Universidad Autónoma de Querétaro
Facultad de Informática
Maestría en Ciencias de la Computación

Autenticación facial para dispositivo móvil basado en el algoritmo SURF e implementado en el sistema operativo Android.

Tesis

Que como parte de los requisitos para obtener el grado de
Maestro en Ciencias de la Computación

Presenta:
ISC. Cyntia Mendoza Martínez

Dirigido por:
Dr. Jesús Carlos Pedraza Ortega

SINODALES

Dr. Jesús Carlos Pedraza Ortega
Presidente — Firma

Dr. Saúl Tovar Arriaga
Secretario — Firma

Dr. Juan Manuel Ramos Arreguín
Vocal — Firma

Dr. Efrén Gorrostieta Hurtado
Suplente — Firma

Dr. Arturo González Gutiérrez
Suplente — Firma

M.I.S.D. Juan Salvador Hernández Valerio
Director de la Facultad

Dra. Ma. Guadalupe Flavia Loarca Piña
Directora de Investigación y Posgrado

Centro Universitario
Querétaro, Qro.
Febrero de 2016
México

RESUMEN

En este trabajo se propone una fase de preprocesamiento de imágenes así como del uso del algoritmo SURF (Speeded Up Robust Features) dentro de la etapa de extracción de características del proceso de autenticación facial, el cual es ejecutado en diferentes dispositivos móviles como Smartphones y Tablets con sistema operativo Android. La metodología propuesta consta de los siguientes seis pasos principales: imágenes del rostro, normalización, detección del rostro, extracción de características (preprocesamiento), coincidencias y decisión, donde a partir de la definición de un umbral heurístico se determina si la autenticación fue exitosa o errónea. Con el fin de que cada imagen tenga una distribución uniforme de sus niveles de gris la técnica de ecualización de histograma es usada en la fase de preprocesamiento, como resultado se obtiene una imagen mejorada para posteriormente pasar al siguiente paso de la metodología propuesta. Dentro de la sección de pruebas se emplearon las bases de datos públicas: The Extended Cohn-Kanade Dataset (CK+), Caltech Faces y FERET, así mismo, se usó la base de datos denominada SURFace la cual fue generada a lo largo de este trabajo. Finalmente, los resultados obtenidos con seis diferentes dispositivos móviles demuestran que la tasa de autenticación facial con las técnicas propuestas fue del 90%.

(**Palabras clave**: android, autenticación facial, biometría, ecualización de histograma, procesamiento de imágenes, SURF)

SUMMARY

In this work a phase of image preprocessing is proposed also the SURF algorithm (Speeded Up Robust Features) into the feature extraction step of face authentication process, which one is executed in different mobile devices such as Smartphones and Tablets with Android operative system. The proposed methodology contains the following six principal steps: face images, normalization, face detection, feature extraction (preprocessing), coincidences and decision, where considering the definition of a heuristic threshold it is determined if the authentication was correct or incorrect. In order that each image has a uniform distribution of its gray levels the histogram equalization technique is used in the preprocessing phase, as a result a better image is obtained to continue with the next step of the proposed methodology. Into the test section the following public face databases were used: The Extended Cohn-Kanade Dataset (CK+), Caltech Faces and FERET, furthermore the face database named SURFace was used, which one was generated throughout this work. Finally, the obtained results with six different mobile devices shows that the face authentication rate with the proposed techniques was 90%.

(**Key words**: android, face authentication, biometrics, histogram equalization, image processing, SURF)

Dedicado a todos los que se preguntan si estoy escribiendo sobre ellos.

AGRADECIMIENTOS

A todos aquellos que NUNCA creyeron en mi…

Pero también a aquellos que NUNCA dejaron de hacerlo.

TABLA DE CONTENIDOS

ÍNDICE DE TABLAS

ÍNDICE DE FIGURAS

1. INTRODUCCIÓN

1.1. Definición del proyecto de investigación

En este proyecto se presenta el desarrollo e implementación de una metodología en una aplicación (app) la cual permite realizar la autenticación facial de individuos en dispositivos móviles con sistema operativo Android. Para ello se realiza una serie de métodos de preprocesamiento en las imágenes utilizadas, así mismo se hace uso del algoritmo SURF (Speeded Up Robust Features) quien extrae diversas características del rostro las cuales se procesan para determinar si las imágenes coinciden (autenticación exitosa) o no (autenticación errónea).

1.2. Justificación

En los últimos años se han desarrollado diversos trabajos como los presentados por (Mukherjee *et al*., 2008), (Pabbaraju *et al*., 2009), (Junered, 2010), (Kremić y Subaşi, 2011), (Ren *et al*., 2013) y (Zhuang, 2013), que resaltan la importancia y la aplicación de la autenticación y el reconocimiento facial, así mismo presentan la implementación de algún algoritmo en particular para la detección de características de los rostros con las cuales se determina la autenticidad y/o reconocimiento de una persona.

En base a estos trabajos realizados, se da la oportunidad de desarrollar nuevas y mejores aplicaciones empleando diversos algoritmos de extracción de características como LDA (Kumar y Kaur, 2012), PCA (Izenman, 2008), SIFT (Lowe, 2004), SURF (Bay *et al., 2006*), entre otros.

Por esta razón y con la finalidad de contar con una aplicación más eficiente y robusta es que se plantea el uso del pre-procesamiento de imágenes así como del algoritmo SURF dentro de la etapa de extracción de características del proceso general de autenticación facial.

1.3. Hipótesis

Es factible desarrollar e implementar el algoritmo SURF dentro del proceso de autenticación facial en un dispositivo móvil Android como una aplicación eficaz y robusta.

1.4. Objetivo general

Desarrollar un sistema de autenticación facial basado en el algoritmo SURF (Speeded Up Robust Features) e implementarlo en dispositivo móvil con sistema operativo Android.

1.5. Objetivos específicos

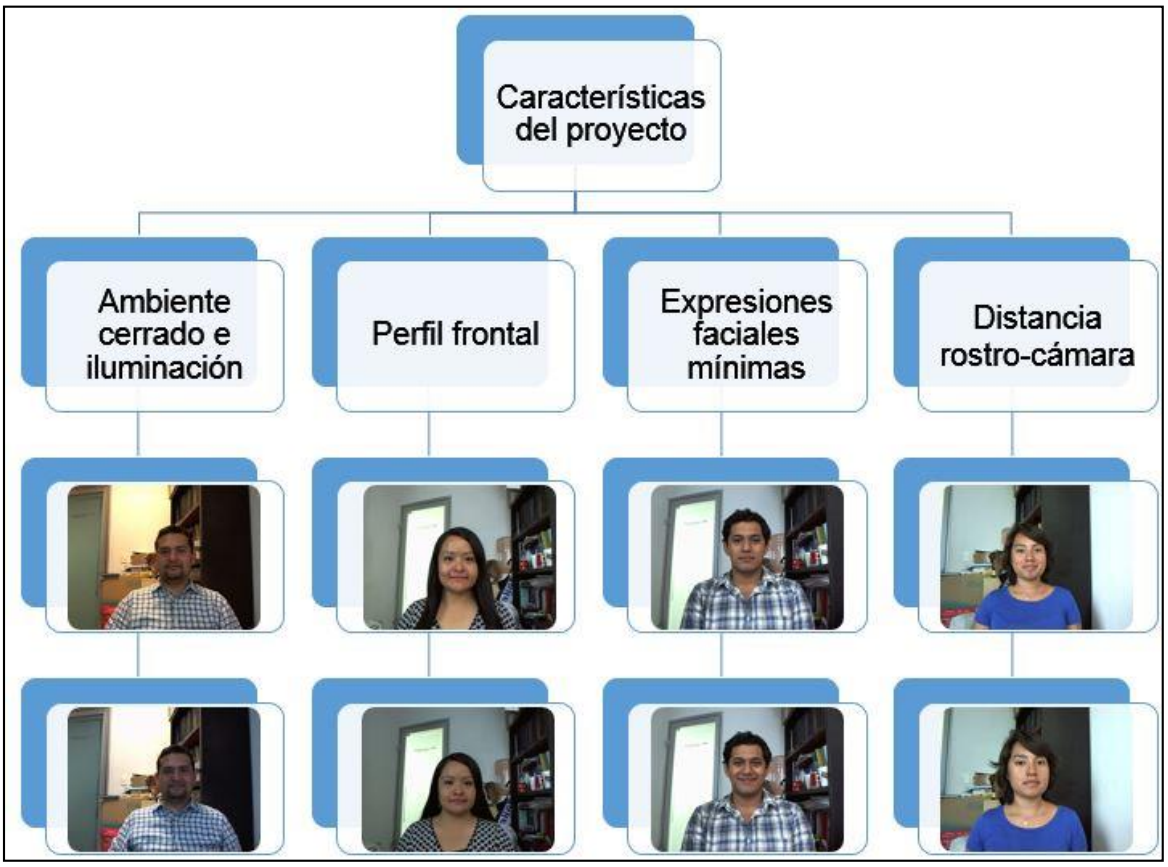
- Adquirir imágenes del rostro de una persona, las cuales se tomarán en un ambiente cerrado, con perfil frontal a la cámara, bajo diferentes condiciones de iluminación, expresiones faciales mínimas y diversas distancias entre el rostro y la cámara.
- Crear y nombrar una base de datos de rostros que contenga las imágenes capturadas.
- Desarrollar una fase de preprocesamiento de imágenes.
- Emplear el algoritmo SURF dentro el proceso de extracción de características de la autenticación facial.
- Implementar la fase de preprocesamiento y el algoritmo SURF en el sistema operativo Android.
- Realizar pruebas de autenticación facial en el dispositivo móvil.
- Analizar y documentar los resultados obtenidos.

1.6. Alcances y limitaciones

Dentro de los alcances y limitaciones de este trabajo se encuentran el uso de dispositivos móviles (Smartphone y Tablet) con sistema operativo Android versiones 4.0.3, 4.1.2, 4.2.2, 4.4.2 y 5.1.1.

Para la adquisición de imágenes de prueba del rostro se consideró un ambiente cerrado (oficina), bajo diferentes condiciones controladas de iluminación, el rostro con perfil frontal a la cámara y expresiones faciales mínimas (neutral, sonriente, etc.), además de considerar diferentes distancias entre el rostro y la cámara. Estas características se pueden apreciar en la Figura 1-1.

Figura 1-1 Características de entrenamiento y prueba del proyecto.



Así mismo, los resultados generales que se pretenden con el proyecto de investigación son los siguientes:

- Contribuir al desarrollo de un sistema de seguridad robusto para dispositivo móvil basado en autenticación facial.
- Aumentar a más del 80% (Gui, 2013) el porcentaje de resultados correctos positivos del sistema de autenticación facial.

- Comparar el porcentaje de resultados correctos positivos que se obtuvieron del sistema de autenticación facial contra el porcentaje obtenido en otros métodos existentes con el fin de ampliar la confiabilidad de los sistemas de autenticación biométrica en dispositivos móviles.
- Publicar los resultados obtenidos del sistema de autenticación facial.

Finalmente, la participación en el proyecto de investigación:

- Adquirir varias imágenes del rostro de una persona.
- Desarrollar el sistema de autenticación facial empleando el algoritmo SURF.
- Implementar el sistema de autenticación facial en Smartphone y Tablet que cuenten con el sistema operativo Android.
- Realizar pruebas del sistema de autenticación facial en cada dispositivo móvil.
- Analizar las pruebas y llevar a cabo una retroalimentación en el sistema de autenticación facial.
- Validar los resultados obtenidos del sistema de autenticación facial con algún otro sistema existente.
- Documentar los resultados obtenidos.
- Publicar un artículo en extenso en un congreso internacional arbitrado y/o revista arbitrada.

1.7. Organización de la tesis

La tesis se encuentra organizada en 6 capítulos y 5 anexos los cuales presentan las actividades realizadas en conjunto con el proyecto de investigación, a continuación se describen cada uno de ellos de manera general.

Capítulo 1: Presenta la definición del proyecto de investigación, justificación, hipótesis, objetivo general, objetivos específicos, alcances, limitaciones y la organización de la tesis.

Capítulo 2: Introduce al lector al estado del arte de la investigación donde se abordan temas como los antecedentes del reconocimiento y autenticación facial, procesamiento y filtrado de imágenes, finalmente algunas aplicaciones y sistemas comerciales relacionados con el tema de tesis que aquí se presenta.

Capítulo 3: Explica de forma detallada el algoritmo SURF, qué es y en qué consiste, así como su relación con el proyecto de investigación.

Capítulo 4: Describe la metodología propuesta para la autenticación facial de usuarios la cual incluye una fase de preprocesamiento de imágenes y la aplicación del algoritmo SURF.

Capítulo 5: Muestra los resultados obtenidos al implementar la metodología explicada en el capítulo 4. Además, se incluye el software y hardware empleados en las diferentes pruebas las cuales fueron realizadas en una computadora portátil, tarjetas de desarrollo Raspberry Pi, Smartphones y Tablets. Finalmente, se presenta un análisis sobre el tiempo de procesamiento de esta metodología en los diferentes dispositivos móviles.

Capítulo 6: Define las conclusiones del proyecto de investigación en base a las pruebas realizadas en el capítulo 5 y establece su trabajo a futuro.

Referencias: Detalla las referencias que fueron consultadas a lo largo del proceso de investigación y desarrollo de este proyecto.

Anexos: Muestra las actividades realizadas por el autor de este trabajo, las cuales fueron llevadas a cabo a lo largo del desarrollo de este proyecto de investigación.

Anexo I: Presenta la configuración de una webcam en el Sistema operativo Raspbian, la instalación de fswebcam y algunos ejemplos de captura de imágenes.

Anexo II: Despliega la selección de un dispositivo móvil realizada en Eclipse.

Anexo III: Lista de artículos escritos como autor y coautor durante el proyecto de investigación.

Anexo IV: Participación del autor de este proyecto de investigación como ponente en el 13TH Mexican International Conference on Artificial Intelligence MICAI 2014 (Congreso Internacional Mexicano de Inteligencia Artificial).

Anexo V: Actividades complementarias realizadas por el autor durante el desarrollo de este proyecto de investigación, las cuales incluyen:

- Participación como coautor de un artículo presentado en el congreso internacional CCE 2014 (International Conference on Electrical Engineering, Computing Science and Automatic Control).
- Realización de una estancia de investigación en la Universidad Autónoma de Baja California, campus Mexicali, como instructor del curso “Procesamiento de imágenes y Reconocimiento de objetos”.
- Colaboración como miembro del comité organizador en el 13er Congreso Nacional de Mecatrónica 2014.
- Participación en el “Curso de entrenamiento de digitalización 3D VISI Series”.
- Obtención de una certificación Microsoft en el tema “Software Development Fundamentals”.

2. ESTADO DEL ARTE

2.1. Antecedentes del reconocimiento y autenticación facial

Avances en el campo de la tecnología de la información han creado un fuerte vínculo entre ésta y la seguridad de la información, la cual hace referencia a la garantía de la confidencialidad, integridad y disponibilidad de la información. Existen muchas herramientas y técnicas que pueden apoyar la gestión de la seguridad de la información, entre ellas la biometría (Bhattacharyya *et al*., 2009).

La biometría se refiere a la identificación de una persona en base a sus características físicas y de comportamiento. Además, incluye el estudio de los métodos para reconocer únicamente los seres humanos basados en uno o más rasgos físicos. 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. (Brumnik *et al*., 2011). Así mismo, es usada para muchos propósitos, tales como la detección de criminales, identificación, el control de acceso, entre otros (Duc y Minh, 2009). Cabe señalar que la biometría se puede dividir en dos clases principales:

1) Biometría fisiológica: está relacionada con la forma del cuerpo:

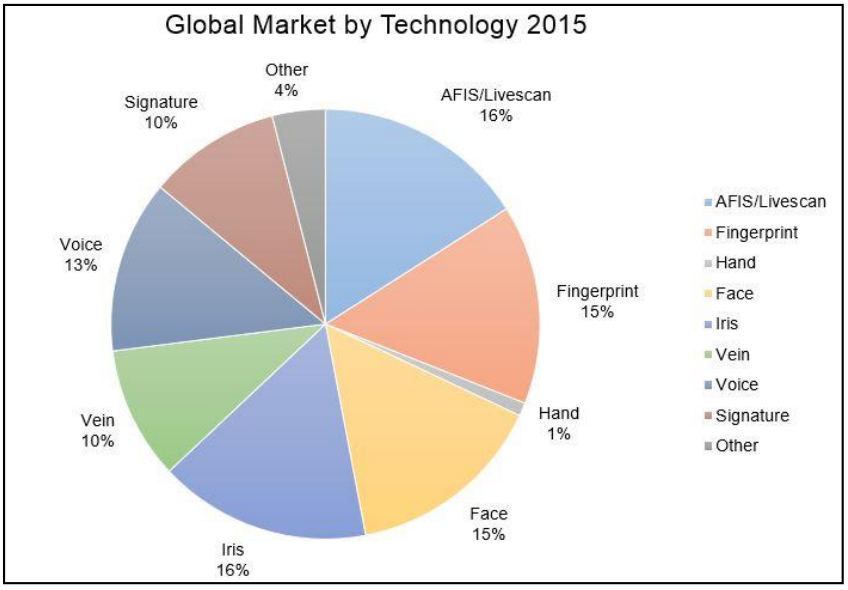
    - Reconocimiento facial.
    - Huella digital.
    - Escaneo del iris.
    - Escaneo de la mano.

2) Biometría del comportamiento: está relacionada con el comportamiento de una persona:

    - Escaneo de la voz.
    - Escaneo de la firma.
    - Pulsación de teclas

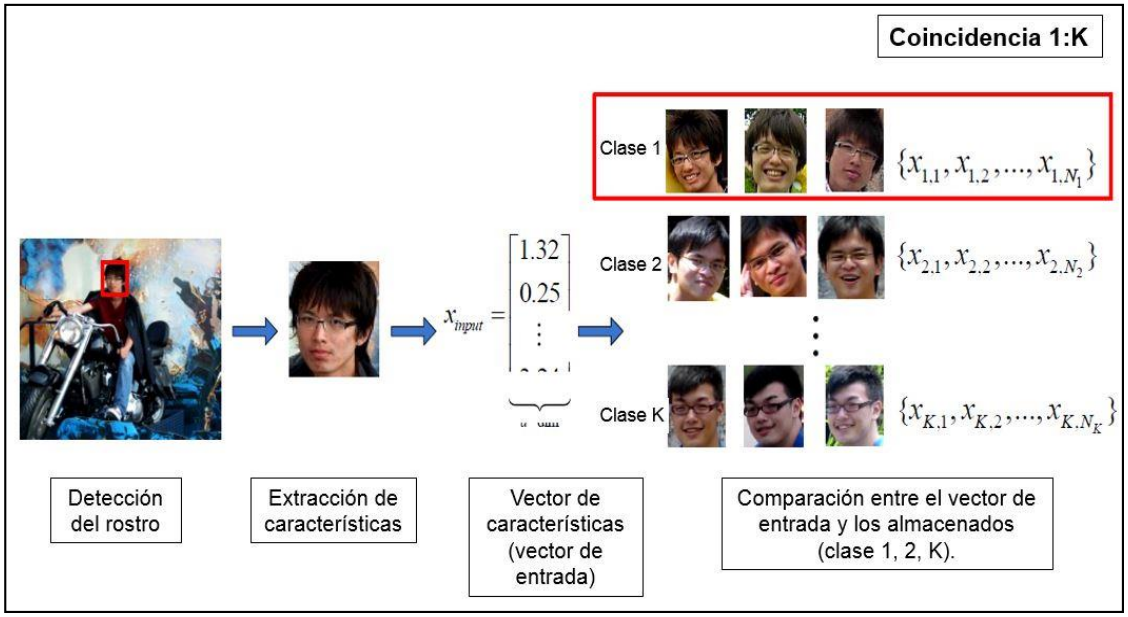
Considerando las dos clases de biometría antes mencionadas, la Figura 2-1 presenta los rasgos biométricos más populares en el mercado proyectados para el año 2015 (Maxine, 2007).

Figura 2-1 Rasgos biométricos más populares en el mercado (Maxine, 2007).



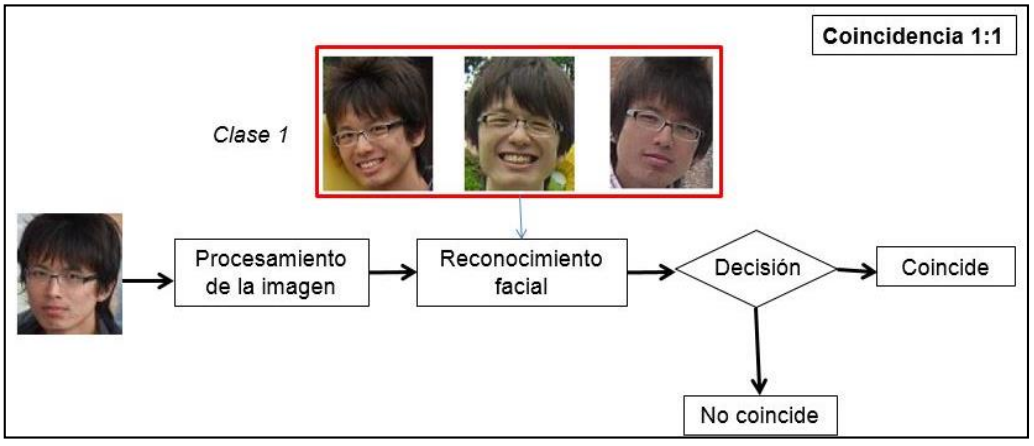
Como una de las aplicaciones más exitosas dentro de la biometría fisiológica destaca el reconocimiento facial, el cual ha recibido mucha atención durante los últimos años. El reconocimiento de rostros humanos sigue atrayendo a investigadores de disciplinas tales como el procesamiento de imágenes, reconocimiento de patrones, redes neuronales, la visión por computadora y la psicología. 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, la Figura 2-2 muestra un ejemplo de cómo estos pasos funcionan en una imagen de entrada (Chao, 2010).

Figura 2-2 Reconocimiento o Identificación facial (Chao, 2010).



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 2-3).

Figura 2-3 Autenticación o verificación facial.



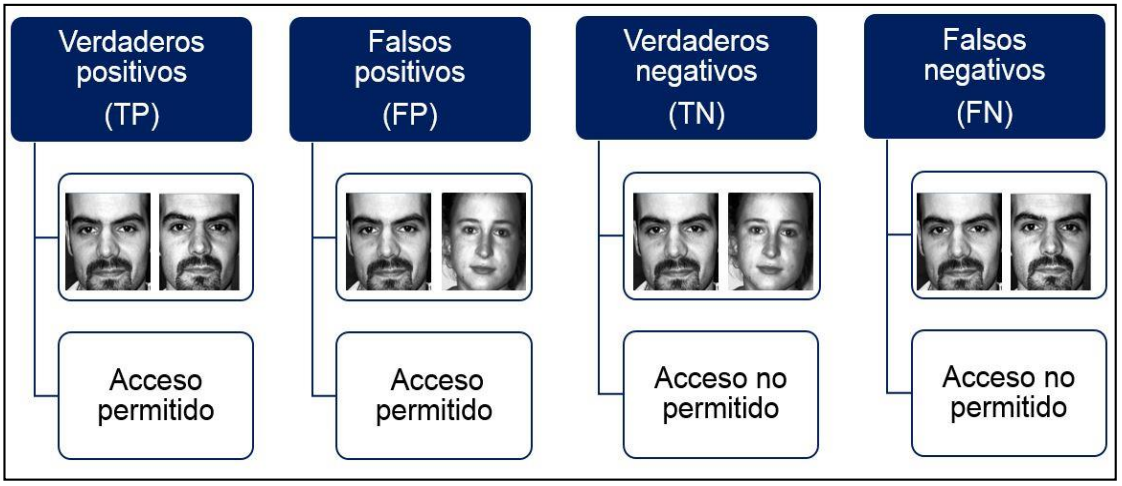
A pesar de las divisiones de mecanismos de reconocimiento y autenticación que existen, todos ellos siguen un proceso bastante general (Iglesias, 2007):

1) El usuario pide acceso a un recurso (por ejemplo a un dispositivo móvil).
2) El sistema le solicita al usuario su medio de autenticación (rostro, iris, etc.).
3) El usuario entrega sus credenciales (características) de autenticación.
4) El sistema verifica las credenciales del usuario.
5) El sistema niega o proporciona al usuario el acceso al recurso.

