La Mecatrónica en México, Vol. 4, No. 2, páginas 53 – 64, Mayo 2015
Disponible en línea en www.mecamex.net/revistas/LMEM
ISSN en trámite, 2014 Derechos de autor y derechos conexos, Asociación Mexicana de Mecatrónica A.C

Sistema de Autenticación Facial mediante la Implementación del algoritmo PCA modificado en Sistemas embebidos con arquitectura ARM

Andrés Ernesto López Sandoval, Cyntia Mendoza Martínez, Luis Ángel Reyes Cruz, Edgar Alejandro Rivas Araiza, Juan Manuel Ramos Arreguín, Jesús Carlos Pedraza Ortega

Facultad de Informática, Universidad Autónoma de Querétaro.
Av. de las Ciencias S/N Campus Juriquilla, Juriquilla, Querétaro, Qro.
C.P. 76230 México. Tel. 1921200 EXT. 5900
reyes.luis1010@gmail.com

Resumen

El reconocimiento facial es un área muy activa en el campo de la visión por computadora y se ha estudiado vigorosamente durante 25 años. El reconocimiento facial puede operar de dos modos: reconocimiento y autenticación. El reconocimiento o autenticación facial presentan una problemática, pues el promedio de aciertos en la estimación de la identificación es bajo, en particular, se estima que se encuentra entre un 35% y un 65% de efectividad, dependiendo de las condiciones de iluminación, tamaño de la imagen, etc. por lo que mediante el procesamiento digital de imágenes se deben realizar los ajustes necesarios de iluminación, ajuste de tamaño y mejora en el algoritmo pueda aumentar el porcentaje de reconocimiento en más de un 70%.

Aunado a lo anterior, en la mayoría de sistemas de control de acceso utilizan como medio de procesamiento de las imágenes una computadora personal y una cámara que captura el rostro y no indican que tipo de procesamiento llevan a cabo, es decir, que algoritmo se implementó. La idea principal de este proyecto es implementar un sistema de acceso por medio de reconocimiento facial e implementado en un hardware de arquitectura abierta. El sistema de reconocimiento facial propuesto se basa en una plataforma embebida de bajo consumo comprende un ARM (Advanced RISC máquinas) módulo central de procesamiento, un módulo de adquisición de vídeo, un módulo de visualización y una interfaz de transmisión de datos periférica. El algoritmo a implementar en el procesamiento digital de imágenes es el Principal Component Analysis (PCA) es robusto, rápido y eficiente para llevar a cabo el reconocimiento facial.

El sistema de reconocimiento facial basado en la plataforma embebida de bajo consumo tiene la ventaja de bajo consumo de energía, alta velocidad de computación, la alta precisión de reconocimiento, amplio campo de aplicación y similares.

Palabras clave: Reconocimiento Facial, PCA, ARM, Phyton.

1. Introducción

En los últimos años, el desarrollo de nuevo hardware y software informático para sistemas de seguridad ha experimentado un gran impulso, tal es el caso de los sistemas de reconocimiento por huella dactilar, voz, iris y facial. Entre estos, destaca por perfilarse como el más prometedor el reconocimiento facial.

La Mecatrónica en México, Vol. 4, No. 2, páginas 53 – 64, Mayo 2015
Disponible en línea en www.mecamex.net/revistas/LMEM
ISSN en trámite, 2014 Derechos de autor y derechos conexos, Asociación Mexicana de Mecatrónica A.C

La identificación de características faciales ha recibido un fuerte impulso gracias al avance en la tecnología de vídeo multimedia propiciándose así un aumento de cámaras en los lugares de trabajo, hogar y dispositivos móviles con un reducido coste [1]. El reconocimiento facial se puede aplicar en el control de accesos a edificios públicos y privados, cajeros automáticos, laboratorios de investigación, como clave secreta de acceso para el uso de ordenadores personales o terminales móviles de última generación así como para servir de tarjeta de visita de una persona.

El proceso de identificación facial se divide básicamente en dos tareas: detección y reconocimiento [2]. La primera de ellas, la detección, comprende la localización de una o varias caras dentro de una imagen, ya sea fija o una secuencia de vídeo. La segunda tarea, el reconocimiento, consiste en la comparación de la cara detectada en el paso anterior con otras almacenadas previamente en una base de datos. Estos procesos, detección y reconocimiento, no deberían ser totalmente independientes debido a que según la forma en la que se detecte una cara puede ser prácticamente imposible su reconocimiento con caras de una base de datos detectadas de manera diferente, de ahí que los sistemas de reconocimiento facial estén fuertemente condicionados por la posición y orientación de la cara del sujeto con respecto a la cámara y las condiciones de iluminación en el momento de realizar la detección.

Para implementar un sistema de reconocimiento de rostros se presentan 6 etapas bien definidas: Captura de la imagen, preprocesamiento, localización, escalamiento y ajuste, extracción de características y por último la clasificación la toma de decisión.

