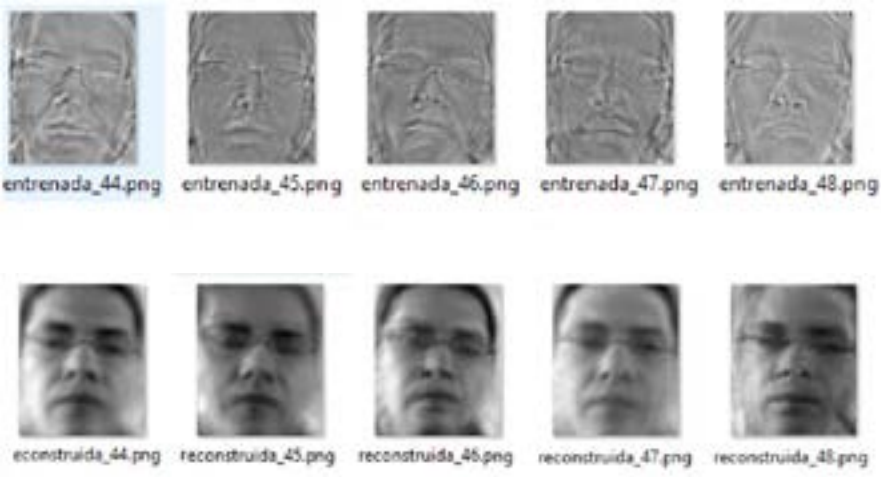


Figura 1. Imágenes de entrada y reconstrucción

Fuente: Elaboración propia

Una vez obtenidos los parámetros del rostro del usuario se procede a la construcción de la red neuronal, la cual genera como resultado una ecuación, que será utilizada en el sistema para la validación de usuarios y el control de acceso o denegación del mismo.

Proceso de validación del usuario en el sistema mediante la red neuronal:

1. **Toma de valores del usuario a autenticar**

```
this.alto = tmp.getValor1();
this.ancho = tmp.getValor2();
this.oAncho = tmp.getValor3();
this.oAlto = tmp.getValor4();
```

2. **Declaración de máximos y mínimos**

```
x1min = 104;
x1max = 228;
x2min = 104;
x2max = 228;
x3min = 113;
x3max = 251;
```

x4min = 29;
x4max = 331;

Ymin = -1;
Ymax = 1;

3. Normalización

x1n = 2 * (x1 - x1min) / (x1max - x1min) - 1;
x2n = 2 * (x2 - x2min) / (x2max - x2min) - 1;
x3n = 2 * (x3 - x3min) / (x3max - x3min) - 1;
x4n = 2 * (x4 - x4min) / (x4max - x4min) - 1;

4. Asignación de pesos red neuronal entrenada

w11 = -0.587100486;
w12 = 0.233240283;
w13 = -3.490420117;
w14 = -1.276337636;

w21 = 1.801362415;
w22 = 0.267724104;
w23 = 0.612835131;
w24 = 2.729071816;

w31 = -6.039753279;
w32 = -4.912155386;
w33 = 0.074250145;
w34 = -13.83817677;

ws1 = -1.94773E-05;
ws2 = -3.6281E-05;
ws3 = 0.999964837;
b11 = -2.513905805;
b12 = 2.542091713;
b13 = -13.14111851;
b21 = -1.81472E-05;

5. Cálculos de salida

z1 = w11 * x1n + w12 * x2n + w13 * x3n + w14 * x4n + b11;
z2 = w21 * x1n + w22 * x2n + w23 * x3n + w24 * x4n + b12;
z3 = w31 * x1n + w32 * x2n + w33 * x3n + w34 * x4n + b13;

y1 = java.lang.StrictMath.tanh(z1);
y2 = java.lang.StrictMath.tanh(z2);
y3 = java.lang.StrictMath.tanh(z3);

z21 = ws1 * y1 + ws2 * y2 + ws3 * y3 + b21;
Yn = (z21 + 1) / 2 * (Ymax - Ymin) + Ymin;

```
if (Yn >= 0.85) {
nombreU = "Jose Luis Ibarra Estévez";
}
```

La comunicación cliente, servidor es de manera directa, mientras que la comunicación entre el servidor y el sistema es como se indica en la Fig. 2.