Una vez concluido este proceso el siguiente paso es llevar a cabo la evaluación general del sistema para medir su desempeño, por lo cual diversos autores como (Yin *et al.*, 2011), (Ruiz *et al.*, 2013), (Valstar *et al.*, 2015), entre otros, toman en cuenta los siguientes parámetros (ver Figura 2-4):

- Verdaderos positivos (True positive, TP): El sistema reconoce las credenciales de un usuario conocido (los datos del usuario se encuentran almacenados en una base de datos) y le permite el acceso a un recurso o dispositivo.
- Falsos positivos (False positive, FP): El sistema reconoce las credenciales de un usuario no conocido (los datos del usuario no se encuentran almacenados en una base de datos) y le permite el acceso a un recurso o dispositivo.
- Verdaderos negativos (True negative, TN): El sistema no reconoce las credenciales de un usuario no conocido (los datos del usuario no se encuentran almacenados en una base de datos) y no permite el acceso a un recurso o dispositivo.
- Falsos negativos (False negative, FN): El sistema no reconoce las credenciales de un usuario conocido (los datos del usuario se encuentran almacenados en una base de datos) y no le permite el acceso a un recurso o dispositivo.

Figura 2-4. Verdaderos y Falsos positivos así como los Verdaderos y Falsos negativos.



Durante la última década se han propuesto diversos algoritmos de autenticación y reconocimiento facial, los más usados en este campo son LDA, PCA, SIFT y SURF, sin embargo las principales limitantes de los sistemas que usan estos algoritmos es su dependencia a las condiciones de iluminación, posición, forma y tamaño del rostro (Mendoza-Martinez *et al*., 2014). A continuación se presenta una breve descripción de cada uno de ellos.

LDA (Linear Discriminant Analysis).

Es un algoritmo bien conocido para la extracción de características y la reducción de dimensión (Kumar y Kaur, 2012). Se utiliza para reducir el número de características a un número más manejable y construir un subespacio discriminante para el reconocimiento de la identidad del rostro (Lu, 2003).

PCA (Principal Component Analysis).

Empleado para la selección de características y la reducción de la dimensión de la imagen. Se basa en la descomposición de imágenes del rostro en un pequeño conjunto de características de imágenes llamada “Eigenfaces”, la cual es fiel a las imágenes originales, su tasa de reconocimiento disminuye el reconocimiento ante variaciones de pose e iluminación (Kumar y Kaur, 2012).

SIFT (Scale Invariant Feature Transform).

Transforma una imagen en una gran colección de vectores de características locales, cada uno de los cuales es invariante a la translación de la imagen, la escala y la rotación, y parcialmente es invariante a cambios en la iluminación (Lowe, 2004).

SURF (Speeded Up Robust Features).

Es un detector de puntos de interés y descriptor robusto, que se enfoca en la extracción de características de una imagen. SURF es invariante a la rotación, escala, brillo y después de que se realiza la reducción de la imagen a la unidad de longitud, es invariante al contraste (Bay *et al.*, 2006).

En este contexto y ligado a los algoritmos presentados, el reconocimiento facial es una de las aplicaciones más relevantes dentro del análisis de imágenes (Marqués, 2010) que ha sido estudiado mediante la aplicación del algoritmo SIFT (descrito previamente), el cual es uno de los métodos más importantes desde su desarrollo en 2004 (Lowe, 2004).

Sin embargo, con el continuo desarrollo de nuevas metodologías para el campo del reconocimiento facial, en 2006 se introdujo un nuevo algoritmo llamado SURF (Bay *et al.*, 2006), que ha empezado a atraer la atención de los expertos en el área de la autenticación y el reconocimiento facial, los cuales han realizado diversos estudios computacionales empleando este algoritmo.

Así mismo, avances recientes han abierto la posibilidad a las computadoras para competir con la capacidad humana de reconocer una cara en cualquier condición natural ya que casi siempre han sido capaces de memorizar más caras de lo humanamente posible. Partiendo de esta idea surge un concepto relativamente nuevo y se trata del dispositivo móvil (Junered, 2010).

Tan solo en un estudio realizado por Gartner en Octubre del 2014 se muestra una proyección del crecimiento en el número de dispositivos vendidos alrededor del mundo entre el 2013 y el 2015 (Gartner, 2014), donde los principales son los teléfonos móviles y las tabletas, estos resultados se pueden apreciar más claramente en la Figura 2-5.

Figura 2-5 Número de dispositivos vendidos alrededor del mundo (Gartner, 2014).

Worldwide Device Shipments by Segment (Thousands of Units)

Device Type	**2013**	**2014**	**2015**
Traditional PCs (Desk-Based and Notebook)	296,131	276,457	261,005
Ultramobile Premium	21,517	37,608	64,373
PC Market Total	**317,648**	**314,065**	**325,378**
Tablets	207,082	229,085	272,904
Mobile Phones	1,806,964	1,859,946	1,928,169
Other Hybrids/Clamshells	2,706	6,462	8,609
Total	**2,334,400**	**2,409,558**	**2,535,060**

Source: Gartner (October 2014)

Por otro lado, la proyección de dispositivos vendidos alrededor del mundo en base a su sistema operativo se muestra en la Figura 2-6, donde se puede observar que el líder de todos ellos es Android.

Figura 2-6 Proyección de los dispositivos vendidos alrededor del mundo en base a su sistema operativo (Gartner, 2014).

Worldwide Device Shipments by Operating System in Emerging Markets (Thousands of Units)

Operating System	**2013**	**2014**	**2015**
Android	632,517	928,135	1,117,860
Windows	187,474	194,091	221,804
IOS/Mac OS	78,928	95,304	112,647
Others	772,562	520,605	383,914
Total	**1,671,480**	**1,738,135**	**1,836,225**

Shipments include mobile phones, ultramobiles (including tablets) and PCs

Source: Gartner (October 2014)

En base a este estudio se puede apreciar una estimación del número de dispositivos existentes alrededor del mundo y cuál es el sistema operativo que sobresale entre ellos, esta es información muy valiosa ya que permite saber cuáles son los dispositivos más comunes entre la población y cuál es el sistema operativo más demandado en el mercado, lo que da pie a desarrollar un sinfín de aplicaciones para cada uno de ellos.

En este contexto cabe señalar que la autenticación facial está ganando terreno para identificarse en dispositivos que incorporen una cámara digital. Además, esta técnica en concreto no requiere la colaboración por parte del individuo y se produce en tiempo real por lo cual se puede decir que el uso de sistemas biométricos libera al usuario del uso de elementos externos auxiliares (Travieso *et al*., 2011).

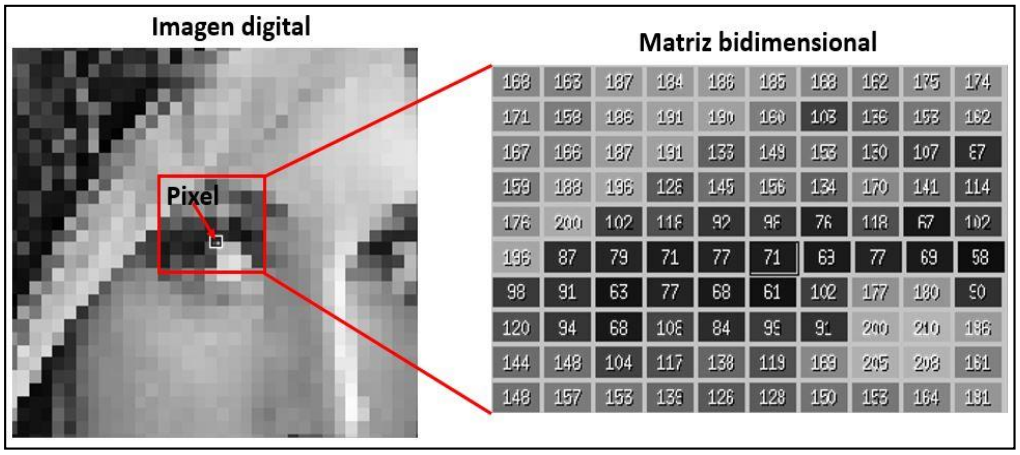
De esta manera se proporciona un nivel más alto de seguridad ya que los parámetros utilizados son unívoca "firma" de una característica humana que no puede ser fácilmente adivinada o descifrada.

Así mismo, es altamente notable la estrecha relación que existe entre los algoritmos tanto de reconocimiento como autenticación facial y su implementación en dispositivos móviles. Prueba de ello son los trabajos que se han llevado a cabo y que resaltan el desarrollo de diferentes sistemas de reconocimiento y autenticación facial, por ejemplo los realizados por (Bigun *et al*.., 2005), (Abeni *et al*., 2006), (Hadid *et al*., 2007), (Boehm *et al*., 2008), (Fong y Seng, 2009), (Tao *et al*., 2010), (Kremić y Subaşi., 2011), (Ren *et al*., 2013), (Zhuang, 2013) y (Chen *et al*., 2014), estos han sido posibles gracias a la continua investigación y desarrollo de nuevos algoritmos que permiten hacer más eficiente la autenticación, así como al avance de la tecnología móvil ya que hoy en día es posible fusionar ambos elementos de tal manera que puedan servir para muchas aplicaciones de seguridad, vigilancia, control de acceso, etc.

2.2. Preprocesamiento de imágenes

Una imagen digital se compone de una agrupación de píxeles, el cual es el menor de los elementos de una imagen con un valor de intensidad o brillo asociado. Esta imagen digital se representa mediante una matriz bidimensional, de forma que cada elemento de la matriz se corresponde con cada píxel en la imagen (Gámez, 2009), tal y como se puede observar en la Figura 2-7.

Figura 2-7 Representación de una imagen digital (Falcao, 2003).



Por lo tanto, el objetivo del preprocesamiento de imágenes es mejorar la calidad de las imágenes para su posterior utilización o interpretación (Florencia, 2004). Existen tres niveles de procesamiento: bajo, medio y alto. En el nivel bajo se hacen sólo operaciones primitivas de procesamiento para reducir ruido o mejorar contraste y brillo. En este caso la entrada es una imagen y la salida sigue siendo una imagen. En el nivel medio, los procesos incluyen tareas como la segmentación y la clasificación, por ejemplo reconocer objetos. En este segundo caso la entrada del proceso es una imagen pero la salida son generalmente algunos atributos extraídos de aquellas imágenes tales como limites, contornos o esquinas. Por último, el nivel alto se refiere a los procesos que incluyen “entender” los resultados obtenidos (interpretados) para luego aplicarles operaciones similares a las que realiza la visión humana (Jiménez, 2009).

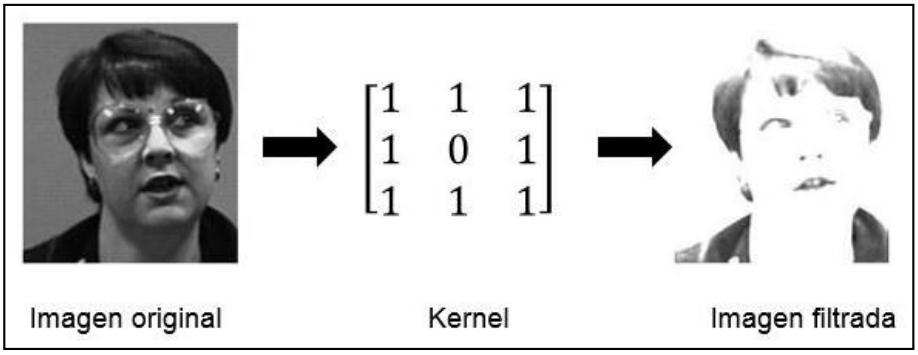
En la mayoría de los casos el preprocesamiento de imágenes se aplica directamente sobre imágenes en escala de grises, debido al bajo consumo de cómputo de éste. Así mismo, la mayoría de métodos matemáticos deterministas que se utilizan en su procesamiento, están basados en la diferencia de niveles de grises, por lo que no existen muchos métodos para el preprocesamiento de imágenes en color, aun cuando estos pueden ser utilizados en este tipo de formato de imagen (Florencia, 2004).

2.3. Filtrado de imágenes

Los filtros se utilizan para la modificación de imágenes ya sea para detectar los bordes de una escena o para modificar el aspecto, otra función de los filtros es para la eliminación de ruido de la imagen. Como se explica en (Gámez, 2009), existen diferentes tipos de filtros como el espacial, en frecuencia, morfológico y de textura.

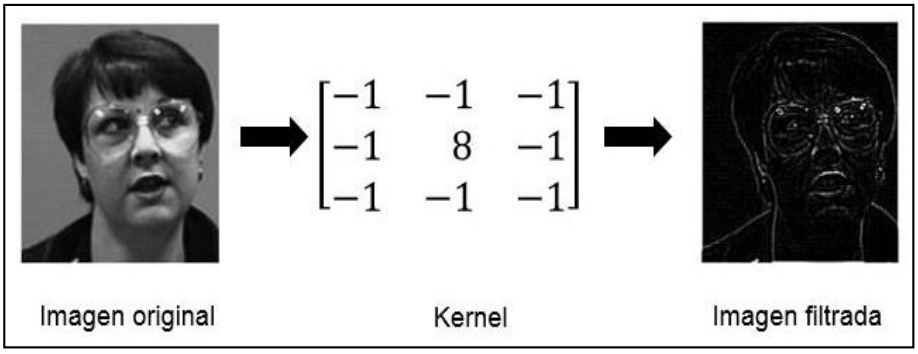
El filtrado espacial es la operación que se aplica a las imágenes para mejorar o suprimir detalles espaciales con el fin de mejorar la interpretación visual. Ejemplos comunes incluyen aplicar filtros para mejorar los detalles de bordes en imágenes, o para reducir o eliminar patrones de ruido. El filtrado espacial es una operación "local" en procesamiento de imagen en el sentido de que modifica el valor de cada píxel de acuerdo con los valores de los píxeles que lo rodean, se trata de transformar valores de grises originales de tal forma que se parezcan o diferencien más de los correspondientes a los píxeles cercanos. Los filtros espaciales se pueden dividir en tres categorías: filtros de paso bajo, paso alto y detectores de bordes. En primer lugar, los filtros de paso bajo enfatizan las bajas frecuencias, suavizando las imágenes y suprimiendo ruidos. Se trata de asemejar los valores de grises originales de cada píxel al de los píxeles vecinos, reduciendo la variabilidad espacial de la imagen, lo cual produce que se desvanezcan los bordes, perdiéndose nitidez visual de la imagen, pero ganando homogeneidad. Un ejemplo de filtro paso bajo se muestra en la Figura 2-8.

Figura 2-8 Filtro de paso bajo con su respectivo Kernel empleado (Gámez, 2009).



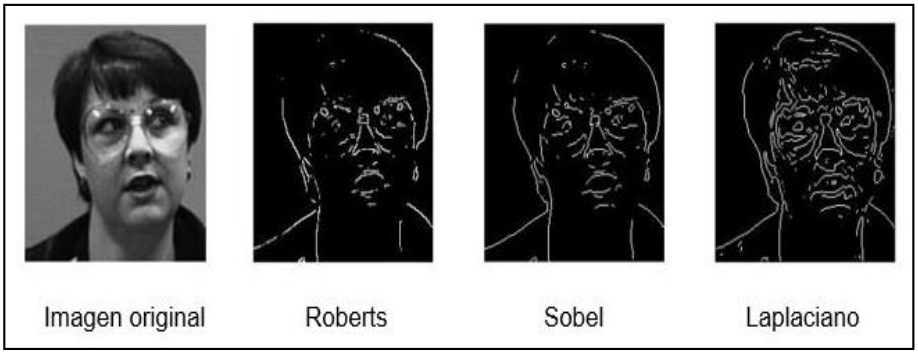
En segundo lugar se tienen los filtros de paso alto, los cuales enfatizan las altas frecuencias, para mejorar o afilar las características lineales como carreteras, fallas, o límites en general. Realizan por tanto el efecto contrario a los filtros pasa-bajos, eliminando estos las bajas frecuencias. En la Figura 2-9 aprecia la aplicación del filtro paso alto en una imagen.

Figura 2-9 Filtro de paso alto con su respectivo Kernel empleado (Gámez, 2009).



En tercer lugar se encuentran los filtros detectores de bordes, Realizan otro tipo de operaciones con los datos, pero siempre con el resultado de enfatizar los bordes que rodean a un objeto en una imagen, para hacerlo más fácil de analizar. Estos filtros típicamente crean una imagen con fondo gris y líneas blancas y negras rodeando los bordes de los objetos y características de la imagen. En esta categoría se encuentran el filtro Roberts, Sobel y Laplaciano, entre otros, como se muestra en la Figura 2-10.

Figura 2-10 Filtros detectores de bordes: Roberts, Sobel y Laplaciano (Gámez, 2009).



Además del filtrado espacial, se tienen otros tipos de filtrado como en frecuencia, esto quiere decir que en el dominio frecuencial también puede realizarse el proceso de filtrado, con mayor grado de comprensión de lo que se está viendo, ya que en una imagen en el dominio frecuencial se sabe dónde se encuentran los distintos rangos de frecuencias. Los resultados que se obtienen son muy parecidos a los que se obtienen con el filtrado espacial (convolución) pero en este caso se trabaja con otras variables y conceptos diferentes.

Otro tipo de filtrado es el morfológico, donde se emplea la morfología matemática la cual es un método no lineal para procesar imágenes digitales basándose en la forma. Su principal objetivo es la cuantificación de estructuras geométricas. Aquí los filtros también vienen definidos por su Kernel, pero no es un Kernel de convolución sino un elemento estructurante. Dentro de los filtros morfológicos destacan la dilatación, erosión, así como la apertura y cierre.

La dilatación, es comúnmente conocida como relleno, expansión o crecimiento. Puede ser usado para rellenar huecos de tamaño igual o menor que el elemento estructurante con la que se opera la dilatación. La dilatación de una imagen se aprecia en la Figura 2-11.

Figura 2-11 Dilatación de una imagen (Gámez, 2009).

Por otro lado, la erosión es lo opuesto a la dilatación, realiza con el fondo lo que la dilatación al primer plano. También en este caso, existe un elemento estructurante que se utiliza para operar con la imagen. Los efectos son de encogimiento, contracción o reducción, así como se muestra en la Figura 2-12.

Figura 2-12 Erosión de una imagen (Gámez, 2009).

Al resultado de aplicar iterativamente dilataciones y erosiones o viceversa, se le conoce como apertura y cierre de una imagen, donde su objetivo es la eliminación del detalle específico en la imagen menor que el elemento estructurante, sin la distorsión geométrica global de características no suprimidas. Por ejemplo, si en una imagen se aplica primero el proceso de erosión seguido de una dilatación, a esto se le conoce como apertura de una imagen con la cual se suavizan sus contornos y se eliminan pequeños picos.

Por el contrario, si se aplica primero el proceso de dilatación seguido de una erosión, a esto se le conoce como cierre de una imagen con la cual se eliminan pequeños agujeros y se rellenan brechas en los contornos de la imagen. La Figura 2-13 muestra la apertura y cierre de una imagen.

Figura 2-13 Apertura y cierre de una imagen (Gámez, 2009).

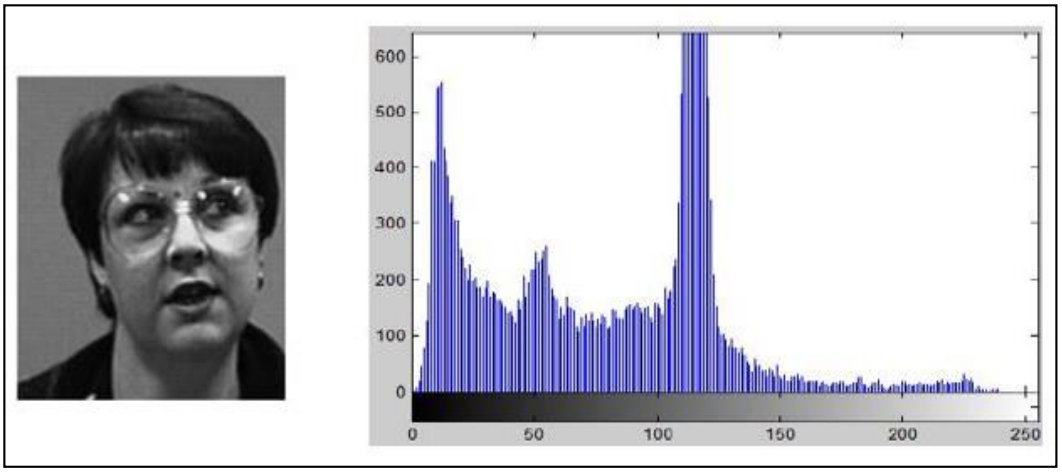
Otro tipo de filtro es el de textura. Muchas imágenes contienen regiones caracterizadas por variaciones del nivel de gris, más que por un valor único de grises. La textura se refiere precisamente a la variación espacial del nivel de gris de una imagen como función de escala espacial. Para que los píxeles de una determinada área puedan ser definidos como texturalmente diferentes, sus niveles de gris deben ser más homogéneos como unidad que áreas de diferente textura.

Además de cada uno de los filtros presentados anteriormente, existen otras técnicas para modificar una imagen, por ejemplo las técnicas de modificación del histograma. Estas técnicas van principalmente enfocadas a mejorar la visualización de una imagen.

El histograma de una imagen es un gráfico que ofrece una descripción global de la apariencia de la imagen. En el eje de abscisas se representa el rango de valores de píxeles de la imagen, mientras que en el eje de ordenadas se representa el rango de valores que pueden tomar esos píxeles.

La expansión del contraste es una de estas técnicas. Consiste en que, dado un rango de valores de grises (NDmax - NDmin) menor que el rango disponible por el dispositivo de visualización (NVmax – Nvmin), se está perdiendo contraste (entendido éste como relación entre los valores máximo y mínimo de una imagen). En la Figura 2-14 se presenta el histograma de una imagen.

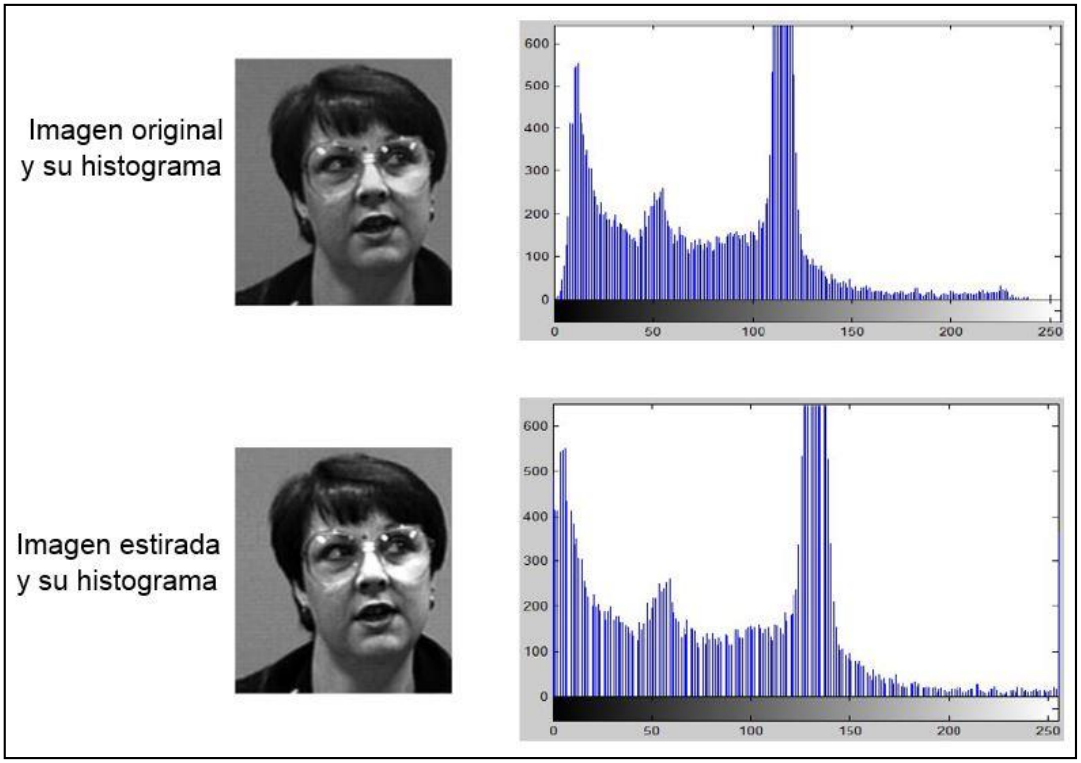
Figura 2-14 Histograma de una imagen (Gámez, 2009).