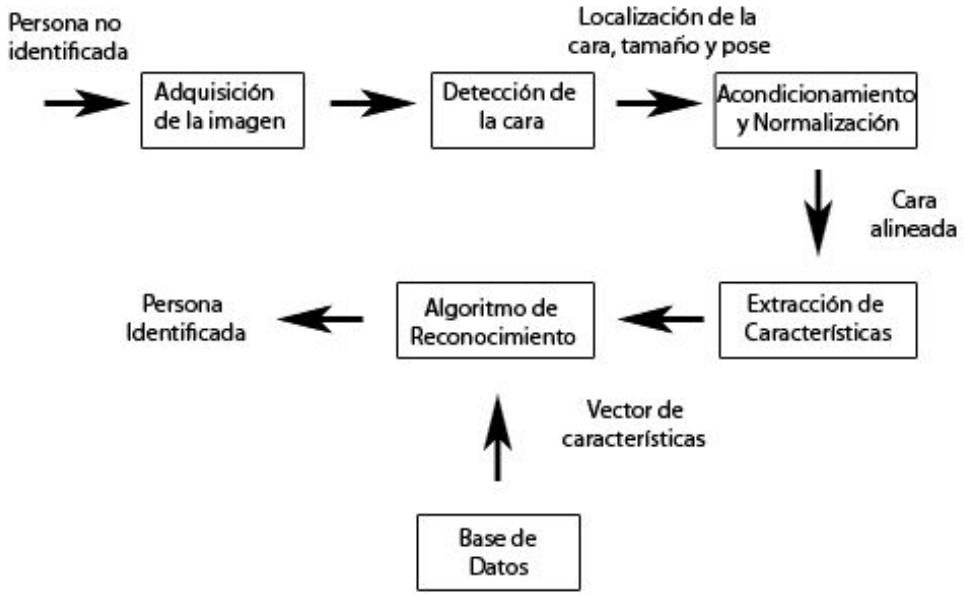


Figura 1. Esquema general para implementar un sistema de reconocimiento facial [3].

Dentro de la captura de la imagen se encuentra la selección de la cámara digital y las características del ambiente de la fotografía que se realizara como la iluminación, ya sean controladas o no controladas.

El preprocesamiento de la imagen capturada incluye la selección del espacio de color en el que se desea trabajar o la extracción de la intensidad en el caso de que se trabaje con escala de grises.

La Mecatrónica en México, Vol. 4, No. 2, páginas 53 – 64, Mayo 2015
Disponible en línea en www.mecamex.net/revistas/LMEM
ISSN en trámite, 2014 Derechos de autor y derechos conexos, Asociación Mexicana de Mecatrónica A.C

Una vez preprocesada la imagen de entrada se determina las coordenadas donde se encuentra la posición de la cara dentro de la escena, normalmente se desea determinar las coordenadas de una sub-imagen formada solo por la zona de la cara delimitada por las orejas, la frente y el mentón. Para determinar estas coordenadas normalmente se utiliza un algoritmo basado en una cascada de clasificadores básicos. Otras estrategias para localizar el rostro consisten en determinar la posición de los ojos, y en otros casos se utiliza la información del color de la piel como metodología para determinar la región que forma exclusivamente la cara, o clasificadores basados en redes neuronales.

En algunos sistemas se realiza la normalización de la cara ya sea utilizando la información de partes como los ojos, nariz u otras características, o simplemente realizando un escalado de la imagen. Los sistemas que solo hacen hasta las operaciones ahora mencionadas se llaman sistemas de localización.

Determinada la región que contiene el rostro se procede a extraer sus características. Para ello se puede utilizar diversas técnicas como lo es PCA, entre otras como SIFT (Scale Invariant Feature Transform) y SURF (Speeded Up Robust Features). Normalmente esta operación produce un vector de características de baja dimensión que debe ser comparado con una base de datos de personas previamente almacenada [4].

1.1 Sistemas embebidos con arquitectura ARM

Se puede definir los sistemas embebidos como un sistema electrónico de procesamiento programado para realizar funciones o tareas para un objetivo específico. Cuando los sistemas son más grandes se pueden incluir además de elementos electrónicos y de software, partes mecánicas, eléctricas y electromecánicas.

En la actualidad, los sistemas embebidos forman parte de la vida cotidiana de todos. En general, la sociedad no tiene conocimiento de la gran cantidad de sistemas embebidos que forman parte de la vida diaria. Por ejemplo, relojes digitales, teléfonos celulares o el horno de microondas.

El software embebido difiere del software convencional de una computadora por las siguientes características:

- Los sistemas embebidos pueden ser de tiempo real.
- Tienen una interfaz directa con el hardware del dispositivo.
- Suele considerarse las pruebas de hardware como parte del desarrollo del sistema embebido.
- Suele haber más control del tiempo de respuesta y manejo de recursos como memoria.
- Requiere de recursos humanos sumamente especializados en las áreas informáticas, electrónicas, etc.

Los sistemas embebidos, por lo tanto, han sido y seguirán siendo cruciales en la mayoría de los dispositivos electrónicos. La industria electrónica sigue cambiando, necesitando modelos y arquitecturas de diseño más complejas en ciclos de desarrollo más reducidos. Los dispositivos programables lograron un cambio profundo en los esquemas de desarrollo al integrar hardware y software en componentes reconfigurables, conservando atributos vitales como eficiencia, costo, tiempo de desarrollo, entre otros [5].

En los últimos años se ha desarrollado toda una nueva industria de tarjetas de desarrollo electrónicas para sistemas embebidos, es decir, para sistemas móviles que muchas veces corren de manera automática e independientemente.