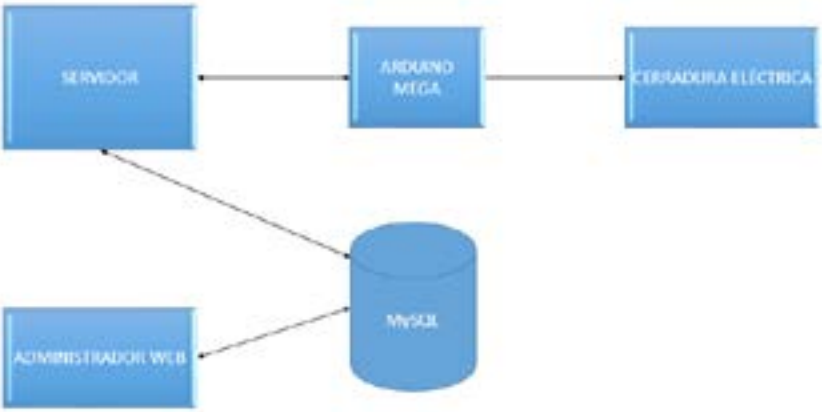


Figura 2. Comunicación entre interfaces

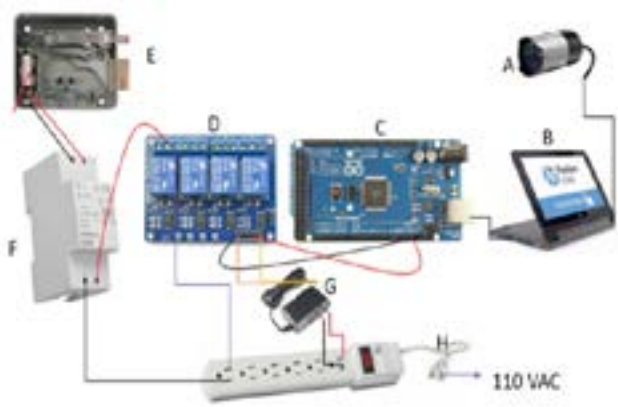
Fuente: Elaboración propia

El sistema inicia al momento que el usuario ingresa su contraseña de identificación, si es la correcta permite mostrar la pantalla de reconocimiento facial para que el usuario seleccione la opción de iniciar, e inmediatamente inicia el proceso de reconocimiento facial, en caso de ser exitoso el reconocimiento facial, el sistema envía el número de usuario a la base de datos y se encarga de registrar la hora y fecha provenientes del reloj en tiempo real y finalmente el sistema envía al Arduino una señal lógica e interactúa con la cerradura eléctrica para permitir el acceso.

La comunicación física entre el sistema con el arduino es por conexión serial, mientras que para la comunicación lógica del sistema con el arduino se realiza mediante comunicaciones RX (Envío) y TX (Recepción), mediante la librería de PanamaHitek_Arduino-2.7.3 (Antony García González 2017).

En la Fig. 3 se pueden observar las conexiones entre cada uno de los componentes físicos del sistema de control

de acceso basado en redes neuronales artificiales.



A. - Webcam Microsoft LifeCam Studio 1080p HD. - Se encarga de obtener video al momento de hacer el reconocimiento facial.

B.- Notebook HP.- Aloja el sistema DaxaControlAcces, es decir hace las veces de servidor.

C.- Arduino mega 2360.- Guarda la programación que interactúa con la cerradura eléctrica.

D.- Módulo de relays de 4 canales para Arduino.- Actúa como un control de voltaje.