Visualmente es claro el efecto, al observar que no existe mucha diferencia entre los tonos más claros y más oscuros. Mediante distintas operaciones matemáticas se pueden transformar esos valores de grises en otros con un rango mayor que se adapte plenamente a la capacidad del dispositivo de visualización como el estiramiento lineal o la ecualización del histograma.

Por su parte, el estiramiento lineal es la forma más sencilla de efectuar el contraste. Consiste en buscar una función lineal que ajuste de forma que el rango NDmin a NDmax se transforme en NVmin a NVmax, por lo tanto NDmax = NVmax y NDmin = NVmin. El resto de valores ND (valores de los niveles de grises) serán transformados en otros según esa transformación lineal. La Figura 2-15 se muestra el estiramiento lineal de una imagen.

Figura 2-15 Estiramiento lineal (Gámez, 2009).



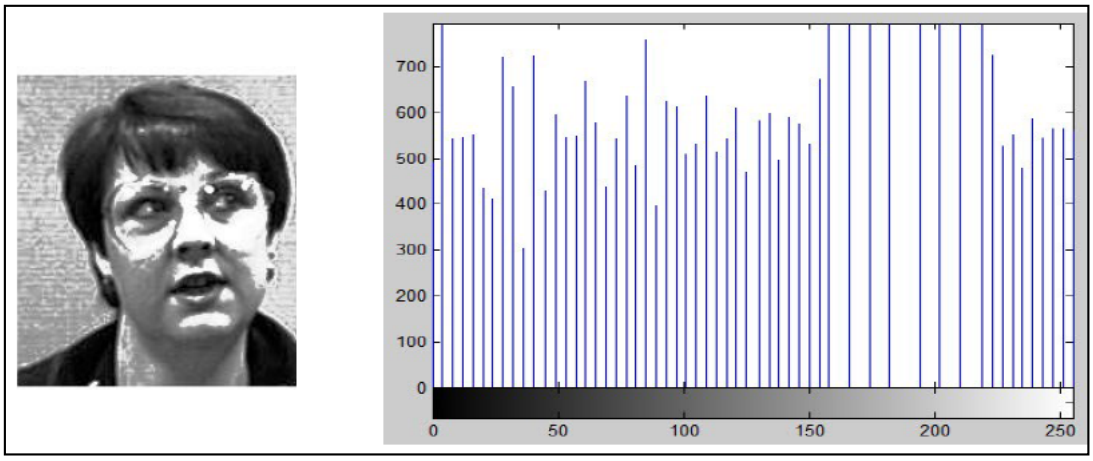
En este ejemplo se puede ver como en el histograma de la imagen estirada hay píxeles en todo el rango de la tabla de escala de grises, mientras que en el histograma de la imagen original no se cubre todo el rango.

Como caso particular de la transformación lineal, cabe destacar la transformación lineal por trozos, que aplica esta misma fórmula no a todo el rango de ND sino a un subrango determinado que se quiera enfatizar especialmente, incluso se pueden aplicar diferentes estiramientos lineales, con diferentes coeficientes a distintos rangos de ND del histograma.

Otra técnica de transformación es la ecualización del histograma. Como el estiramiento lineal sólo tiene en cuenta como parámetros los valores máximo y mínimo del histograma original, emplear una técnica más depurada puede considerar también la forma de la distribución de frecuencias.

Así, el NV (valores de los niveles de grises disponibles por el dispositivo de visualización) de cada ND está en proporción no sólo a su valor sino también a su frecuencia, esto es, al número de píxeles con ese determinado valor. Aquellos ND con mayor número de píxeles serán los que proporcionalmente ocupen un mayor rango de visualización. En la Figura 2-16 se observa la ecualización del histograma de una imagen.

Figura 2-16 Ecualización del histograma de una imagen (Gámez, 2009).



Obsérvese cómo los valores de los píxeles se intentan distribuir de forma uniforme en todo el rango 0-255. Como no es posible separar un valor cualquiera en dos diferentes, donde hay relativamente gran número de píxeles se separa del resto en proporción del número de píxeles de ese valor, por lo tanto el resultado visual es mucho más disperso.

La ecualización del histograma genera una imagen cuyos niveles de intensidad son igualmente probables y, además, cubren el rango [0,1]. El resultado neto de este proceso es una imagen cuyo rango dinámico ha sido incrementado, que tenderá a poseer un mayor contraste (González y Woods, 2002). Esta transformación se representa en la ecuación 2.1.

$$T(r_k) = \sum_{j=1}^{k} p_r(r_j) = \sum_{j=1}^{k} \frac{n_j}{n} \qquad (2.1)$$

Donde:

k es el número de niveles de gris.

p_r es la probabilidad de in cierto nivel de gris.

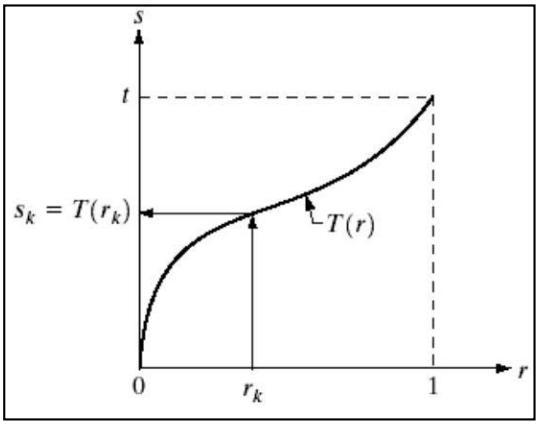
r_j es un nivel de gris “j” especifico.

n_j es el número de pixeles con un nivel “j”.

n es el total de pixeles.

La Figura 2-17 muestra la representación gráfica de la transformación $T(r_k)$ realizada.

Figura 2-17 Transformación $T(r_k)$.



2.4. Aplicaciones

Existen numerosas áreas de aplicación del reconocimiento y autenticación facial las cuales van desde gubernamentales hasta comerciales, a continuación se describirán algunas de ellas (Jafri y Arabnia, 2009).

Seguridad: control de acceso a edificios, aeropuertos, puertos marítimos, cajeros automáticos, control fronterizo, computadoras (Figura 2-18), seguridad de la red y autenticación de correo electrónico en estaciones de trabajo multimedia.

Figura 2-18 Control de acceso facial en una computadora (Luxand, 2015).

Vigilancia: un gran número de circuitos cerrados de televisión pueden ser monitoreados en busca de delincuentes conocidos, traficantes de drogas, etc., y las autoridades pueden ser notificadas cuando alguno se encuentre (Figura 2-19).

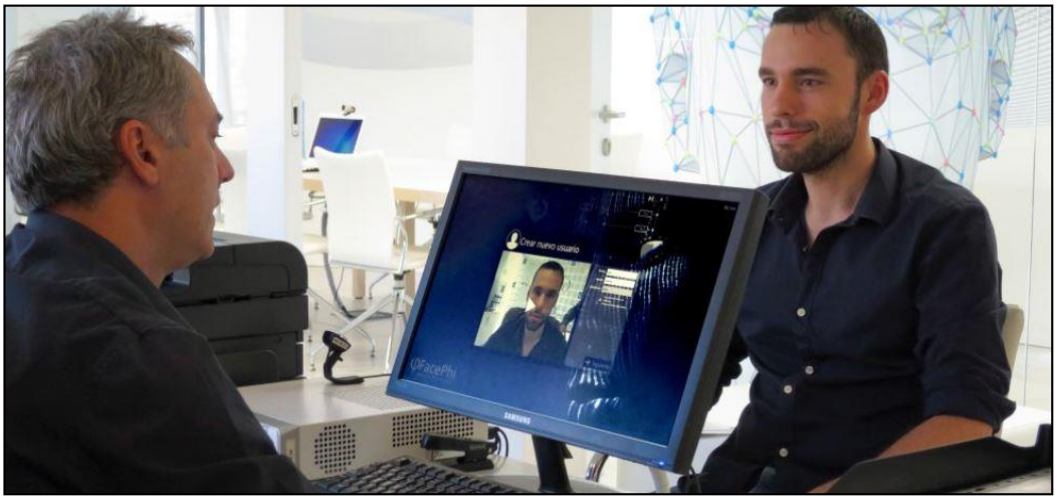
Figura 2-19 Vigilancia de circuitos cerrados (Rivera, 2013).

Verificación general de la identidad: por ejemplo en el registro electoral, la banca, comercio electrónico, identificación de recién nacidos, documentos nacionales de identidad, pasaportes, licencias de conducir y el número de un empleado (Figura 2-20).

Figura 2-20 Verificación de la identidad de un empleado (CareerDiva, 2009).

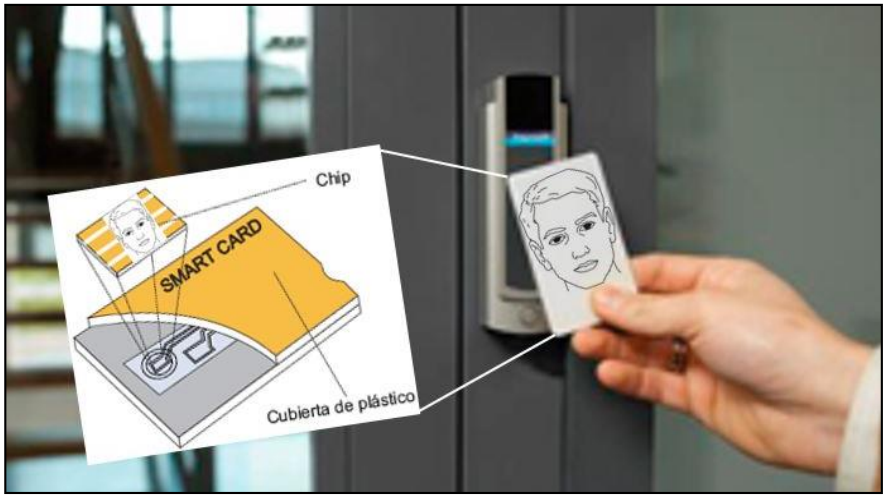
Investigaciones de base de datos de imágenes: búsqueda de bases de datos de imágenes de los conductores con licencia (Figura 2-21), beneficiarios de prestaciones, niños desaparecidos e inmigrantes.

Figura 2-21 Bases de datos de imágenes de los conductores con licencia (Sainz, 2014).



Tarjetas inteligentes (Smart Card): en lugar de mantener una base de datos de imágenes de la cara, la impresión de una cara puede ser almacenada en una tarjeta inteligente, código de barras o banda magnética, el proceso de autenticación se lleva a cabo haciendo coincidir la imagen en directo y la plantilla almacenada (Figura 2-22).

Figura 2-22 Tarjetas inteligentes y autenticación facial de usuarios.



Entornos multimedia con interfaces adaptivas hombre-máquina: control de comportamiento en los centros de cuidado de niños o ancianos, reconocer a los clientes y evaluar sus necesidades (Figura 2-23).

Figura 2-23 Reconocimiento de clientes (DIGINFO, 2012).

2.5. Sistemas comerciales

Existen diversas compañías que comercializan productos de software y hardware de reconocimiento y autenticación facial ya sea para empresas o de uso personal (por ejemplo en dispositivos móviles iOS y Android). A continuación se presenta una descripción de algunos de estos productos en el mercado.

NeoFace: es un sistema de reconocimiento facial de consumidores el cual fue desarrollado por NEC[1] como una estrategia de marketing, ya que con él se pretende conocer las preferencias de los consumidores para saber por dónde conseguir captarle. De momento NeoFace es capaz de identificar a las personas, su género, la edad y la frecuencia con la que visita un establecimiento, pero esto parece un primer paso, el siguiente, como se ha indicado, posiblemente sea conocer sus preferencias y consumo, los productos que habitualmente adquiere, si lee las etiquetas de los productos, si los carteles de oferta centran su atención, etc. Finalmente, NeoFace tiene un porcentaje de reconocimiento del 95.9% y su precio es de $800 USD por unidad, dicho sistema se muestra en la Figura 2-24.

Figura 2-24 NeoFace (NeoFace, 2014).

[1] Sitio web NEC: http://mex.nec.com

FaceID F710: es un sistema de autenticación facial el cual ofrece control de acceso y control de presencia de usuarios. De forma general, se trata de una aplicación de software que permite autenticar a los usuarios autorizados, registrar los intentos de autenticación correctos y fallidos, registrar el uso de privilegios especiales del sistema y emitir señales de alarma cuando alguien no autorizado quiera acceder. Su precio es de $490 USD por unidad, dicho sistema se muestra en la Figura 2-25.

Además, el terminal utilizado es el terminal biométrico facial FaceID que incorpora grandes ventajas como:

- Control de acceso rápido: tiene un algoritmo de reconocimiento facial altamente rápido y preciso.
- Control de acceso higiénico: no requiere contacto con el usuario, cosa que permite una identificación muy higiénica.
- Control de acceso altamente preciso: tiene una tasa de error del 1%, cosa que permite una identificación de hasta el 99%.

Figura 2-25 FaceID F710 (Hanvon, 2009).

FacePass Pro: es un dispositivo de reconocimiento facial que incorpora el nuevo algoritmo núcleo BioNANO y una plataforma de hardware que garantiza la velocidad de identificación de menos de 1 segundo (1:300), permite hasta 400 usuarios, 100,000 registros y su porcentaje de reconocimiento es del 99%. Su diseño con luz infrarroja permite al terminal trabajar en las peores condiciones de iluminación. Este es un dispositivo seguro y apropiado para cualquier tipo de usuario independientemente de su piel, estilo de pelo o expresión facial. El sistema está compuesto por dos cámaras que analizan la cara, tomas diferentes imágenes desde diferentes posiciones y crean unos puntos de referencia únicos. El sistema tiene auto-aprendizaje (Anviz Intelligent Management) es decir cada vez que pasamos va adaptando los parámetros para evitar que cambios de “look” puedan hacer que con el tiempo no nos reconozca.

Permite identificar con gafas de sol, con o sin afeitar, con cortes, etc. y por supuesto no se activa con la mera presentación de una fotografía o una imagen de móvil gracias a su sistema de dual cámara. Posee además una fuente de iluminación IR que permite que podamos trabajar con cambios de iluminación e incluso en total oscuridad. Su precio es de $399 USD + IVA por unidad, dicho sistema se muestra en la Figura 2-26.

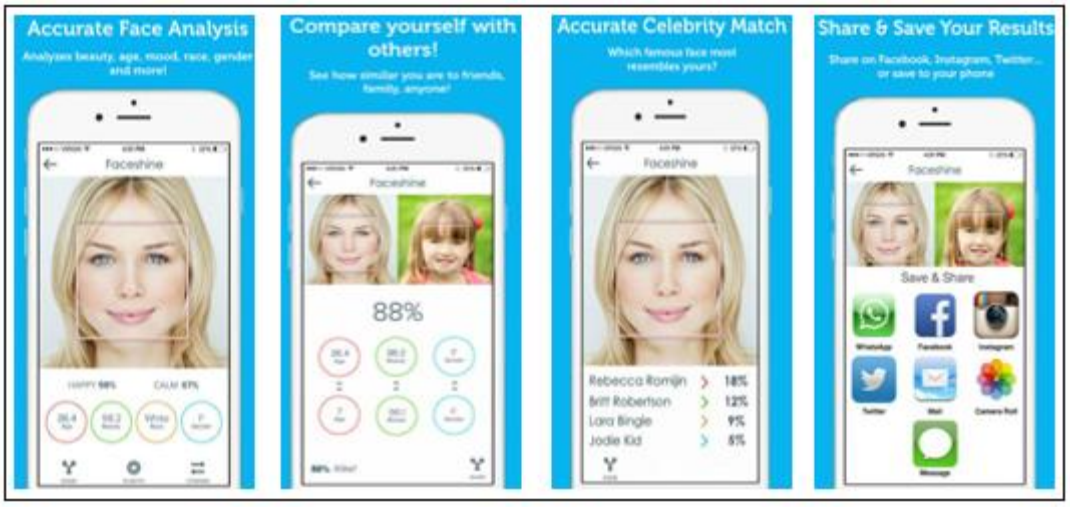
Figura 2-26 FacePass Pro (Anviz, 2013).

Faceshine: es una aplicación de análisis facial para dispositivos iOS. Faceshine analiza la cara de un usuario para definir con precisión su edad, belleza, humor, raza, género y aún más cuando se hace clic en la opción de profundidad. Lo único que tiene que hacer el usuario es tomarse una fotografía o elegir alguna que ya se tenga almacenada en el dispositivo.

Con esta aplicación el usuario se puede comparar con otras personas y saber cuánto se parece a algún amigo o familiar o quien es más atractivo, incluso se puede investigar cuales son las cuatro celebridades que se parecen más al rostro del usuario. Además, se pueden compartir los resultados obtenidos con amigos a través de las redes sociales o mensajería directa, dicho sistema se muestra en la Figura 2-27.

Faceshine se encuentra en la versión 1.0.1, ocupa 1.6 MB de almacenamiento en el dispositivo, requiere versiones 8.1 o superiores de iOS, se encuentra disponible para iPhone, iPad y iPod touch, aunque está optimizada para el iPhone 5, su desarrollador es Matt Gibson (© 2015 Matt Gibson) y su precio es de $1 USD por unidad.

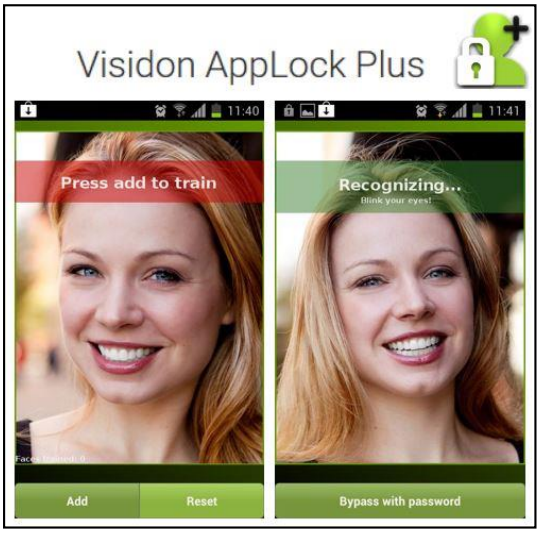
Figura 2-27 FaceShine (Gibson, 2015).



Visidon AppLock Plus: es una aplicación para teléfonos Android en la cual de manera rápida, cómoda y fresca se protege el teléfono móvil con reconocimiento facial. Se puede proteger cualquier aplicación (es decir, SMS, Galería, E-Mail, Facebook, etc.) en el teléfono mediante el reconocimiento de rostros con el objetivo de aumentar la seguridad de las aplicaciones privadas y contenidos.

Esta aplicación le permite al usuario elegir las aplicaciones que deban protegerse “su cara es la llave para abrirlos”. La aplicación utiliza la cámara frontal del teléfono móvil y verifica en tiempo real que el rostro coincida con los datos almacenados previamente y de esta manera acceder sólo a las aplicaciones seleccionadas por el usuario. Su precio aproximado es de $2.29 USD por unidad, dicho sistema se muestra en la Figura 2-28.

Figura 2-28 Visidon AppLock Plus (Visidon, 2014).



Cabe señalar que la mayoría de este tipo de sistemas comerciales presenta un muy buen desempeño de autenticación facial, sin embargo el costo por cada uno de ellos es elevado haciendo más difícil su adquisición. Es por esta razón que el desarrollo y la implementación de algoritmos para autenticación facial se ven favorecidos, ya que estos pueden presentar tasas de autenticación cercanas a las de los sistemas comerciales pero a un muy bajo costo.

3. SPEEDED UP ROBUST FEATURES

SURF, cuyo acrónimo hace referencia al título Speeded Up Robust Features, fue desarrollado por Herbert Bay *et al*. (Bay *et al*., 2006) como un detector de puntos de interés y descriptor robusto.

De forma general, SURF es un algoritmo de visión por computador, capaz de obtener una representación visual de una imagen y extraer información detallada y específica del contenido. Esta información es tratada para realizar operaciones como por ejemplo la localización y reconocimiento de determinados objetos, personas o caras, realización de escenas 3D, seguimiento de objetos y extracción de puntos de interés. Este algoritmo forma parte de la inteligencia artificial, la cual es capaz de entrenar un sistema para que interprete imágenes y determine su contenido.

Cabe mencionar que SURF está basado en su predecesor SIFT (Lowe, 2004), aunque presenta notables diferencias. Los autores afirman que este detector y descriptor presenta principalmente dos mejoras resumidas en los siguientes conceptos (Boullosa, 2011):

- Velocidad de cálculo considerablemente superior sin ocasionar perdida del rendimiento.
- Mayor robustez ante posibles transformaciones de la imagen.

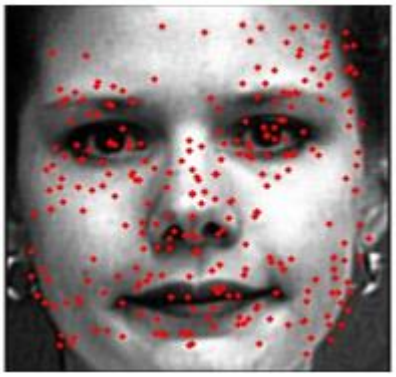
Estas mejoras se consiguen mediante la reducción de la dimensionalidad y complejidad en el cálculo de los vectores de características de los puntos de interés obtenidos. SURF se compone de tres pasos consecutivos (Oyallon y Rabin, 2013), los cuales se explicarán a detalle en la siguiente sección:

I. Detección de los puntos de interés.
II. Descripción de los puntos de interés.
III. Correspondencia entre puntos de interés.

3.1. Detección de puntos de interés

SURF hace uso de la matriz Hessiana, más concretamente, del valor del determinante de la matriz, para la localización y la escala de puntos de interés en una imagen. En la Figura 3-1 se pueden observar algunos de estos puntos.

Figura 3-1 Puntos de interés en una imagen.



Ahora bien, el motivo para la utilización de dicha matriz Hessiana es respaldado por su rendimiento en cuanto a la velocidad de cálculo y a la precisión. Lo realmente novedoso del detector incluido en el descriptor SURF respecto de otros detectores es que no utiliza diferentes medidas para el cálculo de la posición y la escala de los puntos de interés individualmente, sino que utiliza el valor del determinante de la matriz Hessiana en ambos casos.

Por lo tanto, dado un punto $p = (x, y)$ de la imagen I, la matriz Hessiana definida como $H = (p, \sigma)$ del punto p y perteneciente a la escala σ se define como se puede observar en la ecuación 3.1.

$$H(p,\sigma) = \begin{bmatrix} L_{xx}(p,\sigma) & L_{xy}(p,\sigma) \\ L_{xy}(p,\sigma) & L_{yy}(p,\sigma) \end{bmatrix} \quad (3.1)$$

Donde $L_{xx}(p,\sigma)$ representa la convolución de la derivada parcial de segundo orden de la Gaussiana $\frac{\partial^2}{\partial x^2} g(\sigma)$ con la imagen I en el punto p. De manera análoga ocurre con los términos $L_{xy}(p,\sigma)$, $L_{yy}(p,\sigma)$ de la matriz.

A pesar de que los filtros gaussianos son óptimos para el análisis del espacio-escala, se ha implementado una alternativa a los filtros gaussianos en el detector SURF debido a una serie de limitaciones de estos filtros (como la necesidad de ser discretizados, la falta de prevención total del indeseado efecto aliasing, etc.), esta alternativa son los filtros tipo caja (box-filters).

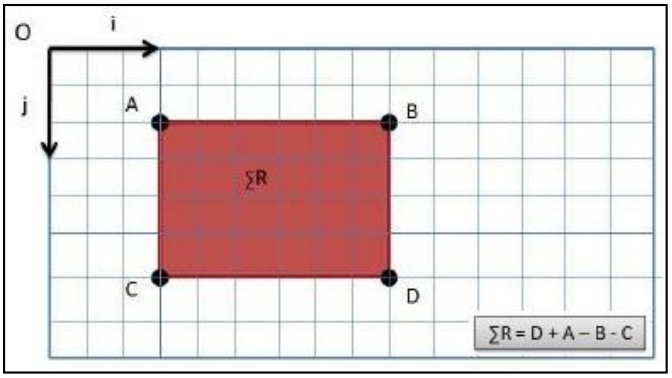
Estos nuevos filtros aproximan las derivadas parciales de segundo orden de las gaussianas y pueden ser evaluados de manera muy rápida usando imágenes integrales, independientemente del tamaño de éstas. Las imágenes integrales, cuya definición se encuentra ampliamente detallada en (Derpanis, 2007) y (Viola y Jones, 2002) son calculadas mediante la ecuación 3.2.

$$Ii_{\sum}(x,y) = \sum_{i=1}^{i \leq x} \sum_{j=1}^{j \leq y} I(i,j) \qquad (3.2)$$

Donde (x,y) representa la posición del punto en la imagen y $Ii(x,y)$ representa la intensidad de la imagen en el punto. Una vez que la imagen integral ha sido creada, se puede calcular la suma de las intensidades de una región por medio de la ecuación 3.3, tal y como se puede observar en la Figura 3-2.