Considerando un sistema embebido como se ha mencionado anteriormente, y específicamente en el procesador que tiene incluido, que contiene una arquitectura ARM. Podemos considerar las siguientes características [6]:

La Mecatrónica en México, Vol. 4, No. 2, páginas 53 – 64, Mayo 2015
Disponible en línea en www.mecamex.net/revistas/LMEM
ISSN en trámite, 2014 Derechos de autor y derechos conexos, Asociación Mexicana de Mecatrónica A.C

- Bajo consumo
- Capacidad de procesado
- Reducción del tiempo de desarrollo hardware
- Alta escalabilidad
- Tamaño muy compacto
- Soportan varios módulos embebidos de ARM
- Sistemas operativos Linux y Android
- Plataforma de desarrollo flexible

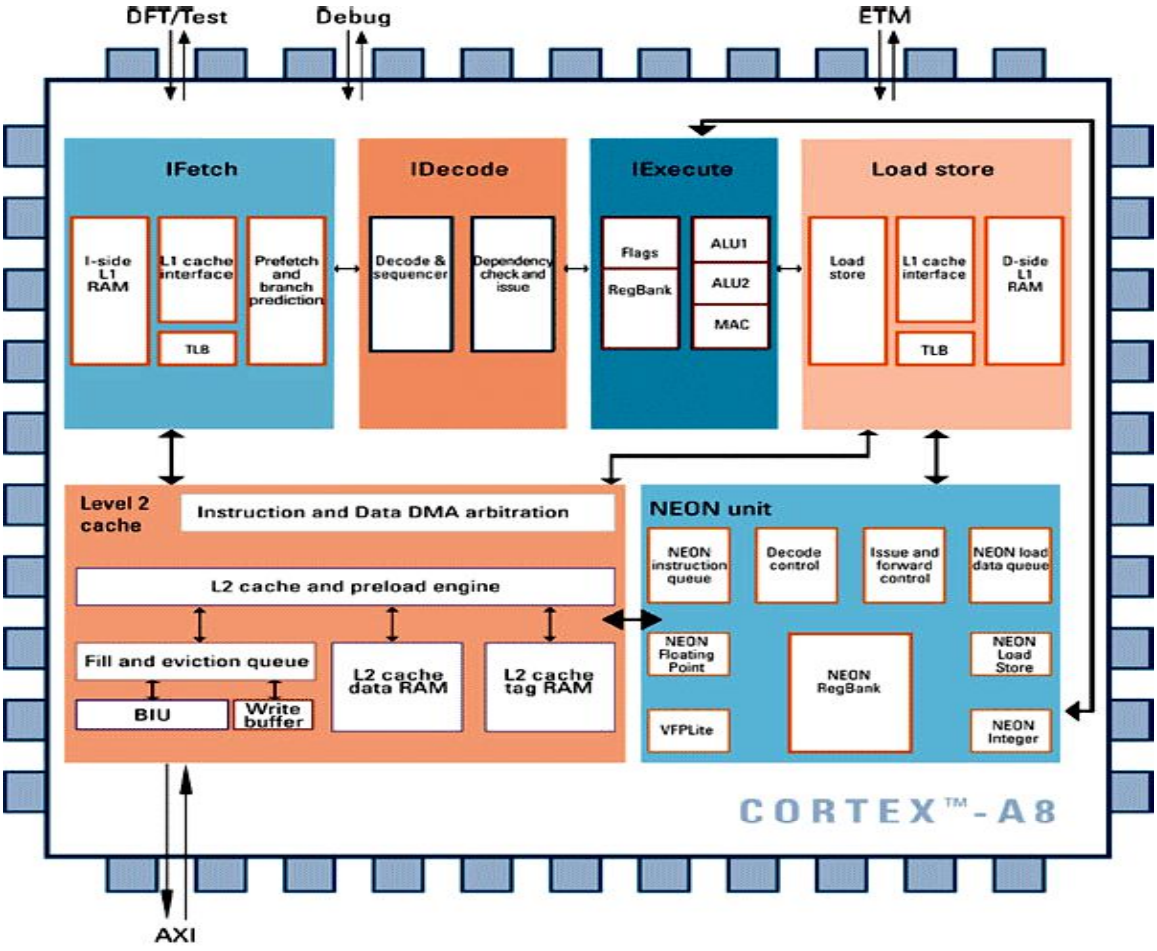


Figura 2. Esquema general de la arquitectura ARM [7].

Este tipo de sistemas ya se encuentran en muchos lugares y sirven para medir la temperatura ambiente, para llevar el control de la seguridad de una fábrica o para enviar información de manera inalámbrica. Los usos sólo están limitados por la imaginación de los desarrolladores.

1.2 Justificación de la investigación

En la mayoría de sistemas de reconocimiento facial utilizan como medio de procesamiento de las imágenes una computadora personal y una cámara que captura el rostro y no indican que tipo de procesamiento llevan a cabo, es decir, que algoritmo se implementó. El sistema de reconocimiento facial propuesto se basa en una plataforma embebida de bajo consumo, comprende un procesador con arquitectura ARM (Advanced RISC máquinas) módulo central de procesamiento, un módulo de

La Mecatrónica en México, Vol. 4, No. 2, páginas 53 – 64, Mayo 2015
Disponible en línea en www.mecamex.net/revistas/LMEM
ISSN en trámite, 2014 Derechos de autor y derechos conexos, Asociación Mexicana de Mecatrónica A.C

adquisición de vídeo, un módulo de visualización y una interfaz de transmisión de datos periférica. El algoritmo que se planea implementar (PCA) tiene entre otras característica el ser robusto, rápido y eficiente.

El sistema de reconocimiento facial basado en la plataforma embebida de arquitectura abierta tiene la ventaja de bajo consumo de energía, alta velocidad de computación, la alta precisión de reconocimiento, amplio campo de aplicación y similares.