E.- Cerradura eléctrica viro de 12v.- Es la encargada de quitar la traba de la puerta y aperturar la misma

F.- Transformador.- Convierte una entrada de 110V a 12V que es lo que recibe la cerradura eléctrica

G.- Fuente de poder.- Se encarga de recibir 110V y enviar 5V, con la finalidad que no exista sobre carga de voltaje.

H.- Cortapico.- Proporciona 6 tomas eléctricas.

Figura 3. Conexiones del Sistema

Fuente: Elaboración propia

La Fig. 4 ilustra el esquema de las actividades llevadas a cabo para el control de acceso diseñado.

Figura 4. Diagrama lógico de la capa de datos

Fuente: Elaboración propia

Este sistema fue implantado en la empresa Distribuidora Paredes, ubicada en la ciudad de Ibarra en Ecuador, con resultados altamente satisfactorios ya que permite el acceso automático a los empleados de la empresa, permite un registro de ingresos y egresos de la compañía e igualmente permite monitorear el intento de ingreso por personas desconocidas o no autorizadas a las instalaciones de la empresa.

Conclusiones

Con el desarrollo del control de acceso basado en reconocimiento facial mediante el uso de redes neuronales artificiales, se tiene un mayor control en el acceso a la empresa debido a que accede al reconocimiento facial una vez que se ingrese correctamente la contraseña del usuario, la misma que es generada por el sistema de forma automática, esto hace que el sistema sea más confiable.

El uso del sistema de acceso biométrico basado en el reconocimiento facial, permite que se monitoreen las fechas y horas de ingreso, a través de reportes generados por el sistema.

El sistema de control de acceso presentado es poco invasivo al usuario, dado que solo tiene que acercar el rostro a la cámara y el sistema se encarga del reconocimiento de usuario.

Se recomienda continuar la investigación utilizando otras técnicas inteligentes o híbridas, buscando nuevas alternativas de reconocimientos faciales de forma rápida.

En el diseño, se pueden realizar los siguientes trabajos futuros: colocar sistemas adicionales de seguridad como pueden ser: registro de usuario y envío de señal de alarma cuando un usuario intente ingresa un número de veces una clave incorrecta o cuando el sistema de reconocimiento facial no logre clasificar al usuario; enviar notificaciones mediante sms (mensajes cortos de texto) de atrasos o faltas a un número o números indicados.

BIBLIOGRAFÍA

Aguilar, J., & Rivas, F. (2001). *Introducción a las técnicas de computación inteligente*. Merida: Meritec.

García González, A., *Panamahitek*. 24 de 12 de 2017. http://panamahitek.com/libreria-panamahitek_arduino/ (último acceso: 3 de 1 de 2018).

OpenCV. OpenCV.org. 2018. www.OpenCV.org (último acceso: 3 de 1 de 2018).

Blázquez, L. (2013). *Reconocimiento Facial Basado en Puntos Característicos de la Cara en entornos no controlados* (tesis de grado). Escuela Politécnica Superior Universidad Autónoma de Madrid, Madrid, España.

Espinosa Duró, V. (2001). *Evaluación de Sistemas de Reconocimiento*. JCEE.

Hagan, M.; Demuth, H.; Beale, M. & De Jesús, O. (2014). *Neural Network Design*. 2nd Edition. USA.

Li, S, & Jain, A. (2004). *Handbook of Face Recognition*. Springer Edition. USA

Motato Toro, Ó. F., & Loaiza Correa, H. (2009). Identificación biométrica utilizando imágenes infrarrojas de la. *REVISTA INGENIERÍA E INVESTIGACIÓN*.

Romero, K. (2006). *Reconocimiento de rostros en tiempo real utilizando una red neuronal* (tesis de grado). Escuela Politécnica Nacional, Quito, Ecuador.

Serratosa, F. (2012). *La biometría para la identificación de las personas*. Editorial UOC. España.