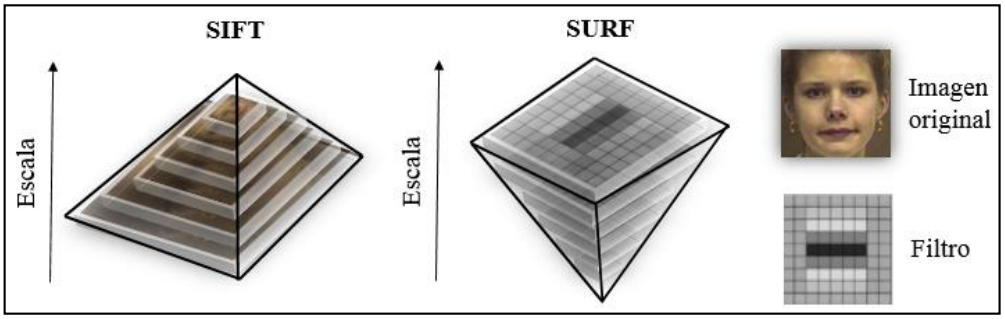
$$\sum I = Ii_D + Ii_A + Ii_B + Ii_C \qquad (3.3)$$

Figura 3-2 Representación de la intensidad de una región respecto de la imagen integral (Boullosa, 2011).



De esta forma, el tiempo necesario para el cálculo de las operaciones de convolución es independiente del tamaño de la imagen. De este modo resulta que el espacio escala es analizado mediante la elevación del tamaño del filtro, en vez de reducir el tamaño de la imagen como es el caso del detector SIFT, esta diferencia se puede apreciar en la Figura 3-3.

Figura 3-3 Representación del espacio escala de SIFT y SURF.

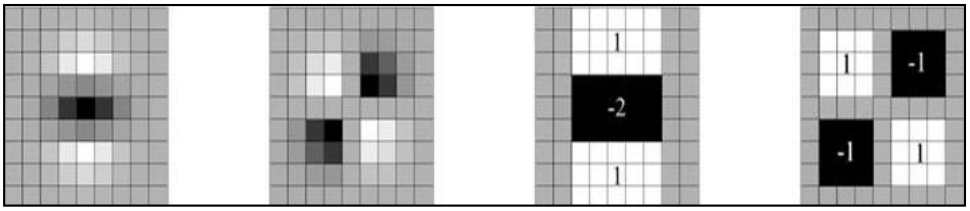


Las aproximaciones de las derivadas parciales se denotan como D_{xx}, D_{xy} y D_{yy}. En cuanto al determinante de la matriz Hessiana, éste queda definido por la ecuación 3.4.

$$\det(H_{aprox.}) = D_{xx}D_{yy} - (0.9D_{xy})^2 \qquad (3.4)$$

Donde el valor de 0.9 está relacionado con la aproximación del filtro gaussiano. En la práctica este valor es constante y no tiene un impacto significante en los resultados de los experimentos (Bay *et al.*, 2008). En la Figura 3-4 se puede observar la representación de la derivada parcial de segundo orden de un filtro gaussiano discretizado y la aproximación de la derivada implementada en el caso del descriptor SURF.

Figura 3-4 Derivadas parciales de segundo orden (Bay *et al.*, 2006).



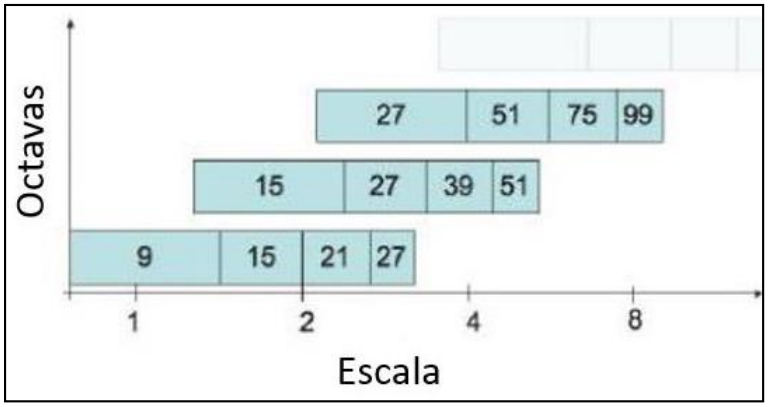
De izquierda a derecha de la Figura 3-4 se aprecian las derivadas parciales de segundo orden discretizadas y recortadas en las direcciones y y xy, así como las aproximaciones de las mismas mediante los filtros tipo caja.

La imagen de salida obtenida tras la convolución de la imagen original con un filtro de dimensiones 9 x 9, que corresponde a la derivada parcial de segundo orden de una gaussiana con $\sigma = 1.2$, es considerada como la escala inicial o también como la máxima resolución espacial ($s = 1.2$, correspondiente a una gaussiana con $\sigma = 1.2$). Las capas sucesivas se obtienen mediante la aplicación gradual de filtros de mayores dimensiones, evitando así los efectos de aliasing (curvas) en la imagen.

El espacio escala para SURF, al igual que en el caso de SIFT, está divido en octavas. Sin embargo, en SURF las octavas están compuestas por un número fijo de imágenes como resultado de la convolución de la misma imagen original con una serie de filtros tipo caja más grandes.

El incremento o paso de los filtros dentro de una misma octava es el doble respecto del paso de la octava anterior, al mismo tiempo que el primero de los filtros de cada octava es el segundo de la octava predecesora, como se muestra en la Figura 3-5.

Figura 3-5 Representación de la longitud de los filtros de diferentes octavas (Boullosa, 2011).



De esta manera se obtienen las siguientes series de octavas con sus respectivos filtros:

- Octava inicial: $9x9 \overset{6}{\rightarrow} 15x15 \overset{6}{\rightarrow} 21x21 \overset{6}{\rightarrow} 27x27$
- Octava siguiente: $15x15 \overset{12}{\rightarrow} 27x27 \overset{12}{\rightarrow} 39x39 \overset{12}{\rightarrow} 51x51$
- Octava siguiente: $27x27 \overset{24}{\rightarrow} 51x51 \overset{24}{\rightarrow} 75x75 \overset{24}{\rightarrow} 99x99$
- Y así sucesivamente…

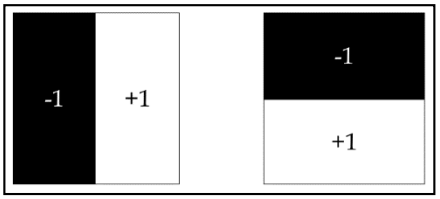
Finalmente para calcular la localización de todos los puntos de interés en todas las escalas, se procede mediante la eliminación de los puntos que no cumplan la condición de máximo en un vecindario de $3x3x3$. De esta manera, el máximo determinante de la matriz Hessiana es interpolado en la escala y posición de la imagen. En este punto se da por concluida la etapa de detección de los puntos de interés.

3.2. Descripción de puntos de interés

Antes de pasar a la creación del descriptor, la siguiente etapa corresponde a la asignación de la orientación de cada uno de los puntos de interés obtenidos en el paso anterior. Es en esta etapa donde se otorga al descriptor de cada punto la invarianza ante la rotación mediante la orientación del mismo.

Primero hay que realizar el cálculo de la respuesta de Haar en ambas direcciones tanto en x como en y, esto se lleva a cabo mediante las funciones representadas en la Figura 3-6, donde el color negro tiene el peso de -1 y el color blanco tiene el peso de $+1$. Además, El área de interés para el cálculo de las respuestas de Haar es el área circular centrada en el punto de interés y de radio $6s$, siendo s (donde $s \geq 1$) la escala en la que el punto de interés ha sido detectado. De la misma manera, la etapa de muestreo depende de la escala, tomándose como valor a s. Respecto de las funciones onduladas de Haar, se toma el valor $4s$, por tanto dependiente también de la escala, como referencia, donde a mayor valor de escala mayor es la dimensión de las funciones onduladas.

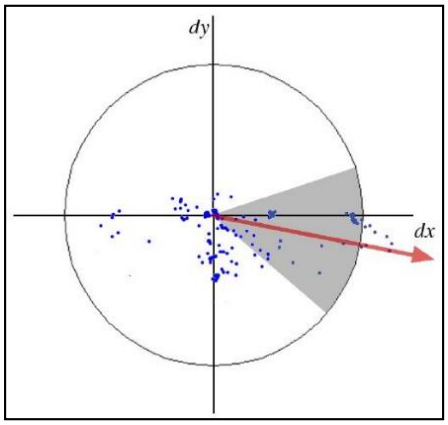
Figura 3-6 Respuestas de Haar en x (izquierda) e y (derecha) (Boullosa, 2011).



Tras haber realizado todos estos cálculos, se utilizan imágenes integrales nuevamente para proceder al filtrado mediante las máscaras de Haar y obtener así las respuestas en ambas direcciones. Asimismo, son necesarias únicamente seis operaciones para obtener la respuesta en la dirección x e y. Una vez que las respuestas onduladas han sido calculadas, son ponderadas por una gaussiana de valor $\sigma = 2.5s$ centrada en el punto de interés.

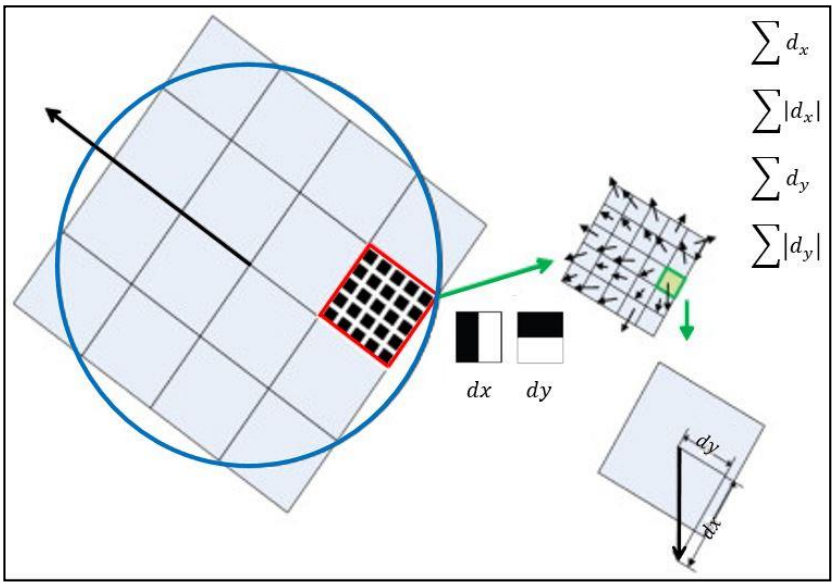
Las respuestas son representadas como vectores en el espacio colocando la respuesta horizontal y vertical en el eje de abscisas y ordenadas respectivamente. Después, se obtiene una orientación dominante por cada sector mediante la suma de todas las respuestas dentro de una ventana de orientación móvil cubriendo un ángulo de $\frac{\pi}{3}$ siguiendo las especificaciones recomendadas por (Bay *et al.*, 2006). La orientación final del punto de interés será finalmente aquella cuyo vector sea el más grande dentro de los seis sectores en los que ha sido dividida el área circular alrededor del punto de interés (ver Figura 3-7).

Figura 3-7 Asignación de la orientación de un punto de interés (Boullosa, 2011).



Ahora bien, se procede con la creación del descriptor SURF para cada punto de interés. Como primer paso se construye una región cuadrada de tamaño $20s$ alrededor del punto de interés con la orientación calculada en la etapa anterior. Esta región es a su vez dividida en $4x4$ sub-regiones dentro de cada una de las cuales se calculan las respuestas de Haar de puntos con una separación de muestreo de $5x5$ en ambas direcciones. Por simplicidad, se consideran d_x y d_y las respuestas de Haar en las direcciones horizontal y vertical respectivamente relativas a la orientación del punto de interés. En la Figura 3-8 están representadas tanto las respuestas de Haar en cada una de las sub-regiones alrededor del punto de interés así como las componentes d_x y d_y de uno de los vectores.

Figura 3-8 Respuestas de Haar en las sub-regiones del punto de interés (Boullosa, 2011).



Para dotar a las respuestas d_x y d_y de una mayor robustez ante deformaciones geométricas y errores de posición, éstas son ponderadas por una gaussiana de valor $\sigma = 3.3s$ centrada en el punto de interés. En cada una de las sub-regiones se suman las respuestas d_x y d_y obteniendo así un valor de d_x y d_y representativo por cada una de las sub-regiones.

Al mismo tiempo se realiza la suma de los valores absolutos de las respuestas $|d_x|$ y $|d_y|$ en cada una de las sub-regiones, obteniendo de esta manera, información de la polaridad sobre los cambios de intensidad. En resumen, cada una de las sub-regiones queda representada por un vector v de componentes d_x, d_y, $|d_x|$ y $|d_y|$, la representación matemática de este vector se puede apreciar en la ecuación 3.5.

$$v = \left(\sum d_x, \sum d_y, \sum |d_x|, \sum |d_y|\right) \tag{3.5}$$

Por lo tanto, englobando las $4x4$ sub-regiones, resulta un descriptor SURF con una longitud de 64 valores para cada uno de los puntos de interés identificados.

3.3. Correspondencia entre puntos de interés

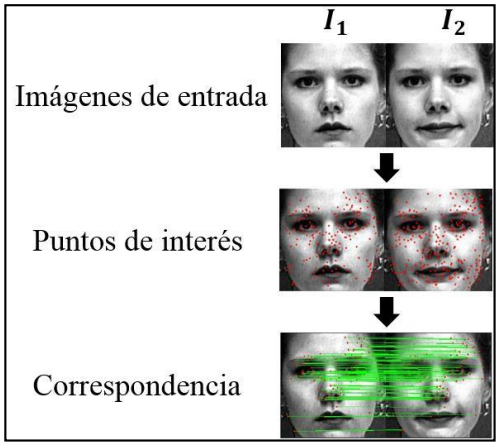
A este último paso del algoritmo SURF también se le conoce como *matching* (coincidencia), ya que tiene como finalidad el cálculo de un valor que represente el grado de similitud entre dos imágenes, y que a continuación se puedan establecer las diferentes conclusiones. El cálculo de este valor, representado como distancia y conocido también como *score*, se realiza mediante la aplicación de una métrica o fórmula de la distancia entre ambas imágenes. Previo al cálculo del *score*, es necesario establecer las correspondencias entre los puntos clave. Dicha correspondencia se lleva a cabo mediante el cálculo de la distancia euclidiana entre los vectores de características pertenecientes a diferentes puntos de interés. Este cálculo genera a su vez otro valor que será utilizado para determinar cuál de los puntos de la imagen comparada se corresponde con su homólogo, en el caso de existir, de la primera de las imágenes.

Suponiendo que se quiere realizar el *matching* de puntos entre dos imágenes representadas por I_1 e I_2. Para cada uno de los puntos clave pertenecientes a I_1, se seleccionan los dos mejores candidatos de entre todos los puntos clave pertenecientes a I_2 mediante el criterio de máxima similitud.

Este criterio establece que los mejores candidatos para realizar el *matching* con el punto clave I_1 perteneciente a I_1 cuyo vector de características es v_1, son los puntos clave p'_1 y p'_2 pertenecientes a I_2 cuyos vectores de características v'_1 y v'_2 representan las distancias euclidianas mínimas d_1 y d_2 respectivamente, en relación con v_1.

Si la relación d_1/d_2 entre las distancias mencionadas es suficientemente pequeña, entonces se establece el *matching* entre los puntos p_1 y p'_1 pertenecientes a cada una de las imágenes. De acuerdo con (Bay *et al.,* 2006), se establece un umbral de 0.7 para la razón (división) d_1/d_2. Esta estrategia de *matching* recibe el nombre de "el vecino más próximo". Finalmente la puntuación o *score* entre las dos imágenes se obtiene mediante una relación que tiene en cuenta el número total de puntos correspondientes entre ambas imágenes. La Figura 3-9 muestra un ejemplo de *matching* entre I_1 e I_2.

Figura 3-9 Correspondencia (matching) entre dos imágenes.



A pesar del buen desempeño del algoritmo SURF en diferentes aplicaciones como las realizadas por (Terriberry *et al.*, 2008), (Svab *et. al.*, 2009), (Bouris *et al.*, 2010), (Pinto y Anurenjan, 2011), (Murali y MITS, 2012), (Thakoor *et al.*, 2013), (Wang *et al.*, 2014), (Zheng *et al.*, 2015), el porcentaje en la autenticación facial oscila entre el 70 y 80%, por lo tanto si se requiere que este porcentaje mejore es necesario realizar una mejora en dicho algoritmo.

Por esta razón, en este proyecto de investigación se propone la implementación de una etapa adicional de preprocesamiento antes de emplear el algoritmo SURF, todo ello con el fin de obtener mejores resultados dentro de un sistema de autenticación facial. Cabe señalar, que el preprocesamiento tiene como objetivo reducir la influencia de errores o inconsistencias en los valores del brillo de la imagen, lo cual pudiera limitar el desempeño del algoritmo SURF.

4. METODOLOGÍA

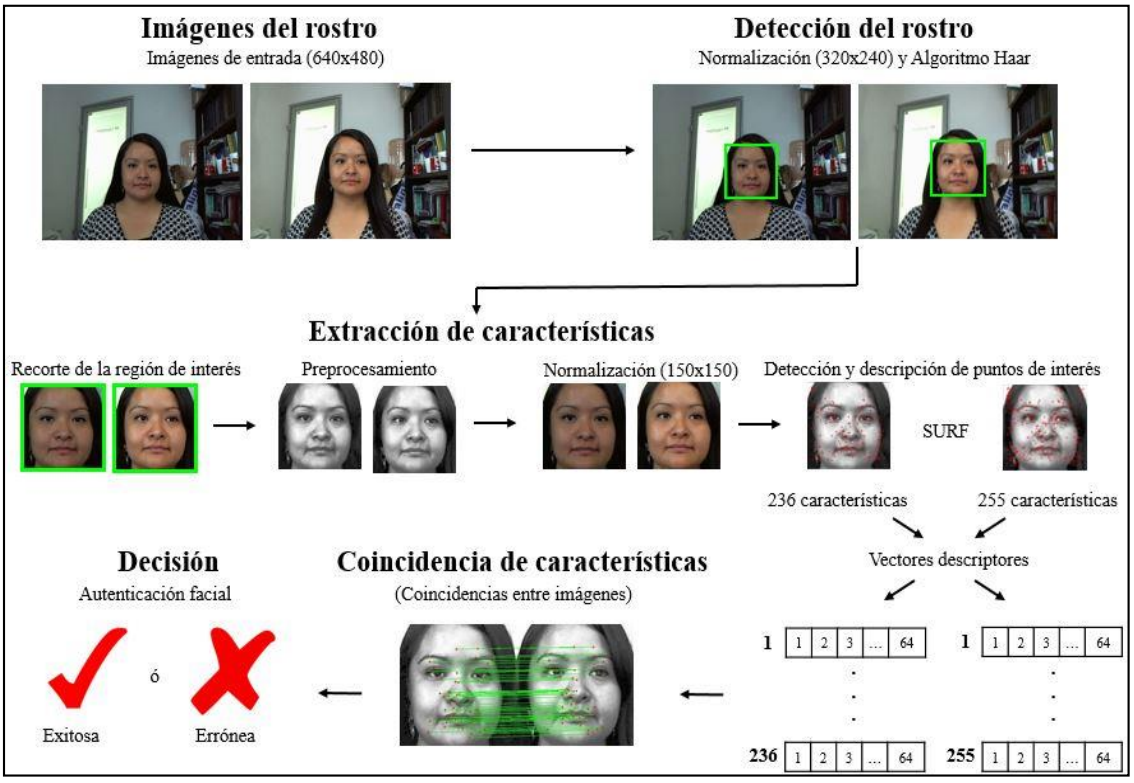
4.1. Descripción general

En este trabajo se propone la implementación de una etapa de preprocesamiento dentro del proceso de autenticación facial. Como se puede observar en la Figura 4-1, esta metodología consta de cinco pasos:

1) Imágenes del rostro.
2) Detección del rostro.
3) Extracción de características.
4) Coincidencia de características (*matching*).
5) Decisión.

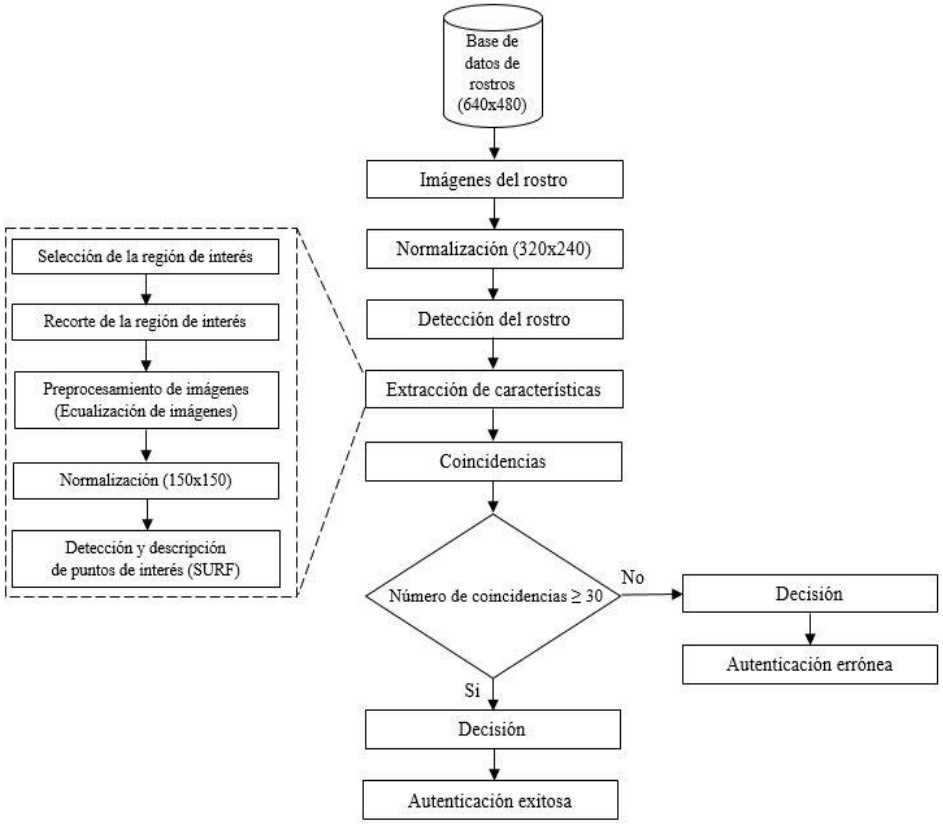
Cabe destacar que la aportación de este trabajo se realiza en la etapa de extracción de características.

Figura 4-1 Metodología propuesta.



La Figura 4-2 presenta el diagrama general de la metodología implementada en este trabajo.

Figura 4-2 Diagrama general de la metodología propuesta.



4.2. Imágenes del rostro

La adquisición de cada una de las imágenes del rostro se obtiene mediante el uso de una cámara web Logitech® HD Pro Webcam C910 empleando la consola de Raspbian[2] y el siguiente comando (para más información consultar el Anexo I): fswebcam -r resolucion sin_banner nombre_imagen.jpg

Donde:

- fswebcam es el comando que manda llamar la cámara web.

[2] Sitio web del sistema operativo Raspbian: http://www.raspbian.org/

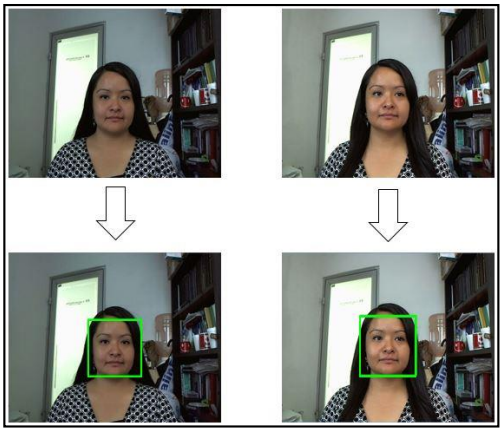
- -r es el comando para establecer la resolución de la imagen.
- resolución se utiliza para describir cuán nítida será la imagen.
- sin_banner es el comando que indicará que la imagen no contendrá ninguna cinta (banner) en el pie de la misma.
- nombre_imagen.jpg es el nombre y extensión que se le asignará a la imagen obtenida.