2. Metodología

La biometría se refiere a la identificación de una persona en base a sus características físicas y de comportamiento. Los sistemas que se basan en la biometría incluyen las características de: huellas dactilares, geometría de la mano, la voz, el iris, el rostro, etc. [8]. La biometría es usada para muchos propósitos, tales como la detección de criminales, identificación, el control de acceso, entre otros [9].

"El reconocimiento facial" es un área muy activa en el campo de la visión por computadora y datos biométricos, ya que se ha estudiado vigorosamente durante 25 años y finalmente produce aplicaciones en seguridad, la robótica, la interfaces hombre-máquina, cámaras digitales, juegos y entretenimiento.

El reconocimiento facial puede operar de dos modos: reconocimiento o identificación y autenticación o verificación. Llevar a cabo un reconocimiento o identificación facial significa dar una imagen de la cara y se requiere que el sistema diga quién (si él o ella) es la más probable identificación. En este procedimiento se dice que la coincidencia es de 1:K, donde K representa el número de clases, es decir, se compara la imagen de entrada con las K existentes en la base de datos para concluir si se trata de una coincidencia o no [10].

Mientras que en la autenticación o verificación facial, dada una imagen del rostro y una estimación de la identificación, se requiere que el sistema diga si es verdadera o falsa la estimación que se realizó. En este caso la coincidencia es de 1:1 ya que dada una imagen de entrada se compara con una sola clase de imágenes (la cual representa un conjunto de imágenes de la misma persona, ver Figura 4).

El reconocimiento o autenticación facial presenta una problemática, pues el promedio de aciertos en la estimación de la identificación es bajo, en particular, se estima que se encuentra entre un 35% y un 65% de efectividad, dependiendo de las condiciones de iluminación, tamaño de la imagen, etc. por lo que el sistema de autenticación facial mediante procesamiento digital de imágenes debe realizar los ajustes necesarios (compensar) de iluminación, de ajuste de tamaño y de mejora en el algoritmo de reconocimiento facial para aumentar el porcentaje de reconocimiento en más de un 70%.

Aunado a lo anterior, en la mayoría de sistemas de control de acceso utilizan como medio de procesamiento de las imágenes una computadora personal y una cámara que captura el rostro y no indican que tipo de procesamiento llevan a cabo, es decir, que algoritmo se implementó. En la mayoría de los sistemas trabajan con 1 o máximo 2 algoritmos, sin que se pueda modificar. En este caso la propuesta es utilizar un sistema basado en un módulo de procesamiento con núcleo ARM (Advanced RISC máquinas) y un sistema de adquisición de imágenes utilizando una webcam de alta definición (HD). El desarrollo propuesto se llevará a cabo con herramientas de código abierto, lo que facilitara el proceso de implementar diferentes algoritmos en el mismo sistema de desarrollo.

Para el desarrollo de este proyecto es necesaria la adquisición de una imagen de entrada, a la cual se le aplicará el algoritmo PCA para adquirir sus puntos de interés.

La Mecatrónica en México, Vol. 4, No. 2, páginas 53 – 64, Mayo 2015
Disponible en línea en www.mecamex.net/revistas/LMEM
ISSN en trámite, 2014 Derechos de autor y derechos conexos, Asociación Mexicana de Mecatrónica A.C

Una vez que se ha realizado este proceso, el siguiente paso consiste en enviar la información de estos puntos mediante una conexión inalámbrica para hacer una comparación de las características de la imagen de entrada con las características de las imágenes que se encuentran almacenadas en el servidor.

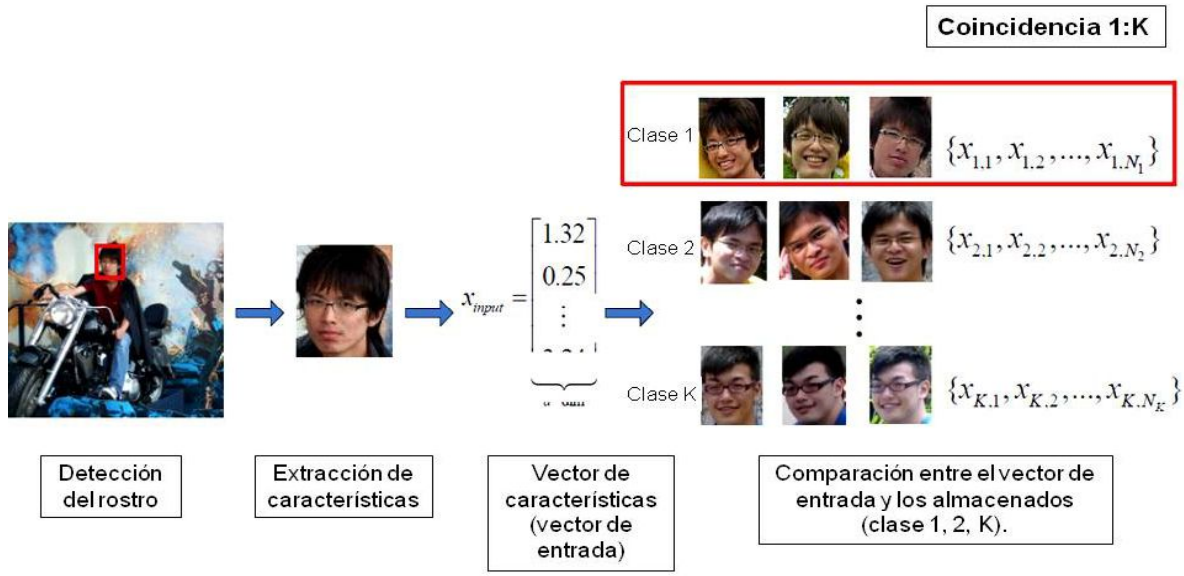


Figura 3. Reconocimiento o Identificación facial [10].