Dentro del proceso de adquisición de imágenes destaca la obtención de una imagen del rostro de la persona directamente de la cámara, tal y como se puede observar en el primer bloque de la Figura 4-2 denominado imágenes del rostro, dentro de este proceso únicamente se captura una imagen desde un dispositivo (este puede ser una cámara web) y se toma una imagen del usuario que se encuentra almacenada en la base de datos, de esta manera las dos imágenes pasan al siguiente proceso que es la detección del rostro.

4.3. Detección del rostro

Una vez seleccionadas las dos imágenes, cada una de ellas se normaliza a 320x240 pixeles y se le aplica el algoritmo Haar como método de detección de rostro (ver Figura 4-3), este es considerado como el paso previo al procesamiento de cada una de las imágenes. Información más detallada sobre este método puede ser consultada en (Viola y Jones, 2001).

Figura 4-3 Detección del rostro.



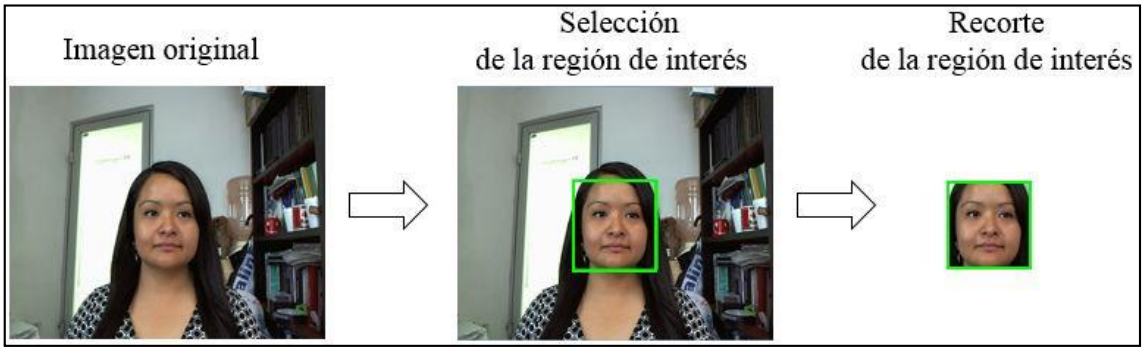
4.4. Extracción de características

En este paso se implementa una fase de preprocesamiento a las imágenes de entrada que fueron seleccionadas previamente (la imagen del dispositivo y la de la base de datos). Por lo tanto, el objetivo de la extracción de características es obtener sólo las imágenes del rostro (sin el fondo de la imagen, ya que esto facilitará su tiempo de procesamiento) y posteriormente implementar el algoritmo SURF para la detección y descripción de características en las imágenes del rostro. De esta manera se busca la obtención de un mejor resultado de todo el proceso de autenticación facial.

Como se muestra en la Figura 4-2 dentro de la etapa de extracción de características, se definen cinco sub-etapas: selección de la región de interés, recorte de la región de interés, preprocesamiento de imágenes, normalización de imágenes, finalmente la detección y descripción de puntos de interés.

En la primer sub-etapa se selecciona una región de interés, la cual está definida por el resultado obtenido en la fase de detección del rostro (en la imagen original se dibuja un recuadro de color verde alrededor del rostro de la persona). Posteriormente, en la sub-etapa de recorte de la región de interés se recorta dicha área obteniendo únicamente la imagen del rostro tal y como se puede apreciar en la Figura 4-4.

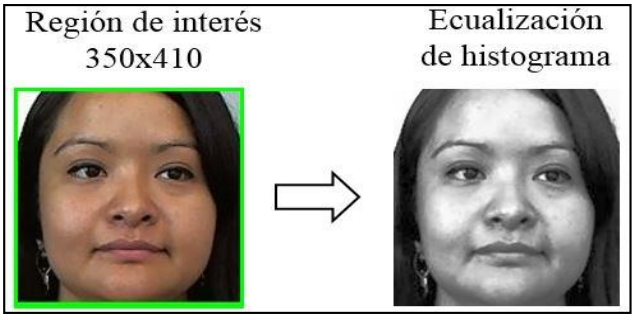
Figura 4-4 Selección y recorte del área de interés.



Una vez que ya se ha recortado la región de interés, la sub-etapa posterior consiste en aplicar a las imágenes de entrada una técnica denominada ecualización de histograma (HE), este proceso en particular se considera como la principal aportación de este trabajo ya que la HE es uno de los métodos más usados para realzar efectivamente el contraste de una imagen (Paik, 2011), además de que esta modificación previa al uso del algoritmo SURF no había sido propuesta en investigaciones previas.

Además, la HE modifica el valor de los pixeles de tan manera que la intensidad del histograma de la imagen resultante llegar a ser uniforme, además esta imagen hace uso de todos valores de brillo posible por lo tanto resulta una imagen realzada en su contaste (Han *et al., 2011*). El resultado de esta sub-etapa se ilustra en la Figura 4-5.

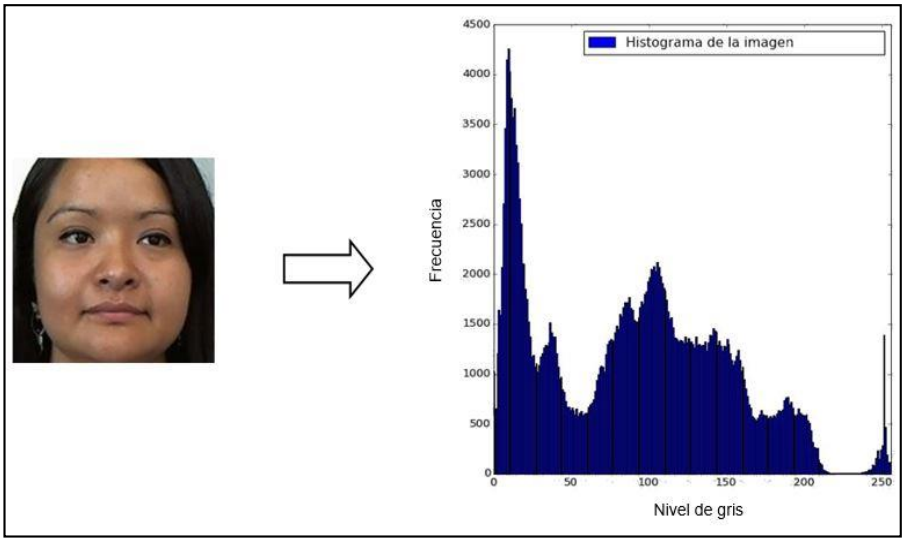
Figura 4-5 Región de interés y ecualización de histograma.



Un ejemplo más claro sobre la HE se presenta en las Figuras 4-7 y 4-8 ya que es posible apreciar la diferencia entre los histogramas de dos imágenes de entrada, donde la primera de ellas sólo es una imagen recortada y no se le ha aplicado la ecualización a diferencia de la segunda imagen.

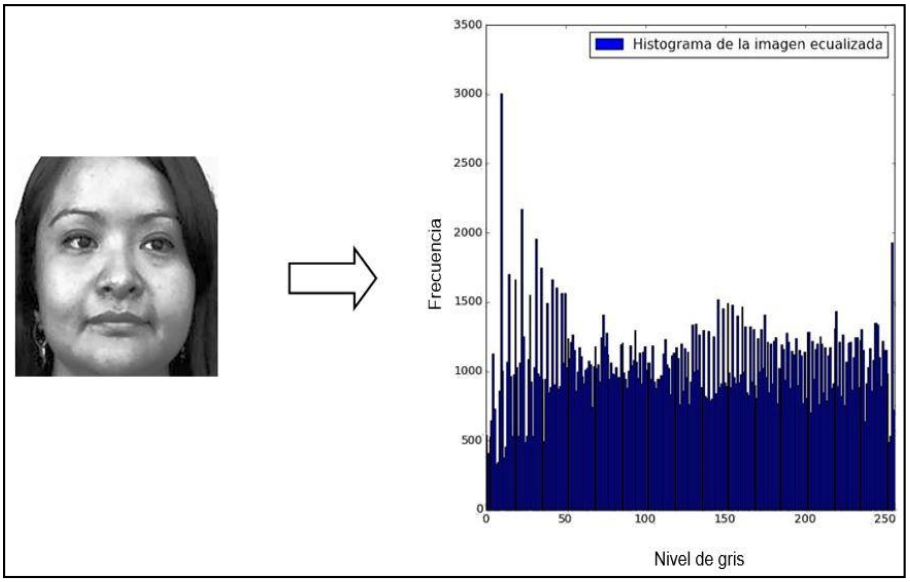
En la Figura 4-6 se puede observar como la representación del brillo y contraste de la imagen se encuentran concentradas en una sola región del histograma, esto quiere decir que la imagen es menos clara y definida.

Figura 4-6 Histograma de la imagen recortada.



Por el contrario, la Figura 4-7 presenta una mejor distribución del histograma de la imagen en cuanto su brillo y contraste, donde como resultado se obtiene una imagen más clara y definida, esta es una característica muy importante ya que la imagen es mejorada para los siguientes pasos del proceso de autenticación facial, todo ello gracias a la aplicación de esta técnica (HE).

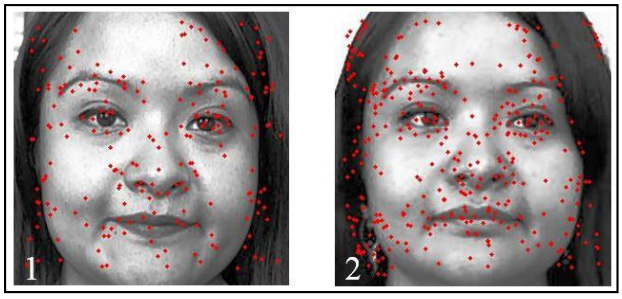
Figura 4-7 Histograma de la imagen ecualizada.



La posterior sub-etapa es la normalización, la cual consiste en adaptar el tamaño de las imágenes ecualizadas a 150x150 pixeles, esto con el objetivo de que ambas tengan las mismas dimensiones tanto ancho como alto y de esta manera procesarlas bajo las mismas circunstancias (en este caso por su tamaño el cual será constante dentro de todo el proceso de autenticación facial).

Una vez realizada la normalización, el siguiente paso dentro del proceso de extracción de características es aplicar el algoritmo SURF para la detección y descripción de puntos de interés en las imágenes de entrada, cabe señalar que a estos puntos también se les conoce como descriptores. Cada descriptor contiene un vector de 64 elementos, los cuales servirán como datos de entrada para el siguiente paso de esta metodología. La Figura 4-8 ilustra los descriptores (puntos rojos) detectados en las imágenes de entrada.

Figura 4-8 Descriptores de las imágenes de entrada 1 y 2.

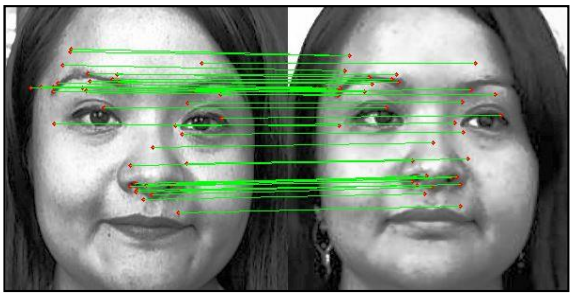


4.5. Proceso de coincidencia

Una vez extraídas las características (descriptores) de las imágenes de entrada, se continúa con el proceso de coincidencia entre imágenes (en la literatura también se le conoce como *matching*) donde de acuerdo a los descriptores localizados en las imágenes de entrada, se comparan los vectores de la imagen 1 con los vectores de la imagen 2 para determinar cuántos de ellos son similares en ambas imágenes. Para que un descriptor de una imagen sea considerado como similar en otra imagen, es necesario encontrar la distancia Euclidiana menor entre ellos. Información más detallada sobre este proceso se puede encontrar en (Deza y Deza, 2009).

Después, todas las coincidencias que fueron encontradas en ambas imágenes son contadas para determinar su número extracto y de esta manera poder continuar con el paso final de la metodología. Este proceso puede ser apreciado en la Figura 4-9 donde cada descriptor de la imagen 1 que coincide con el descriptor de la imagen 2 es unido por una línea de color verde para representar dicha coincidencia.

Figura 4-9 Coincidencias entre las imágenes de entrada.



4.6. Decisión

Dado el número total de coincidencias entre las imágenes, el siguiente paso es la decisión donde tomando como referencia el procedimiento realizado por (Ren *et al., 2013*) para determinar si las imágenes coinciden o no, en este proyecto de investigación se propone un umbral heurístico con valor de 30, esto quiere decir que si el número de coincidencias es mayor o igual a 30, el proceso de autenticación facial se considerará como exitoso (Match). Por el contrario, si es menor a dicho umbral el proceso se considerará como erróneo (Not match).

Con el fin de evaluar esta metodología, los voluntarios, diferentes dispositivos (laptop, tarjetas de desarrollo, Smartphones y Tablets), algunas de las imágenes de la base de datos SURFace y de las bases de datos públicas fueron sometidos a diferentes pruebas. Los resultados obtenidos se presentan en la siguiente sección.

5. RESULTADOS Y DISCUSIÓN

5.1. Software y hardware utilizado

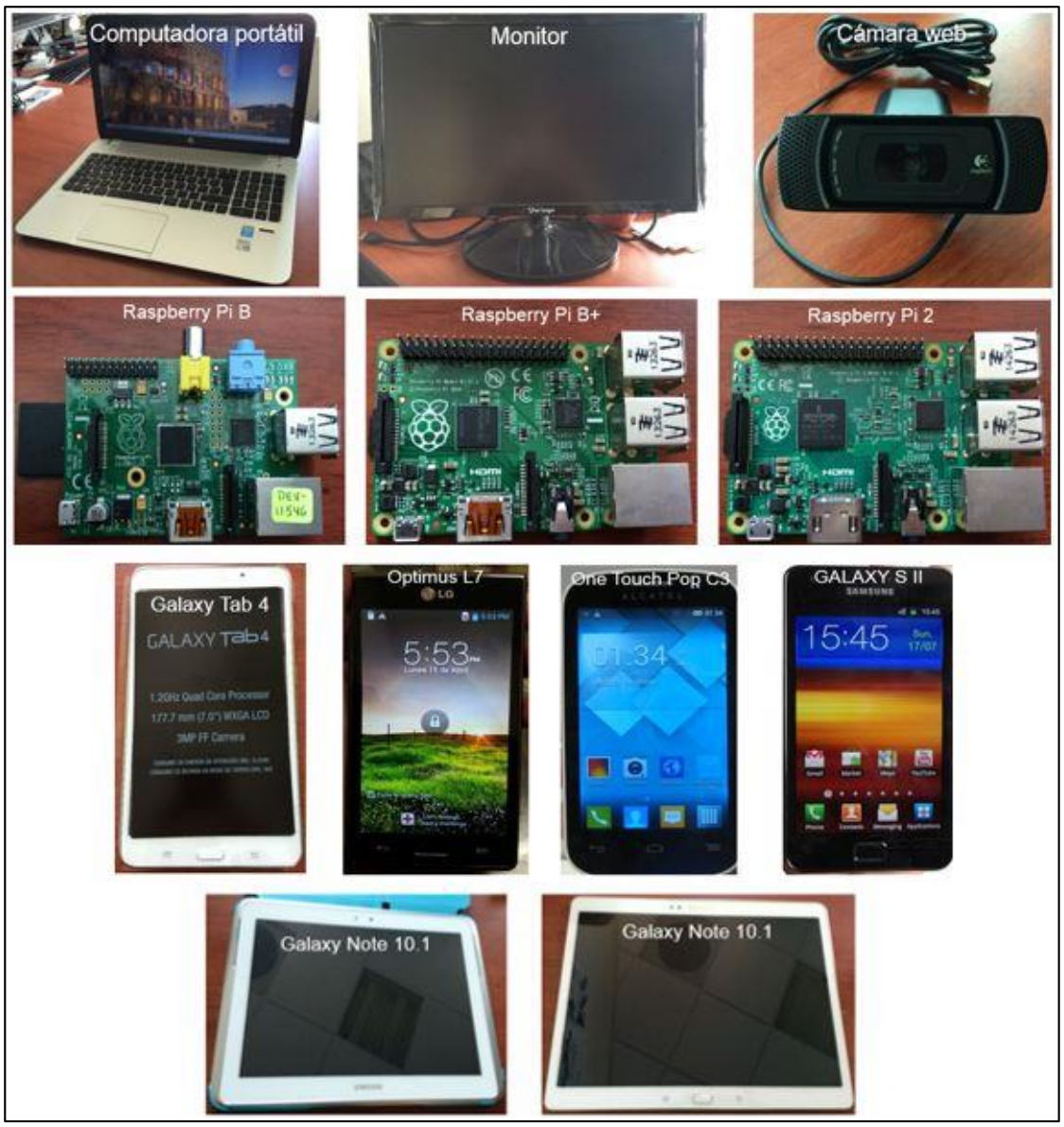
La Tabla 5-1 presenta el software y hardware (ver Figura 5-1) utilizado en las diferentes pruebas del sistema de autenticación facial.

Tabla 5-1 Software y hardware utilizado.

Software	Eclipse	Versión: Kepler (entorno de desarrollo).
	Python	Versión: 2.7.3 (lenguaje de programación).
	OpenCV	Versión: 2.4.9
	Sistemas operativos	Windows 8 x64, Raspbian[3] y Android.
Hardware	Computadora portátil	Notebook HP ENVY 15. Procesador Intel® Core™ i7 CPU 2.4GHz. 16.0 GB (RAM).
	Raspberry Pi	Modelos a) 2, b) B y c) B+. Procesador ARM1176JZF-S 700MHz single-core. 512 MB (RAM).
	Monitor	Vorago Led Widescreen 300.
	Cámara web	Logitech HD Pro Webcam C910.
	Tablet	d) Samsung Galaxy Tab 4. Procesador Quad-Core 1.2GHz. 1.5 GB (RAM). Versión de Android 4.4.2
		e) Samsung Galaxy Note 10.1 Procesador Quad-Core 1.4GHz. 2 GB (RAM). Versión de Android 4.1.2
		f) Samsung Galaxy Tab S. Procesador Octa-Core 1.9GHz. 3 GB (RAM). Versión de Android 4.4.2
	Smartphone	g) LG Optimus L7. Procesador Qualcomm MSM7227A Snapdragon 1GHz. 512 MB (RAM). Versión de Android 4.0.3
		h) Alcatel One Touch Pop C3. Procesador Dual-Core 1.3GHz. 512 MB (RAM). Versión de Android 4.4.2
		i) Samsung GALAXY S II GT-I9100. Procesador Dual Core 1.2GHz. 1 GB (RAM). Versión de Android 5.1.1

[3] Raspbian es un Sistema operativo libre basado en Debian optimizado para el hardware Raspberry Pi (Raspberry, 2015).

Figura 5-1 Hardware para pruebas del sistema de autenticación facial.



Dentro de la sección de pruebas se realizaron una serie de experimentos con diferentes dispositivos, el primero de ellos fue una computadora portátil ya que en esta primera etapa se implementó en Python el preprocesamiento de imágenes y el algoritmo SURF. Posteriormente se llevó a cabo una etapa intermedia de pruebas en tarjetas programables (Raspberry Pi) dado que estas presentan una arquitectura electrónica muy similar a la de los dispositivos móviles (Smartphone y Tablet).

Finalmente, en la última etapa se realizó la migración de la metodología programada en Python a JAVA y C++ para su implementación en dispositivos móviles. En estas pruebas se emplearon algunas imágenes de bases de datos públicas y de la propia (SURFace) con el objetivo de verificar la adquisición de los datos, cada proceso de la metodología propuesta, verdaderos y falsos positivos, verdaderos y falsos negativos, tiempo de procesamiento y desempeño en cada dispositivo (principalmente en los dispositivos móviles).

5.2. Imágenes empleadas

Para el desarrollo y pruebas de la metodología propuesta se emplearon dos tipos de adquisición de imágenes, el primero de ellos es mediante el uso de bases de datos de rostros las cuales se encuentran disponibles de manera pública en internet y el segundo tipo es mediante la adquisición de imágenes desde una cámara web (estas imágenes corresponden a la base de datos propia).

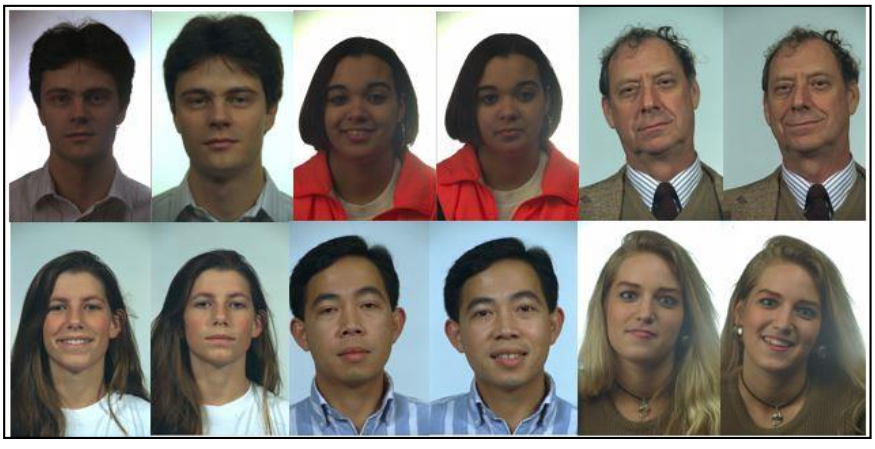
Las bases de datos públicas que se usaron para este trabajo son The Extended Cohn-Kanade Dataset (CK+), Caltech Faces y FERET. Se eligieron estas bases de datos ya que son de las más empleadas en la literatura para pruebas de reconocimiento y autenticación facial. A continuación se dará una breve descripción de cada una de ellas.

Caltech Faces. Base de datos a color (con imágenes capturadas de forma frontal) recolectadas por Markus Weber del Instituto de Tecnología de California. Consta de 450 imágenes de 27 individuos (entre 5 y 21 imágenes por persona considerando hombres y mujeres de diferentes edades), la dimensión de las imágenes es de 896x592 pixeles, cada una en formato JPEG, adquiridas bajo diferentes condiciones de iluminación, expresiones faciales y diversos fondos (Weber, 2000). La Figura 5-2 muestra algunas imágenes correspondientes a esta base de datos.

Figura 5-2 Imágenes de la base de datos Caltech Faces.

FERET. Base de datos a color recolectada en un ambiente semicontrolado por el Dr. Harry Wechsler de la Universidad George Mason (George Mason University) y el Dr. P. Jonathon Phillips del Laboratorio de Investigación del Ejército (Army Research Laboratory). Contiene 14126 imágenes de 1199 individuos (entre 6 y 33 imágenes por persona considerando hombres y mujeres de diferentes edades), la dimensión de las imágenes es de 512x768 pixeles, cada una en formato PPM, adquiridas bajo diferentes condiciones de iluminación, expresiones faciales y fondo uniforme (Phillips *et al.*, 2000). La Figura 5-3 muestra algunas imágenes correspondientes a esta base de datos.

Figura 5-3 Imágenes de la base de datos FERET.



The Extended Cohn-Kanade Dataset (CK+). Base de datos de expresiones faciales a color y en escala de grises recolectada por Patrick Lucey, Jeffrey F. Cohn, Takeo Kanade, Jason Saragih del Instituto de Robótica, Universidad Carnegie Mellon (Pittsburgh), Zara Ambadar del Departamento de Psicología, Universidad de Pittsburgh así como por Iain Matthews de Disney Research, Pittsburgh. Contiene 2300 imágenes de 100 individuos (23 imágenes por persona considerando hombres y mujeres de diferentes edades), la dimensión de las imágenes es de 640x480, 640x490 y 720x480, cada una en formato PNG, adquiridas bajo diferentes condiciones de iluminación, expresiones faciales y diversos fondos (Lucey *et al., 2010*). La Figura 5-4 muestra algunas imágenes correspondientes a esta base de datos.

Figura 5-4 Imágenes de la base de datos The Extended Cohn-Kanade Dataset (CK+).

Por otro lado, como resultado del proceso de adquisición de imágenes desde una cámara web se generó la base de datos propia denominada SURFace, en la cual se controla la iluminación así como la posición y expresión del rostro de 18 voluntarios, adquiriendo 10 imágenes por cada uno de ellos con una resolución de 640x 480 pixeles (se eligió este tamaño para acelerar el proceso de autenticación facial). Más detalles de esta base de datos se pueden consultar la Tabla 5-2.

La Figura 5-5 muestra algunos ejemplos de las imágenes que fueron adquiridas en este proceso.

Tabla 5-2 Características de la base de datos SURFace.

SURFace
18 individuos. 10 imágenes por individuo (180 imágenes en total). Formato de las imágenes: JPG. Resolución de las imágenes: 640x480 Imágenes con diversos fondos, iluminación, expresiones faciales, diferente distancia entre el rostro y la cámara, además en algunos casos se presenta el uso de lentes de aumento.

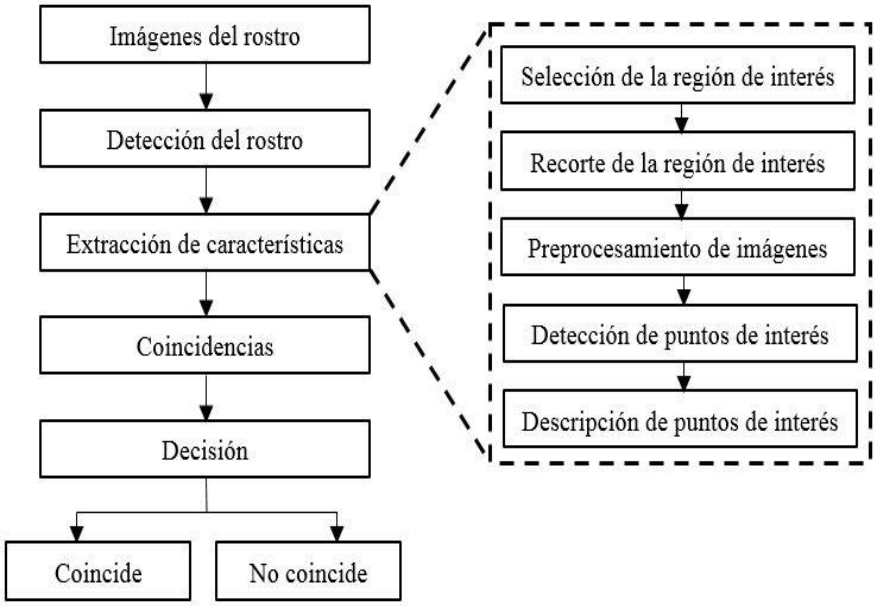
Figura 5-5 Imágenes de la base de datos SURFace.

5.3. Pruebas en computadora

Las pruebas realizadas en computadora consideran únicamente algunos procesos de la extracción de características, el entrenamiento del algoritmo SURF (detección y descripción de puntos de interés) con las bases de datos públicas y en esta fase de desarrollo de la metodología no se consideró el tiempo de procesamiento.

Cabe señalar que a medida que se van realizando pruebas en los diferentes dispositivos (tarjetas de desarrollo y dispositivos móviles) se va implementado la metodología propuesta en este trabajo, permitiendo dentro de esta misma una retroalimentación para obtener mejores resultados. A continuación, la Figura 5-6 muestra el diagrama del proceso descrito para las pruebas en computadora.

Figura 5-6 Metodología propuesta para pruebas en computadora.



Dado el diagrama de la Figura 5-6, se realizaron 15 pruebas con algunas imágenes de las bases de datos The Extended Cohn-Kanade Dataset (CK+) y Caltech Faces.

Los primeros dos procesos (imágenes y detección del rostro) fueron exitosos al 100%. Posteriormente se llevó a cabo la extracción de características. La Tabla 5-3 presenta el resultado del número de características (puntos de interés) obtenido en cada imagen de entrada de las dos bases de datos, además de información como:

- Prueba: número de prueba a realizar (de 1 a 15).
- St: corresponde al estatus de las imágenes (este puede ser Igual: E o Diferente: D).
- Cp: tipo de comparación entre imágenes (Femenino: F o Masculino: M), por ejemplo F – M es una comparación entre una imagen de una mujer (Femenino) y un hombre (Masculino).
- Img 1 y 2: identificador de la imagen de entrada (para realizar este proceso se requieren dos imágenes de entrada es por eso que se considera a Img 1 e Img 2).

Tabla 5-3 Número de características entre imágenes.

	CK+				Caltech Faces			
Prueba	**St.**	**Cp.**	**Img. 1**	**Img. 2**	**St.**	**Cp.**	**Img 1**	**Img 2**
1	E	F-F	431	435	D	M-M	833	998
2	D	F-F	288	435	E	M-M	666	1064
3	E	F-F	693	679	E	M-M	667	801
4	D	F-M	467	774	E	M-M	746	1112
5	E	M-M	450	510	D	F-F	1064	506
6	E	M-M	945	959	E	M-M	749	658
7	D	M-M	494	768	E	F-F	604	776
8	E	M-M	767	873	E	F-F	725	853
9	E	F-F	621	453	D	M-M	984	816
10	E	F-F	401	312	E	F-F	506	735
11	E	F-F	383	362	D	F-M	1141	687
12	D	F-M	383	391	E	M-M	891	915
13	E	M-M	428	497	E	M-M	1172	886
14	E	M-M	484	535	D	F-M	839	587
15	D	F-M	440	547	E	M-M	629	1124

El siguiente paso es la obtención del número de coincidencias entre las imágenes de entrada, los resultados se presentan en la Tabla 5-4.

Tabla 5-4 Coincidencias entre imágenes.

Prueba	CK+	Caltech Faces
1	104	004
2	005	020
3	056	051
4	004	032
5	078	005
6	101	051
7	004	047
8	035	024
9	030	004
10	013	018
11	042	007
12	005	042
13	106	036
14	102	005
15	005	015

El paso final es la decisión, donde de acuerdo al umbral heurístico (coincidencias ≥ 30) se establece si las imágenes de entrada coinciden o no. Los resultados se presentan en la Tabla 5-5 donde se muestran los verdaderos y falsos positivos así como los verdaderos y falsos negativos.

Tabla 5-5 Coincidencias entre imágenes.

Base de datos	TP (%)	TN (%)	FP (%)	FN (%)	Autenticación (%)
CK+	60	33	0	07	93
Caltech Faces	53	33	0	13	86

En las Figuras 5-7 y 5-8 se puede observar el proceso llevado a cabo con esta metodología empleando algunas imágenes iguales y diferentes de las bases de datos The Extended Cohn-Kanade Dataset (CK+) y Caltech Faces, respectivamente, comenzando con las imágenes de entrada, detección del rostro,

selección de la región de interés, preprocesamiento, extracción de características, coincidencias entre imágenes y finalmente la decisión.

Figura 5-7 Pruebas con la base de datos CK+ en imágenes iguales.

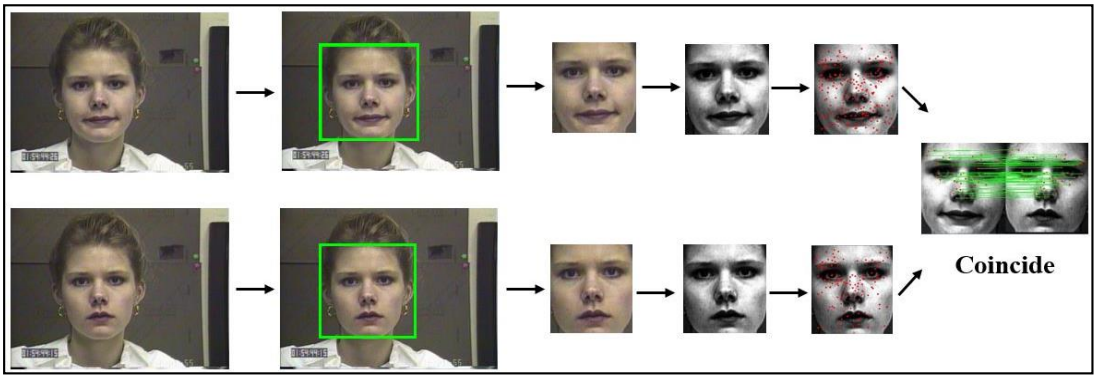
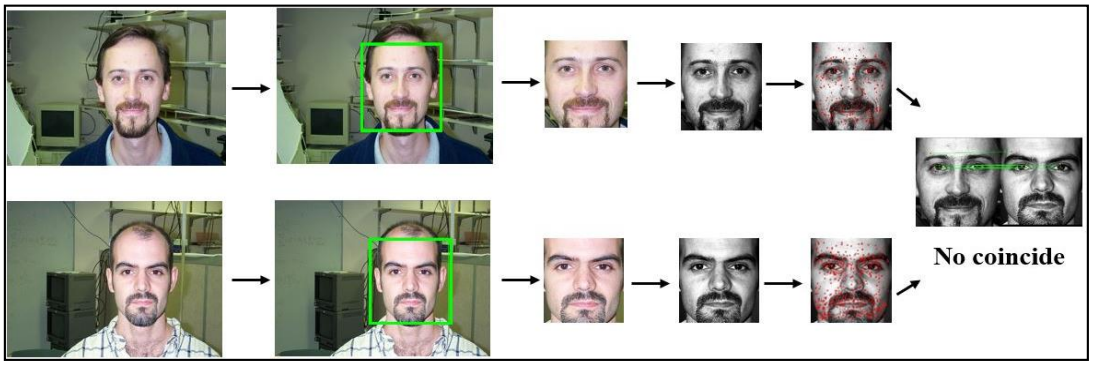


Figura 5-8 Pruebas con la base de datos Caltech Faces en imágenes diferentes.



En base a los resultados obtenidos en las pruebas anteriores, la metodología propuesta se evalúa contra los principales algoritmos de detección de características como lo son LDA, PCA, SIFT y SURF sin preprocesamiento (Mendoza-Martinez *et al.*, 2014). Estos resultados se muestran en la Tabla 5-6.

Tabla 5-6 Comparación entre LDA, PCA, SIFT Y SURF (sin preprocesamiento).

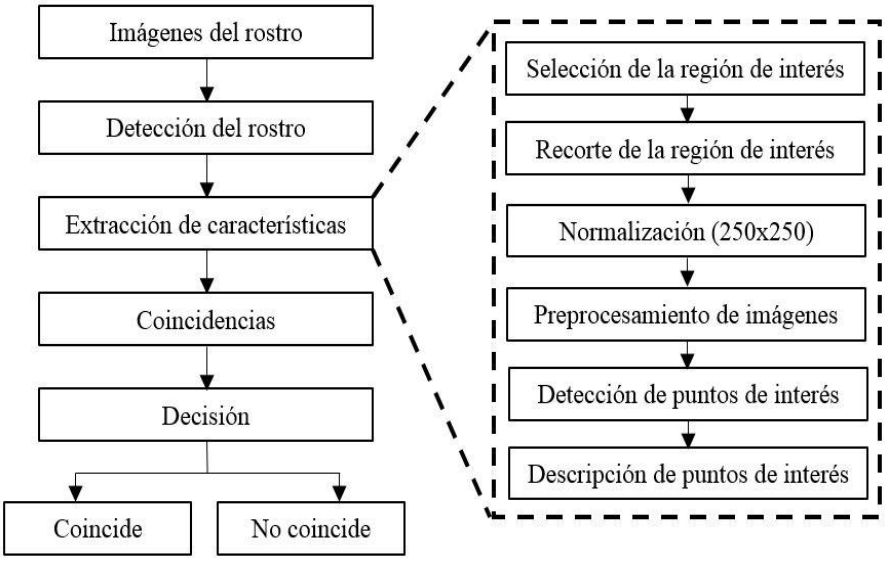
Algoritmo	Tasa de autenticación (%)
LDA	80.90 - 88.75
PCA	69.81 - 83.57
SIFT	50.14 - 83.82
SURF (sin preprocesamiento)	50.14 - 81.47
SURF (con preprocesamiento)	86.00 - 93.00

Gracias a la etapa de preprocesamiento llevada a cabo anteriormente es que se logra incrementar notablemente la tasa de autenticación en las imágenes del rostro (verdaderos positivos, TP) de un mínimo de 50.14% a 86.00% y de un máximo de 88.75% a 93.00%, esto en comparación con los algoritmos más empleados en este ámbito.

5.4. Pruebas en tarjetas de desarrollo Raspberry Pi

Una vez realizadas pruebas en computadora, se analizaron los resultados obtenidos en la sección anterior y se procedió a implementar una retroalimentación a la metodología propuesta con el fin de mejorar el proceso de autenticación facial. Para ello, se llegó a la conclusión que era necesaria una etapa de normalización de imágenes con el fin de que se trabaje bajo las mismas condiciones en ambas imágenes de entrada, esto quiere decir que cada una de ellas deberá tener la misma dimensión. La etapa de normalización se agregó dentro del proceso de extracción de características y por conveniencia se definió la dimensión de las imágenes en 250x250 pixeles. La Figura 5-9 muestra el diagrama de la metodología propuesta con la retroalimentación explicada anteriormente para tarjetas de desarrollo Raspberry Pi 2, B y B+.

Figura 5-9 Metodología propuesta para pruebas en tarjetas Raspberry Pi 2, B y B+.



En esta etapa de pruebas fue considerada la implementación del algoritmo SURF con la etapa de preprocesamiento y sin ella. Se midió el tiempo de procesamiento de esta metodología en cada tarjeta Raspberry Pi (2, B y B+) y se usaron tres bases de datos públicas, donde además de las empleadas en pruebas anteriores se incluyó la denominada FERET. Así mismo, fueron seleccionadas 40 imágenes por cada base de datos y se realizaron 20 pruebas en total. Cabe señalar que se obtuvieron los mismos resultados para cada tarjeta a excepción del tiempo de procesamiento.

Por otro lado, cada tarjeta de desarrollo Raspberry Pi cuenta con el sistema operativo Raspbian y el entorno de desarrollo integrado de Python (IDLE: Integrated DeveLopment Environment, por sus siglas en inglés), las cuales son herramientas imprescindibles para el desarrollo de las pruebas del sistema de autenticación facial. En la Figura 5-10 se muestra la interface general de Raspbian, posteriormente en la Figura 5-11 se puede apreciar la consola de Python y la versión de la librería OpenCV empleada en las pruebas realizadas.

Figura 5-10 Interface del sistema operativo Raspbian.

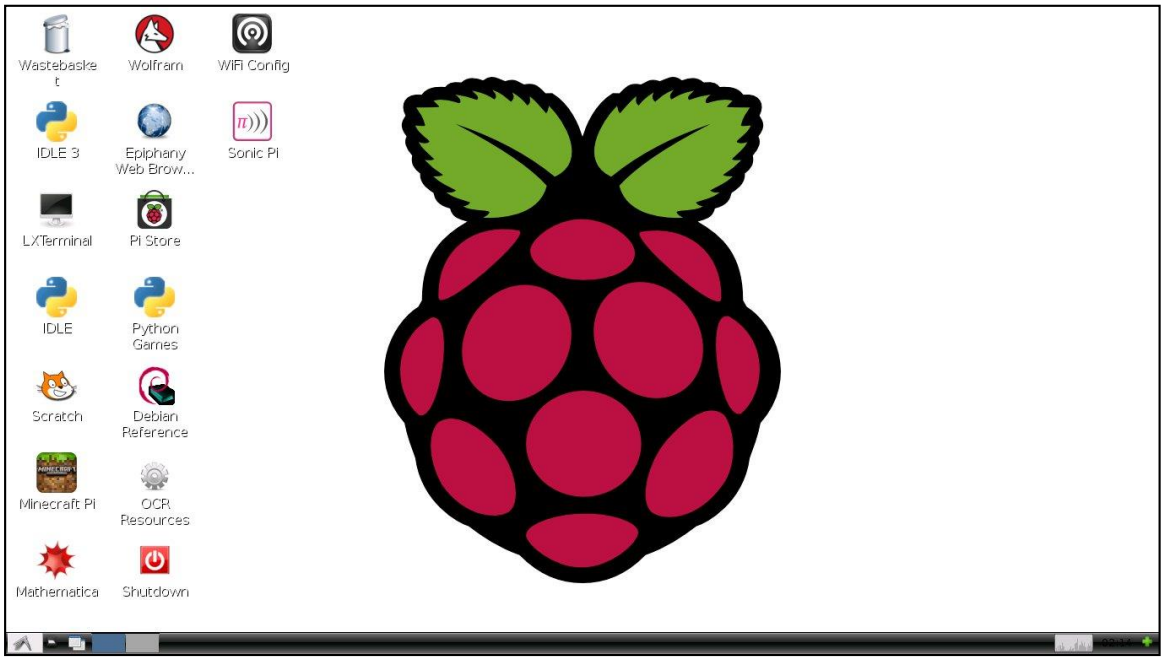
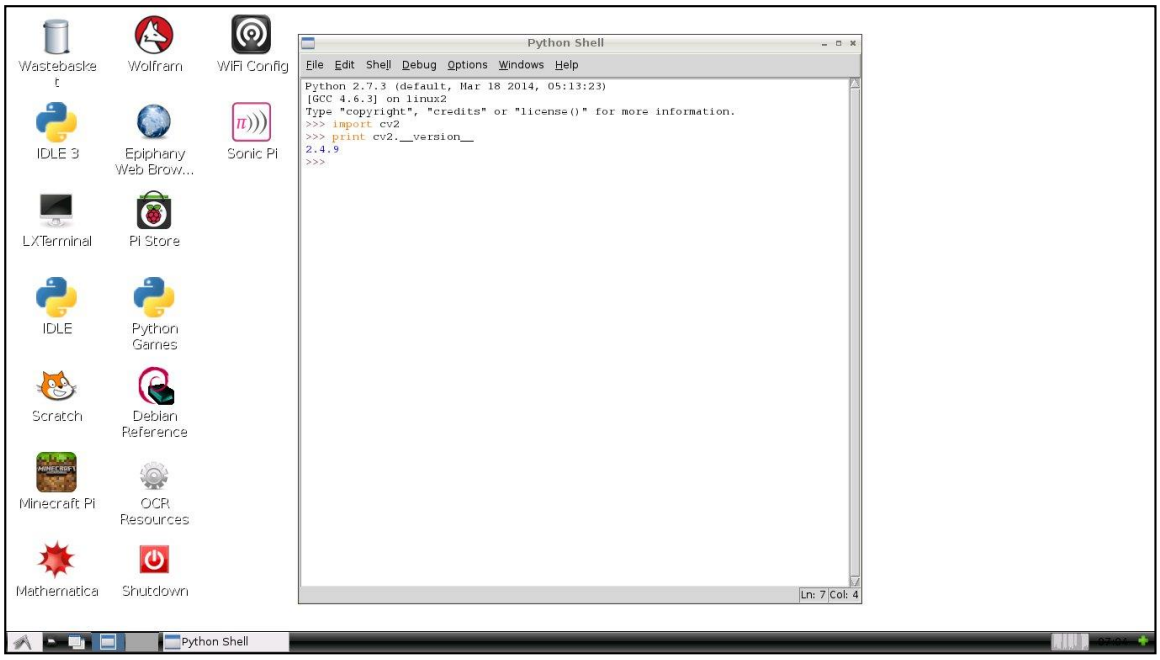


Figura 5-11 Consola de Python en Raspbian.



Siguiendo la metodología de la Figura 5-9, los primeros dos procesos (imágenes y detección del rostro) fueron exitosos al 100%.

Posteriormente se llevó a cabo la extracción de características. Las Tablas 5-7 a 5-9 presentan el resultado del número de características (puntos de interés) obtenido en cada imagen de entrada con y sin preprocesamiento además de información como:

- Prueba: número de prueba a realizar (de 1 a 20).
- Género: género de la persona que se encuentra en la imagen de prueba.
- FImg1 y 2: número de características obtenido en cada imagen de entrada.
- Promedio: promedio del número de características obtenido en cada imagen.

Tabla 5-7 Número de características entre imágenes de la base de datos CK+.

		Sin preprocesamiento		Con preprocesamiento	
Prueba	**Género**	**FImg1**	**FImg2**	**FImg1**	**FImg2**
1	Femenino	179	157	301	275
2	Femenino	187	222	272	293
3	Femenino	146	156	286	288
4	Masculino	191	212	373	391
5	Masculino	200	221	258	287
6	Masculino	172	263	454	443
7	Masculino	158	216	351	392
8	Femenino	179	197	305	346
9	Femenino	199	252	298	354
10	Femenino	167	183	237	228
11	Masculino	245	233	455	438
12	Femenino	173	173	246	315
13	Masculino	151	154	334	346
14	Femenino	176	202	270	287
15	Femenino	206	196	330	349
16	Masculino	175	212	420	391
17	Femenino	142	155	278	293
18	Femenino	179	207	302	338
19	Masculino	194	190	404	427
20	Masculino	183	210	401	414
	Promedio	**180**	**201**	**329**	**345**

Tabla 5-8 Número de características entre imágenes de la base de datos Caltech Faces.

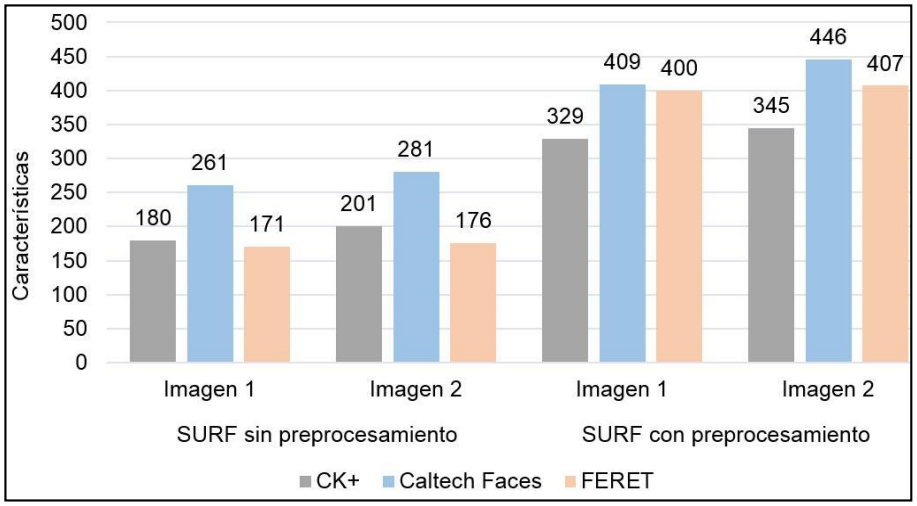
		Sin preprocesamiento		Con preprocesamiento	
Prueba	**Género**	**FImg1**	**FImg2**	**FImg1**	**FImg2**
1	Masculino	339	305	455	526
2	Masculino	203	307	531	596
3	Masculino	159	244	294	411
4	Masculino	220	283	491	545
5	Femenino	456	368	524	479
6	Masculino	351	400	436	527
7	Femenino	139	177	233	264
8	Femenino	234	247	413	516
9	Femenino	150	316	298	431
10	Femenino	298	243	469	408
11	Masculino	148	242	258	301
12	Masculino	323	343	479	523
13	Femenino	294	267	466	417
14	Femenino	282	274	408	377
15	Masculino	293	337	569	673
16	Femenino	161	151	350	398
17	Femenino	280	271	445	468
18	Masculino	309	282	378	362
19	Femenino	191	142	246	238
20	Masculino	385	416	437	467
	Promedio	**261**	**281**	**409**	**446**

Tabla 5-9 Número de características entre imágenes de la base de datos FERET.

		Sin preprocesamiento		Con preprocesamiento	
Prueba	**Género**	**FImg1**	**FImg2**	**FImg1**	**FImg2**
1	Masculino	102	032	286	354
2	Masculino	197	167	459	407
3	Masculino	256	242	547	587
4	Masculino	136	167	389	369
5	Masculino	101	246	438	423
6	Femenino	077	116	309	317
7	Femenino	120	123	280	328
8	Femenino	072	081	308	316
9	Femenino	030	042	313	321
10	Femenino	136	193	297	429
11	Masculino	192	188	374	382
12	Masculino	255	234	471	468
13	Masculino	210	255	532	509
14	Masculino	178	203	479	467
15	Masculino	234	238	520	511
16	Femenino	154	165	388	385
17	Femenino	265	203	402	374
18	Femenino	270	232	443	421
19	Femenino	198	164	356	347
20	Femenino	230	229	414	428
	Promedio	**171**	**176**	**400**	**407**

Como se puede observar en la Figura 5-12 el número de características en promedio es mayor agregando al algoritmo SURF la fase previa de preprocesamiento de imágenes que sin ella.