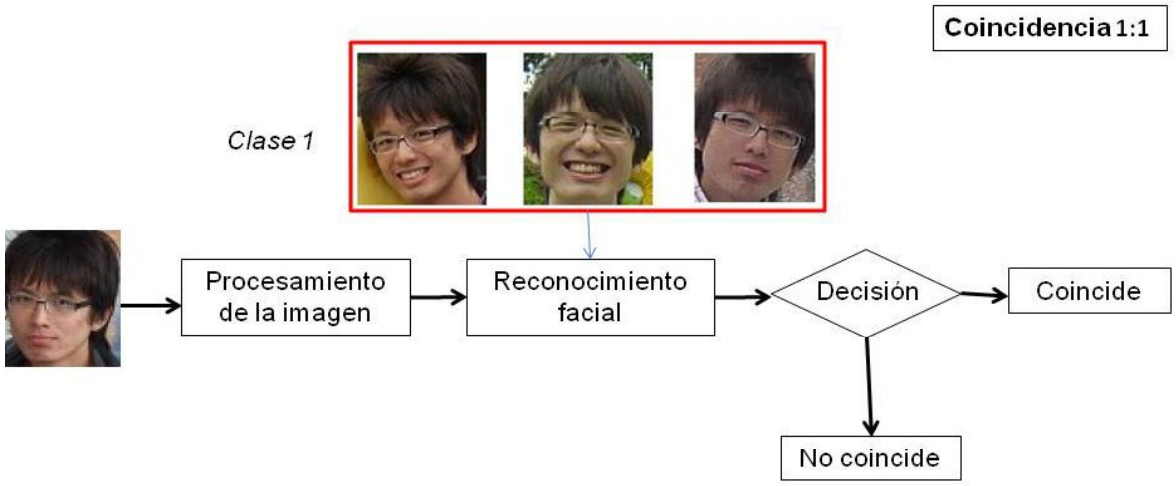


Figura 4. Autenticación o Verificación facial.

Posteriormente se realizará el proceso de autenticación para definir si las características faciales del usuario que intenta tener acceso al dispositivo móvil, corresponden con las del usuario que se tienen almacenadas en el servidor, si el resultado es correcto se podrá acceder al dispositivo móvil pero si el resultado es incorrecto, a este usuario no se le permitirá el acceso.

Los pasos a seguir son los siguientes:

La Mecatrónica en México, Vol. 4, No. 2, páginas 53 – 64, Mayo 2015
Disponible en línea en www.mecamex.net/revistas/LMEM
ISSN en trámite, 2014 Derechos de autor y derechos conexos, Asociación Mexicana de Mecatrónica A.C

- Imagen de entrada desde la webcam. Se obtienen las características de los puntos de interés de la imagen por medio del algoritmo PCA.
- Características de la imagen.
- Comunicación vía inalámbrica.
- Base de datos con las características de las imágenes del usuario. Se realiza comparación entre las características de la imagen de entrada y las almacenadas.
- Resultado de la comparación.
- Se acepta o rechaza el acceso del usuario mediante una señal de salida de la tarjeta de desarrollo.

Uso de Bases de Datos de Imágenes. Con la finalidad de validar la metodología propuesta es necesario implementarla en bases de imágenes confiables, las cuales se utilizan en una gran parte de artículos de la literatura citada en este proyecto.

Adquisición de las imágenes. Además de contar con bases de imágenes, se pueden adquirir un conjunto de imágenes del rostro de una persona [11], con características como; las imágenes se tomarán con perfil frontal a la cámara, bajo diferentes condiciones de iluminación, expresiones faciales mínimas y poca variación en la posición de la cabeza.

Creación de la Base de Datos. En una computadora se creará una base de datos la cual almacenará las características de las imágenes adquiridas, con las cuales se estarán comparando las características de la imagen de entrada para determinar si el sistema permite o no la autenticación del usuario que intenta tener acceso al dispositivo móvil.

El método Eigenfaces adopta un enfoque holístico para el reconocimiento facial: Una imagen de la cara es un punto de un espacio de imagen en un conjunto de alta dimensión y se encuentra representación en una dimensión menor, en la cual la clasificación se lleva a cabo de forma sencilla.

El subespacio dimensional inferior se encuentra con el método PCA, que identifica los ejes con varianza máxima. Si bien este tipo de transformación es óptima desde el punto de vista de reconstrucción, que no toma ninguna etiqueta de clase en cuenta. Imagine una situación en la que se genera la varianza de fuentes externas, por ejemplo la iluminación. Los ejes con la máxima varianza no contienen necesariamente información discriminativa en absoluto, por lo tanto, una clasificación se hace imposible. De esta forma, se puede aplicar una proyección específica de clase con un discriminante lineal para el reconocimiento facial. La idea básica es reducir al mínimo la varianza dentro de una clase, mientras que maximiza la varianza entre las clases al mismo tiempo. Recientemente surgieron varios métodos para la extracción de características locales. Para evitar la alta dimensionalidad de los datos de entrada sólo regiones locales de una imagen se describen las características extraídas son (con suerte) más robusto frente a la oclusión parcial, iluminación y pequeño tamaño de la muestra.