Figura 5-12 Características en promedio del algoritmo SURF sin y con preprocesamiento.



A continuación la Tabla 5-10 muestra el número de coincidencias para cada imagen de entrada. La primera columna de la tabla presenta el número de prueba realizado, posteriormente se indica el nombre de la base de datos donde la primera columna de esta sección es el número de coincidencias sin la fase de preprocesamiento (SP) previo a la aplicación del algoritmo SURF y la segunda columna indica los resultados agregando el preprocesamiento (CP), esta misma información se presenta para cada base de datos.

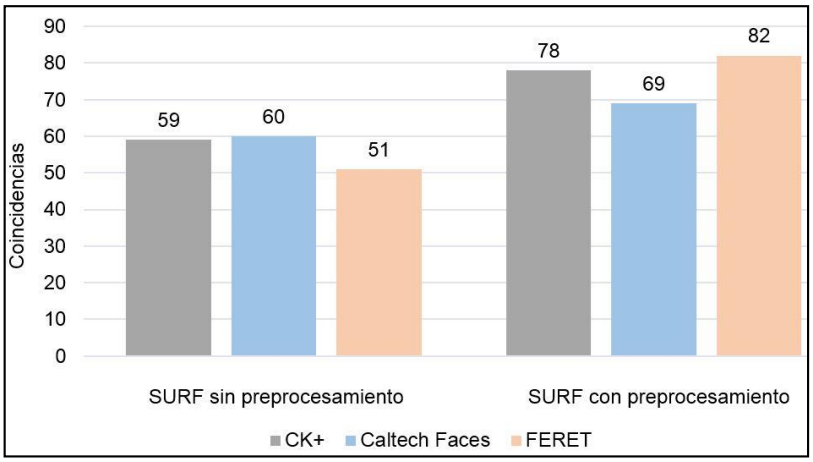
Finalmente, se presenta el promedio del número de coincidencias obtenido para cada imagen de entrada de las bases de datos (Imagen 1 y 2).

Tabla 5-10 Número de coincidencias entre imágenes de entrada de las bases de datos.

Prueba	CK+		Caltech Faces		FERET	
	SP	CP	SP	CP	SP	CP
1	074	098	070	072	011	007
2	092	102	036	032	065	126
3	047	066	043	070	065	064
4	022	043	054	057	034	049
5	051	067	052	060	005	009
6	036	032	074	079	020	043
7	057	078	055	068	022	042
8	023	032	045	040	018	031
9	050	046	027	025	006	038
10	095	097	079	104	032	025
11	127	146	042	050	081	167
12	047	048	032	045	077	108
13	084	163	071	054	095	197
14	087	112	073	078	043	058
15	051	054	060	071	149	261
16	038	071	042	082	035	045
17	060	077	101	116	068	093
18	054	086	094	094	070	094
19	060	089	074	094	074	112
20	028	056	084	087	058	067
Promedio	**059**	**078**	**060**	**069**	**051**	**082**

Como se puede observar en la Figura 5-13 el número de coincidencias en promedio es mayor agregando al algoritmo SURF la fase previa de preprocesamiento de imágenes que sin ella.

Figura 5-13 Coincidencias en promedio del algoritmo SURF sin y con preprocesamiento.



El paso final es la decisión, donde se establece si las imágenes de entrada coinciden o no. Los resultados se presentan en la Tabla 5-11 donde se muestran los verdaderos positivos (TP), falsos negativos (FN) y el porcentaje de autenticidad de las imágenes evaluadas, se consideraron sólo esos parámetros ya que en esta sección se emplearon imágenes de la misma persona en cada prueba.

Tabla 5-11 TP y FN en imágenes sin y con preprocesamiento.

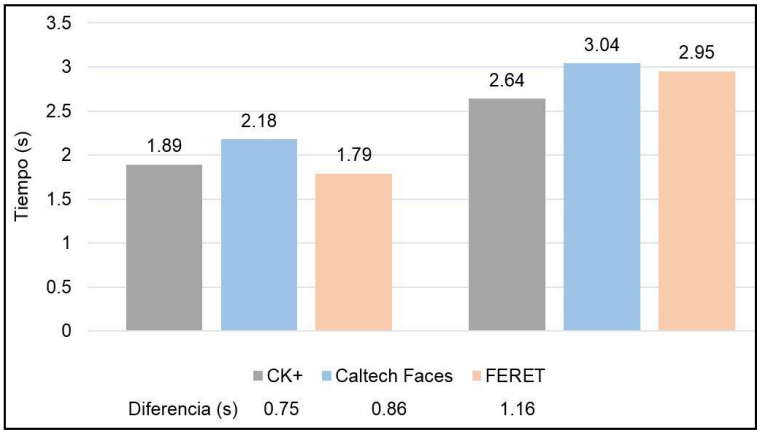
Base de datos	Sin preprocesamiento			Con preprocesamiento		
	TP	**FN**	**Autenticidad**	**TP**	**FN**	**Autenticidad**
CK+	70%	30%	70%	100%	0%	100%
Caltech Faces	95%	5%	95%	100%	0%	100%
FERET	85%	15%	85%	85%	15%	85%
		Promedio	**83.33%**		**Promedio**	**95%**

El siguiente parámetro que se evaluó fue el tiempo de procesamiento, el cual se considera en segundos (s). La Tabla 5-12 y la Figura 5-14 despliegan los resultados obtenidos con la tarjeta Raspberry Pi 2.

Tabla 5-12 Tiempo de procesamiento en la tarjeta Raspberry Pi 2.

Prueba	CK+ (s)		Caltech Faces (s)		FERET (s)	
	SP	CP	SP	CP	SP	CP
1	1.78	2.32	2.48	3.32	1.31	2.43
2	2.09	2.39	2.10	3.85	1.79	2.97
3	1.69	2.43	1.71	2.75	2.27	3.93
4	1.99	2.84	2.04	3.58	1.77	2.86
5	1.91	2.28	2.77	3.36	1.92	3.47
6	2.05	3.26	2.75	3.28	1.37	2.39
7	1.93	2.99	1.68	2.16	1.53	2.45
8	1.85	2.70	2.15	3.29	1.37	2.50
9	2.14	2.68	2.05	2.66	0.97	2.34
10	1.88	2.12	2.07	2.93	1.64	2.78
11	2.18	3.24	1.86	2.22	1.90	2.81
12	1.81	2.24	2.46	3.36	2.14	3.26
13	1.78	2.66	2.17	3.10	2.16	3.70
14	1.78	2.18	2.17	2.87	2.03	3.19
15	1.90	2.61	2.51	4.16	2.06	3.65
16	1.86	3.01	1.66	2.77	1.68	2.72
17	1.71	2.50	2.26	3.24	2.05	2.89
18	1.88	2.54	2.29	2.73	2.13	3.09
19	1.90	2.91	1.69	2.16	1.76	2.66
20	1.86	2.94	2.91	3.10	2.08	2.98
Promedio	**1.89**	**2.64**	**2.18**	**3.04**	**1.79**	**2.95**

Figura 5-14 Tiempo de procesamiento en promedio (Raspberry Pi 2).



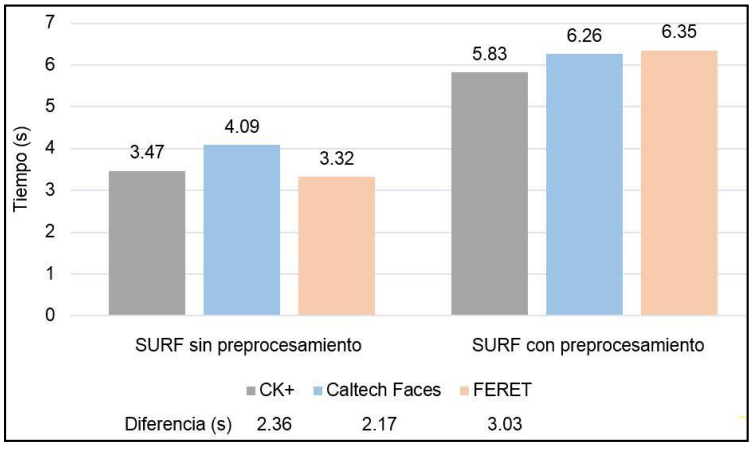
La Tabla 5-13 despliega los resultados obtenidos con la tarjeta Raspberry Pi B considerando las imágenes de entrada de las bases de datos sin y con

preprocesamiento previo a la aplicación del algoritmo SURF. Además, el tiempo de procesamiento en promedio es presentado en la Figura 5-15.

Tabla 5-13 Tiempo de procesamiento en la tarjeta Raspberry Pi B.

Prueba	CK+ (s)		Caltech Faces (s)		FERET (s)	
	SP	CP	SP	CP	SP	CP
1	3.21	5.24	5.26	6.35	2.44	5.43
2	3.72	5.42	4.02	7.05	3.33	6.52
3	3.09	5.42	3.16	4.97	4.11	7.49
4	3.59	6.30	3.79	6.65	3.17	6.27
5	3.53	5.16	5.13	6.16	3.38	7.24
6	3.68	7.06	4.95	6.07	2.58	5.29
7	3.42	6.49	3.00	4.07	2.93	5.65
8	3.40	5.83	3.91	7.11	2.71	5.53
9	3.90	5.76	3.66	5.97	1.85	5.38
10	3.55	5.01	3.86	6.55	3.16	5.88
11	4.11	7.20	3.42	5.08	3.54	6.30
12	3.23	5.25	4.46	7.23	3.95	7.03
13	3.18	5.86	4.09	5.52	4.13	7.66
14	3.38	5.06	4.08	6.29	3.57	7.03
15	3.42	4.96	4.70	8.99	3.65	7.63
16	3.44	6.45	2.97	6.35	3.06	6.10
17	3.15	5.55	4.28	6.93	3.74	6.33
18	3.53	5.70	4.22	5.86	4.00	6.85
19	3.47	6.51	3.27	5.09	3.26	4.91
20	3.41	6.47	5.51	6.79	3.87	6.57
Promedio	**3.47**	**5.83**	**4.09**	**6.26**	**3.32**	**6.35**

Figura 5-15 Tiempo de procesamiento en promedio (Raspberry Pi B).

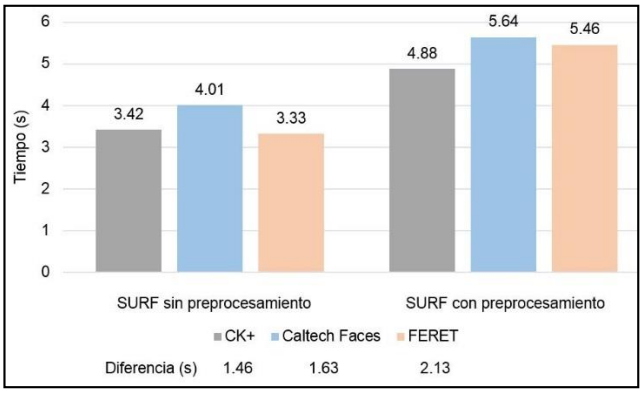


La Tabla 5-14 despliega los resultados obtenidos con la tarjeta Raspberry Pi B+ considerando las imágenes de entrada de las bases de datos sin y con preprocesamiento previo a la aplicación del algoritmo SURF. Además, el tiempo de procesamiento en promedio es presentado en la Figura 5-16.

Tabla 5-14 Tiempo de procesamiento en la tarjeta Raspberry Pi B+.

Prueba	CK+ (s)		Caltech Faces (s)		FERET (s)	
	SP	CP	SP	CP	SP	CP
1	3.17	4.40	4.42	7.55	2.48	4.44
2	3.61	4.62	3.99	6.86	3.18	5.52
3	3.06	4.38	3.16	4.89	4.11	7.23
4	3.59	5.31	3.66	6.54	3.24	5.15
5	3.52	4.13	4.99	6.11	3.32	6.65
6	3.64	6.08	4.87	5.85	2.53	4.30
7	3.36	5.32	2.97	4.06	2.90	4.41
8	3.22	4.64	3.81	5.93	2.56	4.65
9	3.72	4.92	3.68	4.90	1.91	4.38
10	3.43	4.02	3.77	5.52	3.11	5.34
11	3.97	6.15	3.35	4.08	3.50	5.41
12	3.25	4.43	4.83	6.23	3.83	6.03
13	3.23	4.91	4.04	5.61	4.06	7.10
14	3.38	4.06	4.00	5.16	4.03	5.71
15	3.42	4.72	4.57	7.99	4.00	6.47
16	3.43	5.41	3.08	5.00	3.02	5.06
17	3.10	4.48	4.20	5.87	3.75	5.34
18	3.48	4.70	4.27	4.85	3.98	5.77
19	3.45	5.58	3.09	4.02	3.34	4.77
20	3.30	5.31	5.41	5.82	3.79	5.49
Promedio	**3.42**	**4.88**	**4.01**	**5.64**	**3.33**	**5.46**

Figura 5-16 Tiempo de procesamiento en promedio (Raspberry Pi B+).



De acuerdo a los resultados mostrados en las Figuras 5-14, 5-15 y 5-16, la menor diferencia promedio en tiempo de procesamiento entre las tarjetas de desarrollo Raspberry Pi se puede apreciar en la Tabla 5-15, con lo cual se comprueba que la tarjeta que presenta un mejor desempeño es la Raspberry Pi 2.

Tabla 5-15 Diferencia en tiempo promedio de procesamiento entre las tarjetas Raspberry Pi.

Tiempo (s)	CK+	Caltech Faces	FERET
Raspberry Pi 2	0.75	0.86	1.16
Raspberry Pi B+	1.46	1.63	2.13
Raspberry Pi B	2.36	2.17	3.03

En la Figura 5-17 se puede observar el resultado de la ejecución de la metodología propuesta en las tarjetas de desarrollo Raspberry Pi 2, B y B+, donde se implementa la fase de preprocesamiento a las imágenes de entrada, además se incluye el número de coincidencias por ejecución. Así mismo, en la Figura 5-18 se presenta el resultado obtenido pero sin dicha fase y con las mismas imágenes empleadas en la Figura 5-17. Cabe señalar que para estas pruebas se toma como referencia la base de datos FERET.

Figura 5-17 Pruebas realizadas con la fase de preprocesamiento.

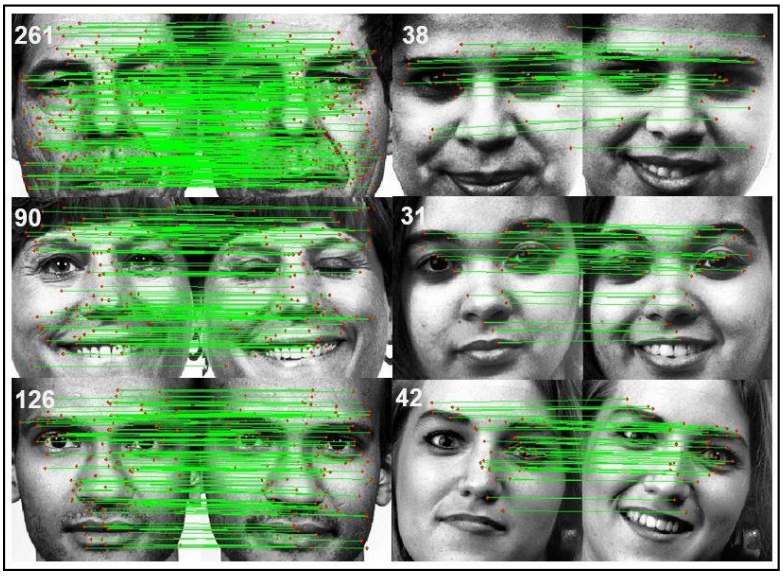
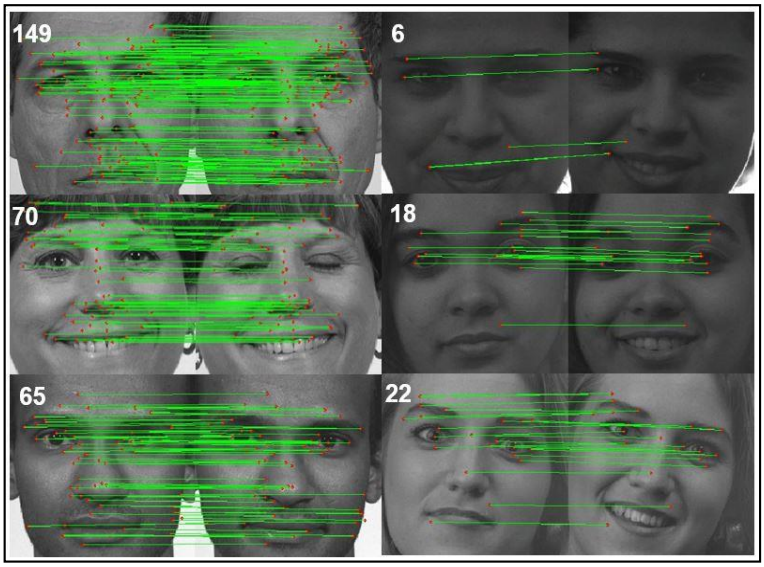


Figura 5-18 Pruebas realizadas sin la fase de preprocesamiento.



A continuación, las Figuras 5-19 a 5-21 muestran la ejecución de la metodología propuesta en esta sección para cada tarjeta de desarrollo. Cabe señalar que se emplea la misma imagen en cada prueba. Además, la computadora que se observa a la derecha de cada figura, se utiliza como fuente de alimentación para las Raspberry Pi.

Figura 5-19 Metodología propuesta ejecutada en la Raspberry Pi 2.

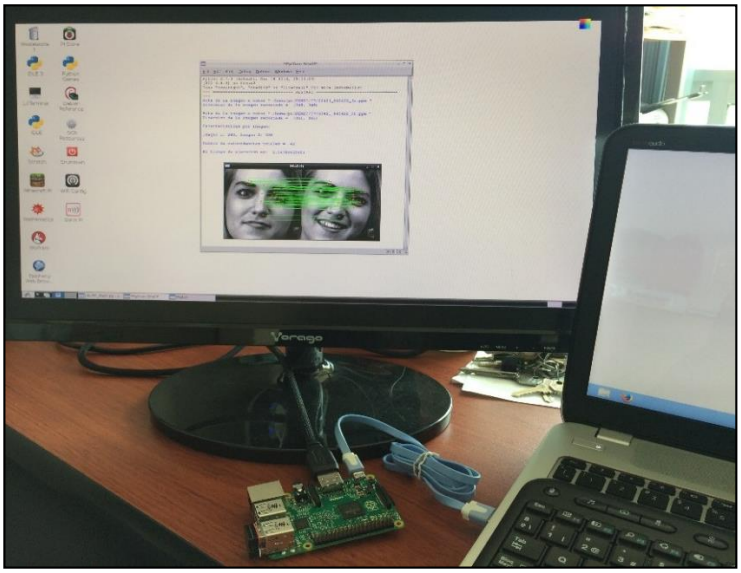


Figura 5-20 Metodología propuesta ejecutada en la Raspberry Pi B.

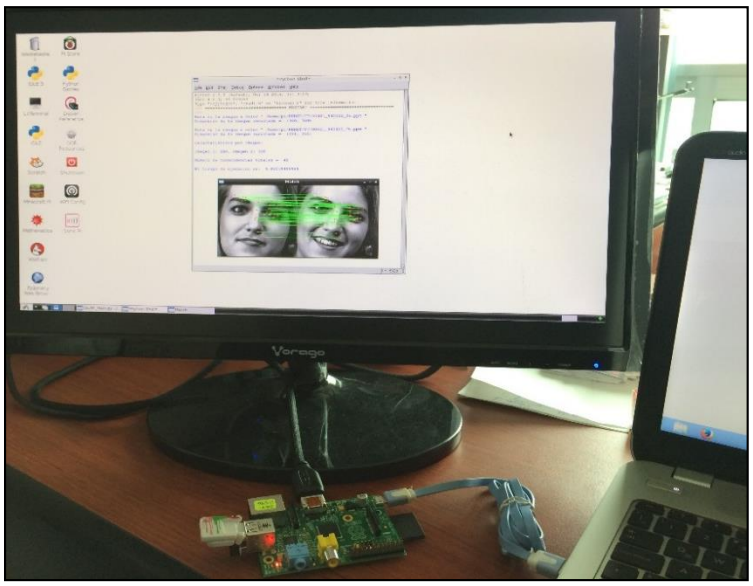
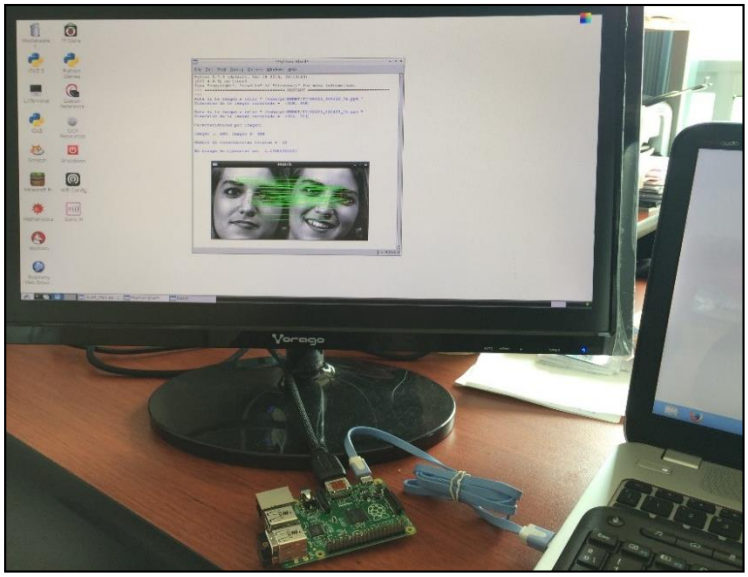
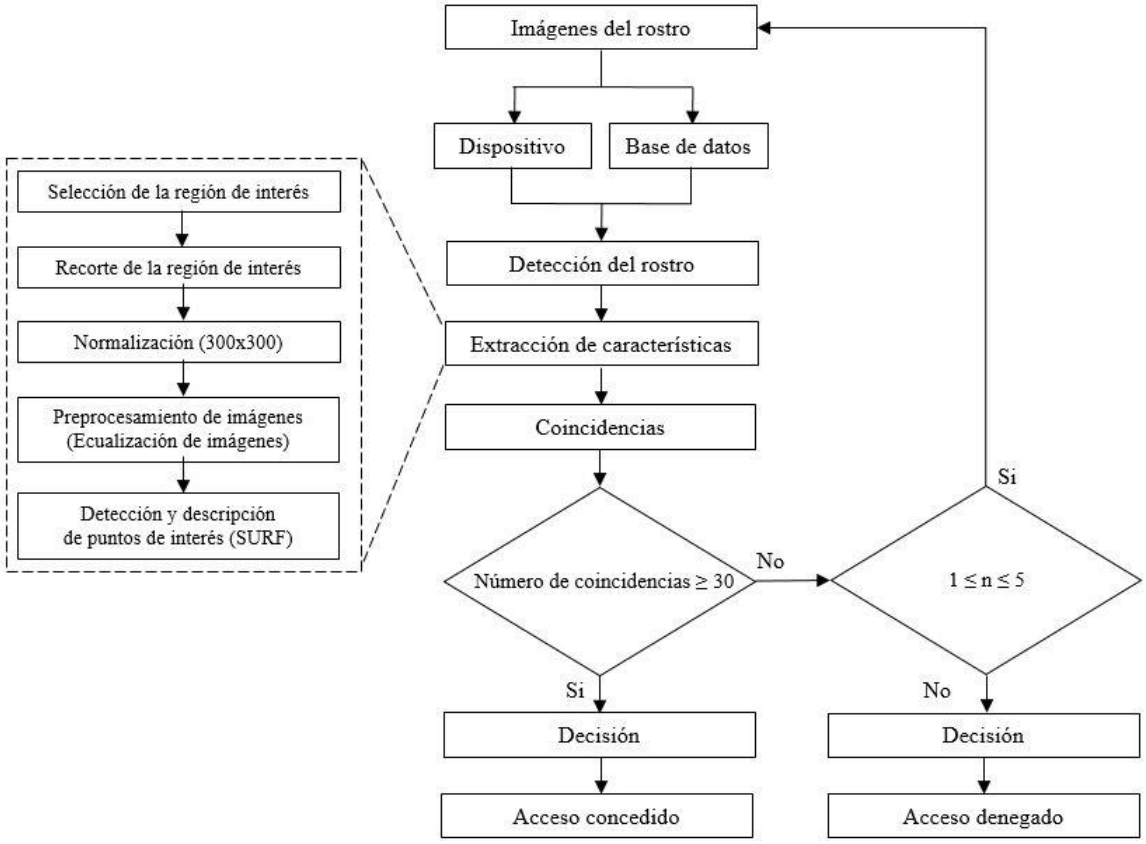


Figura 5-21 Metodología propuesta ejecutada en la Raspberry Pi B+.