El problema que tenemos en la imagen es su alta dimensionalidad. Imágenes bidimensionales (p x q) en escala de grises abarcan un espacio vectorial m = pq-dimensional, de tal forma que una imagen de 100 x 100 pixeles se encuentra en un espacio de imagen 10,000-dimensional. ¿Es demasiada información para cualquier cálculo, pero son todas las dimensiones realmente útiles para nosotros? Sólo podemos tomar una decisión si hay alguna variación en los datos, por lo que lo que estamos buscando son los componentes que representan la mayor parte de la información. El PCA se propuso para convertir un conjunto de variables posiblemente correlacionadas en un conjunto menor de variables no correlacionadas. La idea es que un conjunto de datos de alta dimensión es a menudo descrito por variables correlacionadas y, por tanto, sólo unas pocas dimensiones significativas representan la mayor parte de la información. El método PCA encuentra las direcciones con la mayor varianza en los datos, llamado componentes principales.
A continuación se presenta el algoritmo PCA.

La Mecatrónica en México, Vol. 4, No. 2, páginas 53 – 64, Mayo 2015
Disponible en línea en www.mecamex.net/revistas/LMEM
ISSN en trámite, 2014 Derechos de autor y derechos conexos, Asociación Mexicana de Mecatrónica A.C

Se considere un vector aleatorio $X = \{x_1, x_2, \dots, x_n\}$ con observaciones $x_i \in \mathbb{R}^d$

1. Calcular la media

$$X = \{x_1, x_2, \dots, x_n\} \quad (1)$$

2. Calcular la matriz de Covarianza

$$X = \{x_1, x_2, \dots, x_n\} \quad (2)$$

3. Calcular los eigenvalores λ_i y eigenvectores v_i de *S*

$$Sv_i = \lambda_i v_i \ , \ i = 1,2,3, \dots, n \quad (3)$$

4. Ordenar los eigenvectores en orden descendente por sus eigenvalores. Los *k* componentes principales son los eigenvectores correspondientes a los k eigenvalores mayores.

Los *k* componentes principales del x valor observado, están dados por

$$y = W^T(x - \mu) \quad (4)$$

Donde $W = (v_1, v_2, \dots, v_k)$. La reconstrucción que lleva a cabo el PCA se hace en base a

$$x = Wy + \mu \quad (5)$$

El método de Eigenfaces lleva a cabo el reconocimiento facial mediante los siguientes pasos:

a) Se proyectan todas las muestras de entrenamiento en el sub-espacio PCA utilizando la Ec. 4.
b) Proyectar la imagen que se busca en el sub-espacio PCA utilizando la Ec. 5.
c) Encontrar el vecino más próximo entre las imágenes de entrenamiento proyectadas y la imagen que se busca.

3. Resultados

3.1 Reconocimiento de rostros con eigenfaces (PCA) utilizando C++ y OpenCV

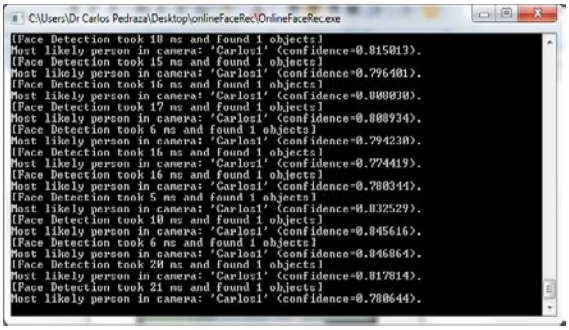
En el proyecto se incluyó el método de "Eigenfaces" debido a que es uno de los métodos más utilizados, además de ser robusto en su implementación, y finalmente por su rapidez en la ejecución. Para este propósito, se tomó como base el desarrollo de herramientas basadas en C++, debido a su velocidad para el cálculo matricial. Además, se utilizó la librería OpenCV para implementar los algoritmos de procesamiento de imágenes. El primer desarrollo fue creado con Visual Studio 2010, y librerías de OpenCV 2.3, como se muestra en la Figura 5.

"El reconocimiento facial" por lo general consta de dos etapas: (i) detección de la cara, donde en la foto se busca encontrar alguna cara, entonces el procesamiento de la imagen se centra en procesar la información de esa cara detectada, reduciendo el área de procesamiento, (ii) reconocimiento facial, donde ese rostro detectado y procesado se compara con una base de datos de caras conocidas, para decidir quién es esa persona.

La Mecatrónica en México, Vol. 4, No. 2, páginas 53 – 64, Mayo 2015
Disponible en línea en www.mecamex.net/revistas/LMEM
ISSN en trámite, 2014 Derechos de autor y derechos conexos, Asociación Mexicana de Mecatrónica A.C

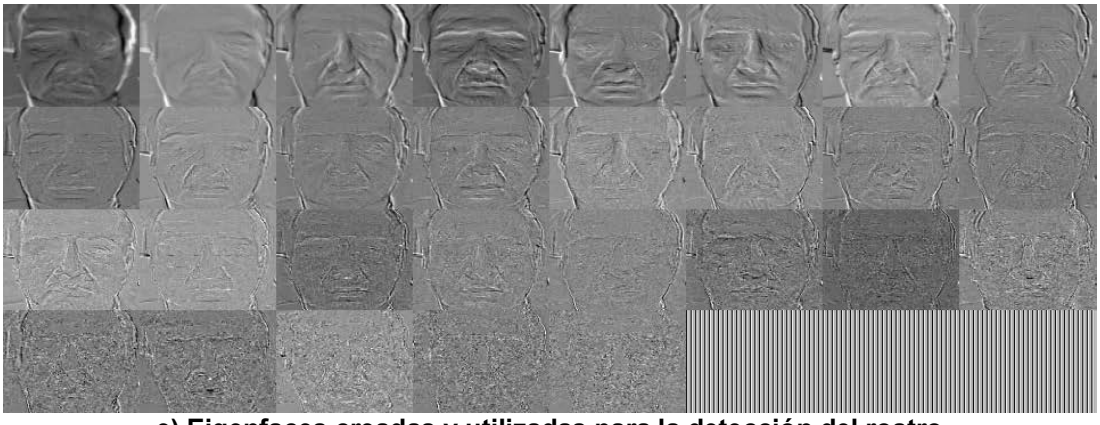
a) Detección de rostro 1

b) Detección de rostro 2



c) Tiempo de detección

d) Imagen promedio



e) Eigenfaces creadas y utilizadas para la detección del rostro

Figura 5. Pruebas del software desarrollado, utilizando el método de Eigenfaces

En la Figura 6 se puede mostrar el software desarrollado en sus 2 etapas, en la parte a) se muestra la imagen, en donde se resalta en color verde la detección del rostro 1, en esta área se

La Mecatrónica en México, Vol. 4, No. 2, páginas 53 – 64, Mayo 2015
Disponible en línea en www.mecamex.net/revistas/LMEM
ISSN en trámite, 2014 Derechos de autor y derechos conexos, Asociación Mexicana de Mecatrónica A.C

localiza la detección de la cara, y abajo de esta localización se muestra el nivel de confidencia con el cual se detectó el rostro. En el inciso c) se muestra el tiempo que se tomó para la detección del rostro. La imagen promedio de las caras utilizadas para la detección, se muestra en el inciso d) de la Figura 5. Finalmente, las Eigenfaces creadas y utilizadas para la detección se muestran en el inciso e) de la Figura 5.

3.2 Reconocimiento de rostros con eigenfaces (PCA) utilizando Python – OpenCV

El reconocimiento de rostros se realiza en dos etapas. La primera etapa consiste en la detección del rostro, donde se busca en la imagen un rostro, y se toma solamente esa sección, que es con la que se trabaja para continuar con la segunda etapa. En la segunda etapa, se toma la imagen exclusivamente del rostro reconocido y esa imagen es procesada y comparada contra una base de datos de rostros conocidos, para decidir qué persona es.

En la figura 6 se muestra un diagrama a bloques del proceso utilizado en Python, para obtener la sección del rostro, para su comparación con una base de datos.

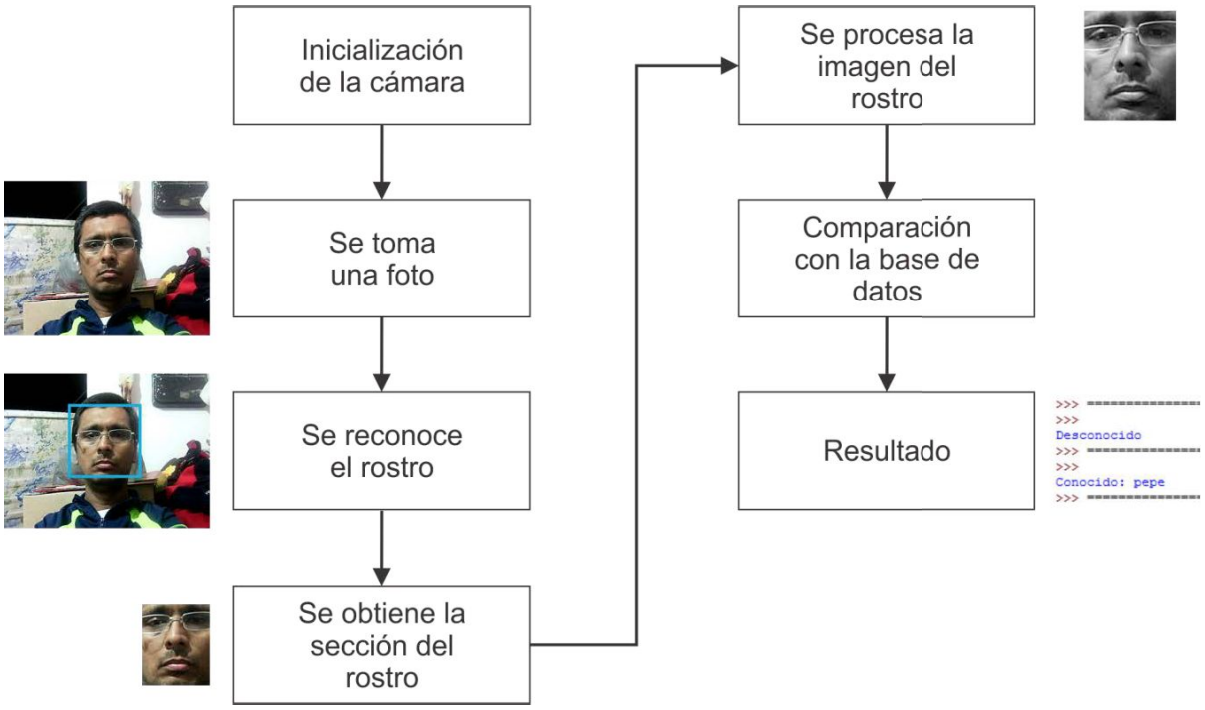


Figura 6. Metodología para el reconocimiento del rostro.

La metodología es implementada utilizando el lenguaje de programación Python, el cual es compatible con el sistema Debian, instalado en una tarjeta Beagleboard, para el desarrollo del proyecto. El programa mencionado utilizó librerías OpenCV para el procesamiento de imágenes. A continuación, se describe brevemente el proceso del programa en Python.

1. La cámara es inicializada utilizando la función VideoCapture(0). El valor 0 es para indicarle el número de la cámara. En caso de contar con dos cámaras, la segunda cámara tendrá el número 1.

2. El video es capturado de manera continua, al tiempo que se está detectando de manera continua el rostro.
3. Una vez detectado el rostro, el mismo es marcado por un cuadrado, en este caso de color azul.
4. Se extrae la sección de la imagen que contiene el rostro.
5. La imagen es redimensionada a un tamaño de 125x150 pixeles.
6. Se convierte la imagen a escala de grises, y se aplica un proceso de ecualizado para lograr un contraste adecuado de la imagen.
7. Se realiza una comparación contra una base de datos, y se devuelve el resultado. En caso de tener una comparación exitosa, se indica el nombre de la persona con la que coincide el rostro y en caso contrario, se devuelve como resultado: “Desconocido”.
8. Termina el programa.

4. Conclusiones

El presente trabajo de investigación muestra una propuesta para autenticación facial utilizando el algoritmo Principal Component Analysis (PCA) modificado. La metodología propuesta se desarrolló en dos etapas; la primera fue la implementación del algoritmo SURF en C++ con librerías OpenCV con la finalidad de valorar el algoritmo, y la segunda se implementó en Python 2.7 y el uso de librerías de OpenCV.

La metodología propuesta fue probada con la adquisición de múltiples imágenes con poses diferentes de varios usuarios, se entrenó al sistema y posteriormente se implementó la parte del reconocimiento facial. Nuestra metodología propuesta tiene un mejor rendimiento en el porcentaje de autenticación y reconocimiento que el algoritmo PCA original.

Creemos que existen algunos aspectos que se pueden cambiar en este proceso para obtener un porcentaje de autenticación y reconocimiento más alto. Entre estos aspectos a considerar tenemos un análisis más profundo en la etapa de preprocesamiento, así como del efecto de la expresión facial y pose.

Como trabajo futuro tenemos la elaboración de una base de datos de imágenes más amplia con diferentes condiciones de iluminación y algunas posiciones del rostro (ejem., frente al dispositivo de captura y con algún ángulo de rotación de la cabeza). Estas bases de datos de imágenes servirán para ver y valorar la repetibilidad del algoritmo y si tiene alguna variación con los porcentajes de autenticación y reconocimiento facial.

Finalmente es necesario mencionar que se pueden implementar las pruebas en diferentes tarjetas con arquitectura ARM; ejem. Raspberry Pi (modelos B, B+ y 2), BeagleBone Black, etc., con la finalidad de verificar el desempeño de este tipo de hardware embebido y poder así plantear el desarrollo de un sistema de reconocimiento facial más robusto y con un número mayor de núcleos de procesamiento.

Referencias

[1] Brunelli, Roberto, and Tomaso Poggio. "Face recognition: Features versus templates." IEEE Transactions on Pattern Analysis & Machine Intelligence 10 (1993): 1042-1052..
[2] Zhao, Wenyi, et al. "Face recognition: A literature survey." ACM computing surveys (CSUR) 35.4 (2003): 399-458..
[3] Hernández, R. G. Estudio de técnicas de reconocimiento facial., Departamento de Procesado de Señal y Comunicaciones. 2010.

http://upcommons.upc.edu/pfc/bitstream/2099.1/9782/1/PFC_RogerGimeno.pdf (Consultado el 28 de Febrero del 2015)

[4] Fuentes, Benoit, Roland Badeau, and Gaël Richard. "Adaptive harmonic time-frequency decomposition of audio using shift-invariant PLCA." Acoustics, Speech and Signal Processing (ICASSP), 2011 IEEE International Conference on. IEEE, 2011.

[5] Aceves M. & Ramos J., “Fundamentos de Sistemas Embebidos”, Asociación Mexicana de Mecatrónica A.C. México. 1ra edición, 2012.

[6] Romero M. E., Martínez E. A.,. Microcontroladores de 32 bits ARM. 2011

[7] Embedinfo, 2014. Embedded System Development Specialist. , http://www.embedinfo.com/en/ARM_Cortex-list.asp?id=15 (Consultado el 28 de Febrero del 2015)

[8] Brumnik, Robert, Iztok Podbregar, & Teodora Ivanuša. “Reliability of Fingerprint Biometry (Weibull Approach)”. INTECH Open Access Publisher, 2011.

[9] Duc, Nguyen Minh, and Bui Quang Minh. "Your face is not your password face authentication bypassing lenovo–asus–toshiba." Black Hat Briefings. 2009.

[10] Chao, Wei-Lun. "Face Recognition.". GICE, National Taiwan University. 2007.

[11] Bhattacharyya, Debnath, et al. "Biometric authentication: A review." International Journal of u-and e-Service, Science and Technology 2.3. 2009.