Posteriormente, se realizó una variación en la metodología propuesta anteriormente, ya que se implementó una cámara web como medio de adquisición de imágenes además del uso de la base de datos propia SURFace y la tarjeta Raspberry Pi 2. En este caso, el diagrama de la metodología propuesta para la tarjeta Raspberry Pi 2 es el presentado en la Figura 5-22.

Figura 5-22 Metodología propuesta con cámara web para la Raspberry Pi 2.



A continuación, las Tablas 5-16 y 5-17 despliegan el resultado de dichas pruebas, donde se puede apreciar información tal como:

- Prueba: número de prueba realizada.
- CTImgE: número de características de la imagen de la cámara.
- CPImgBD: número de características en promedio de las imágenes de la base de datos.
- NComps: número de comparaciones que realiza el sistema con las imágenes de la base de datos (pueden ser de 1-5 comparaciones).
- CImgs: número de coincidencias entre las imágenes de entrada.
- Tiempo: segundos que tarda el sistema en autenticar a un usuario.
- AImgs: resultado del proceso de autenticar al usuario (exitosa o errónea).

Tabla 5-16 Metodología propuesta implementada en la Raspberry Pi 2 (parte 1).

Prueba	CTImgE	CPImgBD	NComps	CImgs	Tiempo	AImgs
1	497	544	1	28	08.85	Exitosa
2	529	565	1	42	08.42	Exitosa
3	481	543	5	9	33.53	Errónea
4	573	563	3	21	20.56	Exitosa
5	592	540	1	23	08.35	Exitosa
6	523	536	1	74	07.98	Exitosa
7	502	497	2	24	14.61	Exitosa
8	500	484	5	13	31.25	Errónea
9	454	495	2	25	13.86	Exitosa
10	509	486	1	79	07.66	Exitosa
11	567	486	1	22	08.25	Exitosa
12	550	527	1	29	08.48	Exitosa
13	536	527	1	35	08.45	Exitosa
14	490	527	1	24	08.03	Exitosa
15	460	525	2	23	13.89	Exitosa
16	427	527	1	20	08.08	Exitosa
17	457	515	5	11	29.96	Errónea
18	509	514	1	27	08.10	Exitosa
19	480	480	1	49	09.09	Exitosa
20	492	501	1	48	10.01	Exitosa
21	530	488	1	29	08.88	Exitosa
22	539	488	1	25	08.91	Exitosa
23	520	488	1	22	08.68	Exitosa
24	519	516	1	29	08.49	Exitosa
25	639	488	1	21	08.58	Exitosa

Tabla 5-17 Metodología propuesta implementada en la Raspberry Pi 2 (parte 2).

Prueba	CTImgE	CPImgBD	NComps	CImgs	Tiempo	AImgs
26	623	488	1	040	08.84	Exitosa
27	509	571	1	061	08.17	Exitosa
28	510	504	1	092	08.36	Exitosa
29	504	494	1	049	08.17	Exitosa
30	532	505	1	026	08.37	Exitosa
31	443	524	1	032	08.13	Exitosa
32	514	524	1	113	08.46	Exitosa
33	495	565	3	026	20.36	Exitosa
34	531	558	5	008	32.89	Errónea
35	509	582	5	009	40.22	Errónea
36	584	570	1	022	08.64	Exitosa
37	443	479	1	130	08.50	Exitosa
38	461	458	1	060	08.46	Exitosa
39	574	513	1	057	08.43	Exitosa
40	471	550	1	070	08.40	Exitosa
41	553	589	1	119	09.07	Exitosa
42	510	530	1	029	08.91	Exitosa
43	604	525	2	036	15.59	Exitosa
44	535	483	1	060	08.65	Exitosa
45	449	493	2	035	14.01	Exitosa
46	560	572	3	036	19.93	Exitosa
47	498	572	3	054	19.85	Exitosa
48	560	547	1	062	08.35	Exitosa
49	649	547	1	038	08.87	Exitosa
50	455	462	1	083	08.44	Exitosa

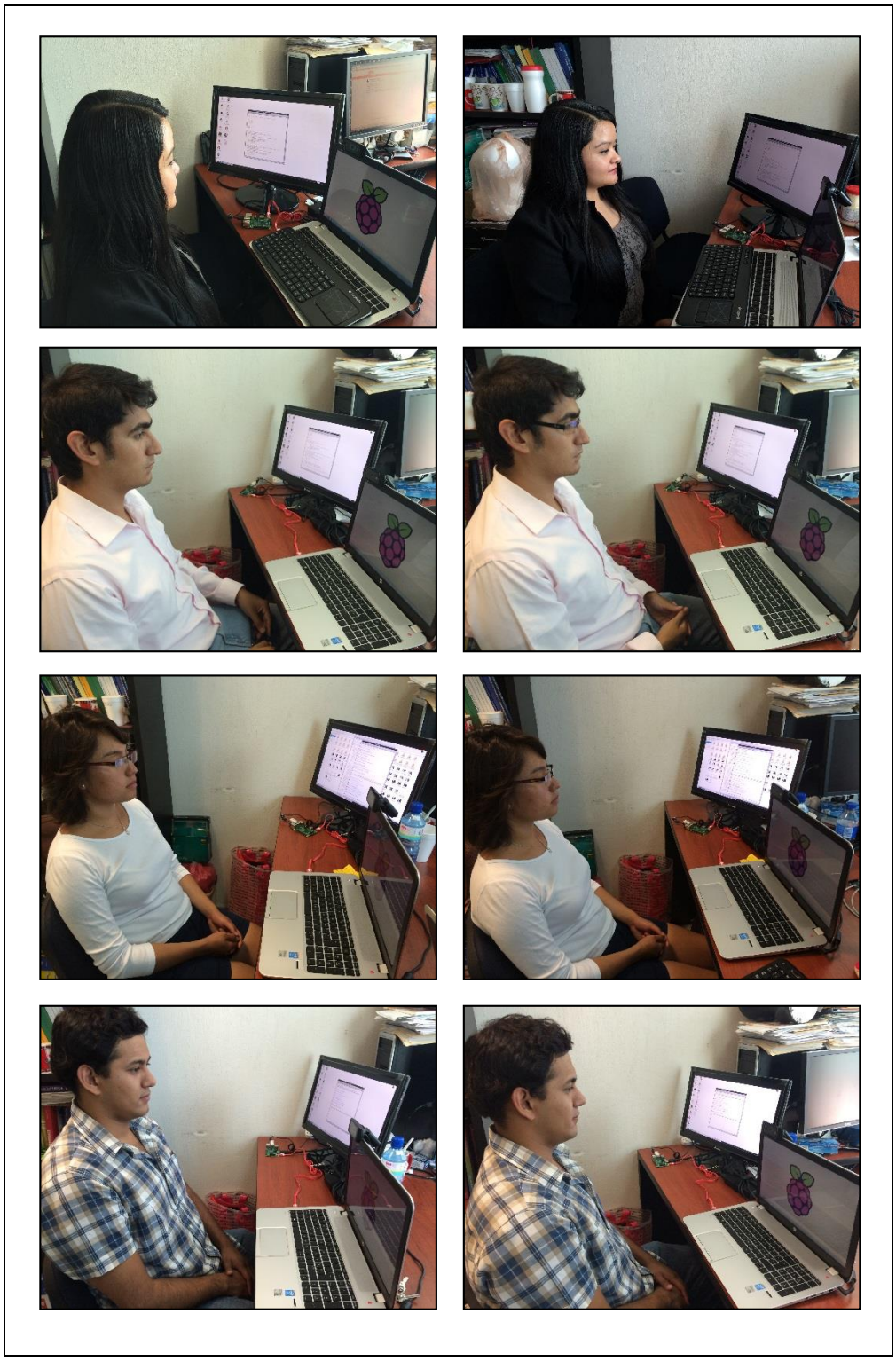
Dados los resultados de las Tablas 5-16 y 5-17, el porcentaje de autenticidad de la metodología propuesta se presenta en la Tabla 5-18 considerando los resultados verdaderos positivos (TP) y falsos negativos (FN).

Tabla 5-18 TP y FN de la metodología propuesta implementada en la Raspberry Pi 2.

Base de datos	TP	FN	Autenticidad
SURFace	90%	10%	90%

A continuación, la Figura 5-23 muestra la ejecución de la metodología propuesta implementada en la tarjeta de desarrollo Raspberry Pi 2.

Figura 5-23 Metodología propuesta implementada en la Raspberry Pi 2.



La siguiente sección presenta un estudio realizado para determinar el rango de aceptación del sistema de autenticación facial empleando la tarjeta de desarrollo Raspberry Pi 2, para ello se consideran diferentes distancias entre la cámara web y el rostro de la persona (las cuales se miden en centímetros, cm). La Tabla 5-19 muestra el resultado obtenido de este análisis, donde:

Distancia cámara – rostro: distancia de prueba en centímetros (cm).

Prueba: número de prueba realizado.

- \- Autenticación errónea.
- \+ Autenticación exitosa.
- x No se realizó prueba.
- ⬚ Rango de aceptación del sistema.

Tabla 5-19 Pruebas con distancia máxima y mínima en Raspberry Pi 2.

Distancia cámara – rostro (cm)	Resultado de la autenticación			
	Prueba 1	Prueba 2	Prueba 3	Prueba 4
20	-	-	-	x
25	+	-	+	x
30	+	+	+	+
40	+	+	+	x
50	+	+	+	+
60	+	+	+	+
70	+	+	+	+
80	-	+	+	x
90	-	+	+	+
100	-	-	+	x
110	-	-	-	x
120	-	+	-	x
130	-	-	-	x
140	-	-	-	x

De las pruebas realizadas, se pudo comprobar experimentalmente que el rango confiable para llevar a cabo las pruebas de autenticación facial es a una distancia entre la cámara y el rostro de 30 y 70 cm. A continuación, la Figura 5-24 muestra algunas de las diferentes imágenes empleadas en este estudio, las cuales fueron tomadas con diferente distancia entre la cámara web y el rostro.

Figura 5-24 Diferente distancia entre la cámara web y el rostro.

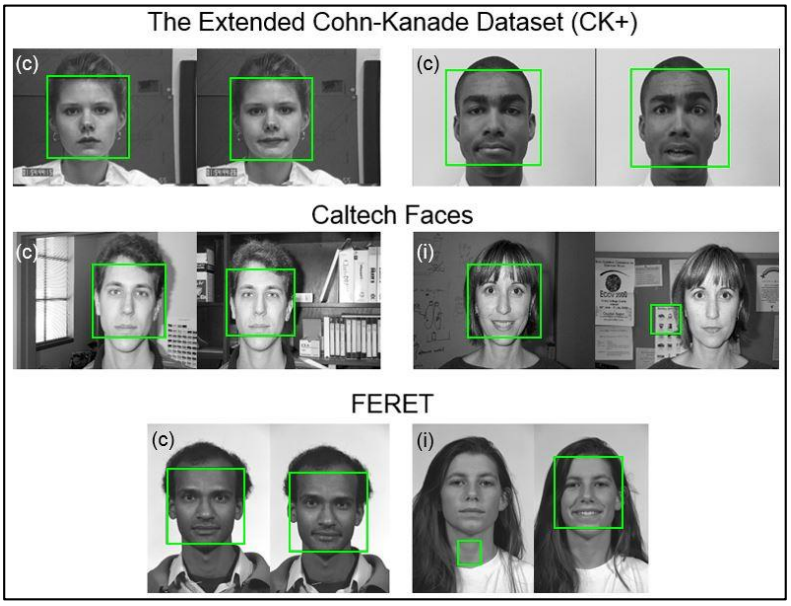
5.5. Pruebas en dispositivos móviles

Empleando el diagrama de la metodología propuesta en la Figura 4-2 se migró la implementación de Python a JAVA y C++ para la realización de diferentes pruebas en dispositivos móviles, donde en conjunto con Eclipse se instaló la aplicación de autenticación facial en cada uno de ellos, de esta manera todo el procesamiento se realiza de forma independiente en cada dispositivo. El Anexo II muestra la selección del dispositivo y su versión de Android. A continuación se presentan los resultados de dicha metodología usando las bases de datos públicas The Extended Cohn-Kanade Dataset (CK+), Caltech Faces y FERET en las Tablets Samsung Galaxy Tab 4 y Note 10.1.

Imágenes del rostro: Se seleccionaron las mismas 40 imágenes de cada base de datos que habían sido empleadas en pruebas anteriores, las cuales fueron usadas en escala de grises y normalizadas a 320x240 pixeles.

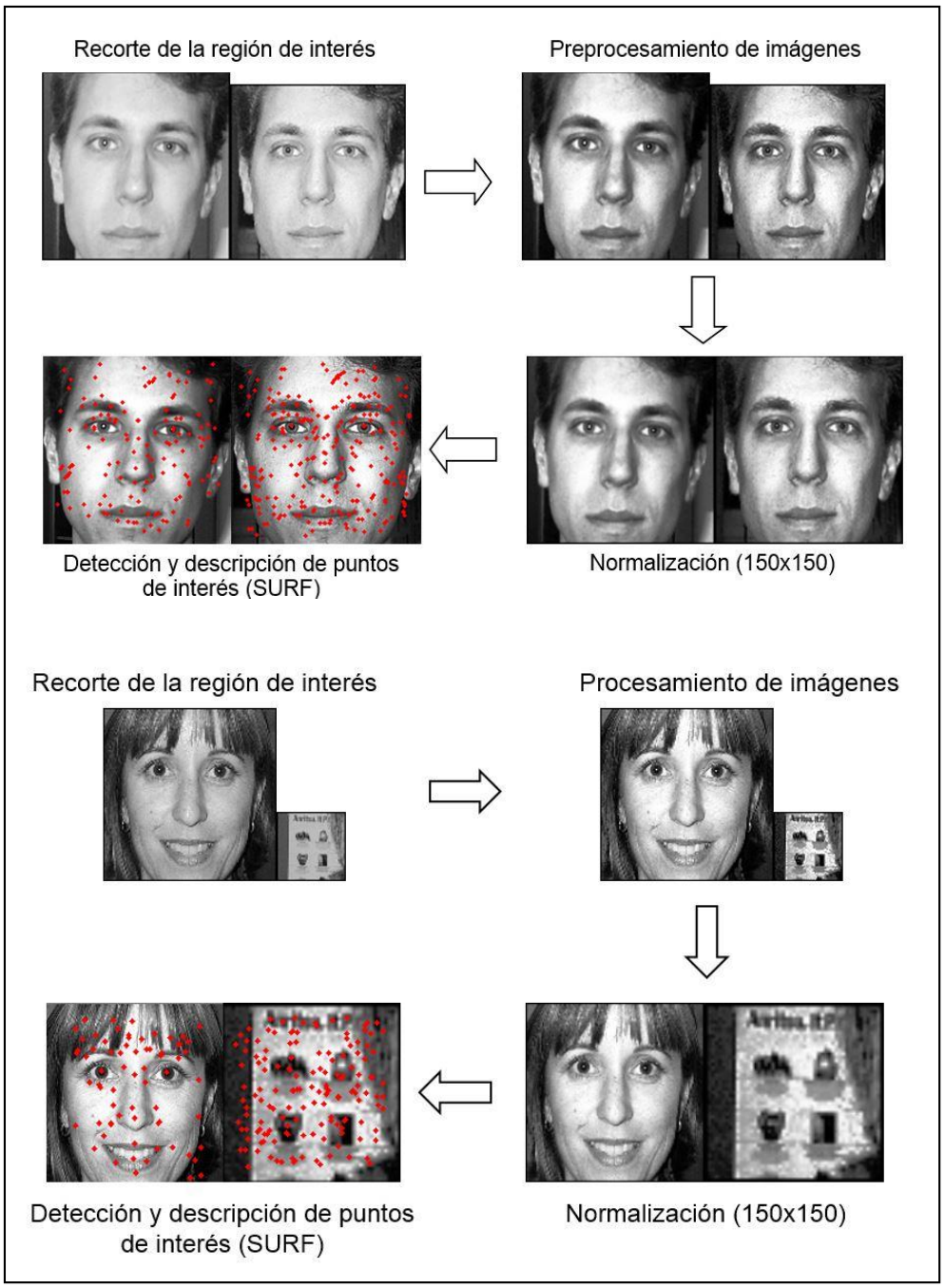
Detección del rostro: La Figura 5-25 presenta algunos de los rostros que fueron detectados correcta (95%) e incorrectamente (5%). En ambos dispositivos se obtuvieron los mismos resultados de este proceso.

Figura 5-25 Detección del rostro correcta (C) e incorrecta (I).



Extracción de características: La Figura 5-26 muestra un ejemplo del proceso de extracción de características en las imágenes de entrada, la cual se considera desde el recorte de la región de interés hasta la detección y descripción de puntos de interés tanto para una detección de rostro correcta como incorrecta.

Figura 5-26 Extracción de características en dispositivos móviles (parte 1).



La Tabla 5-20 despliega los resultados obtenidos en este proceso además del número de características en promedio por cada base de datos. Cabe resaltar que se adquirieron los mismos resultados en ambos dispositivos.

Tabla 5-20 Número de características en dispositivos móviles (parte 1).

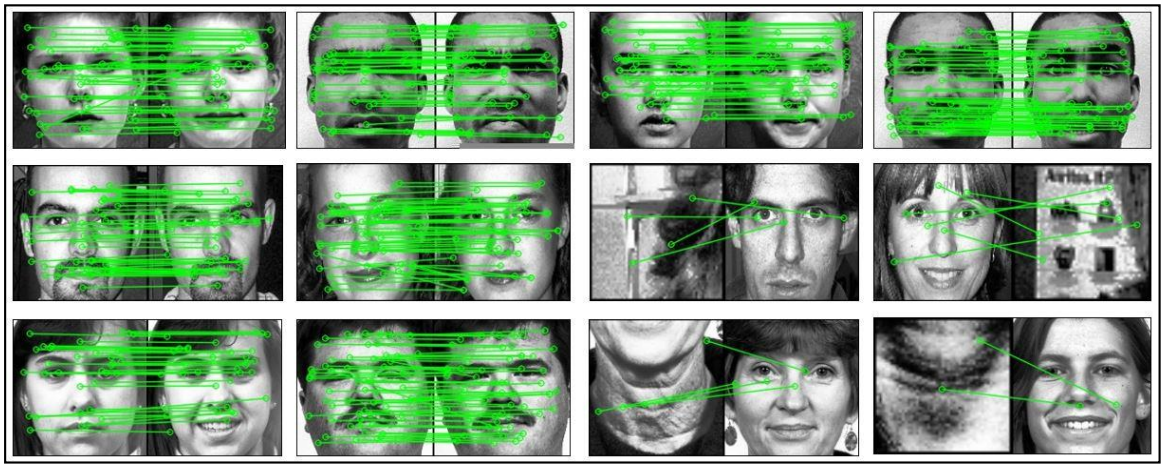
	CK+		Caltech Faces		FERET	
Prueba	**FImg1**	**FImg2**	**FImg1**	**FImg2**	**FImg1**	**FImg2**
1	103	107	125	122	110	114
2	121	104	129	129	142	134
3	091	107	93	113	144	152
4	110	142	125	136	113	130
5	111	105	137	126	121	127
6	127	129	112	137	101	094
7	106	120	111	107	113	106
8	125	124	130	120	107	092
9	115	107	102	088	099	092
10	086	080	119	115	112	130
11	120	140	098	110	104	106
12	103	098	128	134	139	130
13	093	094	130	120	138	134
14	102	097	115	123	125	111
15	119	116	132	154	141	142
16	134	142	100	105	099	114
17	111	106	129	132	125	130
18	119	117	133	112	125	117
19	124	115	111	099	116	096
20	117	137	128	114	108	106
Promedio	**111**	**114**	**119**	**119**	**119**	**117**

Coincidencias: La Tabla 5-21 presenta los resultados obtenidos en este proceso además del número de coincidencias en promedio por cada base de datos. Estos resultados fueron los mismos en ambos dispositivos. Por otro lado, la Figura 5-27 despliega algunos de los resultados tanto exitosos como erróneos del proceso de autenticación facial en las imágenes de las bases de datos The Extended Cohn-Kanade Dataset (CK+), Caltech Faces y FERET, respectivamente.

Tabla 5-21 Número de coincidencias en dispositivos móviles (parte 1).

Prueba	CK+	Caltech Faces	FERET
1	49	31	16
2	62	16	63
3	40	37	51
4	44	37	44
5	45	06	15
6	32	21	33
7	59	08	34
8	31	39	29
9	61	07	31
10	49	05	02
11	78	33	63
12	49	04	57
13	65	31	89
14	55	51	57
15	62	37	97
16	62	31	33
17	65	39	04
18	71	06	54
19	47	53	54
20	51	41	35
Promedio	**53**	**26**	**43**

Figura 5-27 Autenticación facial exitosa y errónea en dispositivos móviles (parte 1).



Decisión: Los resultados se presentan en la Tabla 5-22 donde se muestran los verdaderos positivos (TP), falsos negativos (FN) y el porcentaje de autenticidad de las imágenes evaluadas, con el cual se determina si esta fue exitosa o errónea. Estos resultados fueron los mismos para ambos dispositivos.

Tabla 5-22 TP y FN en imágenes evaluadas en dispositivos móviles (parte 1).

Base de datos	TP	FN	Autenticidad
CK+	100%	0%	100%
Caltech Faces	60%	40%	60%
FERET	75%	25%	75%
Promedio	78%	22%	78%

En las Figuras 5-28 a 5-31 se puede observar el ícono de la aplicación de autenticación facial y la pantalla principal, así como un ejemplo de la implementación de la metodología propuesta, la cual fue ejecutada en las Tablets Samsung Galaxy Tab 4 y Galaxy Note 10.1, respectivamente.

Figura 5-28 Autenticación facial en Tablet Samsung Galaxy Tab 4.

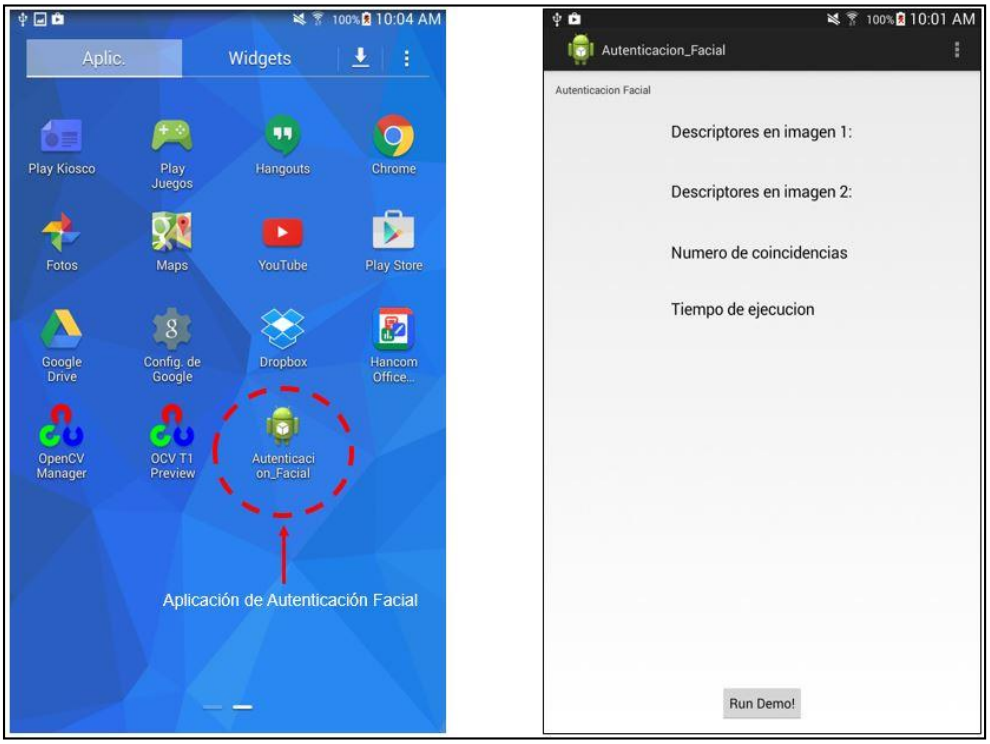


Figura 5-29 Autenticación facial en Tablet Samsung Galaxy Note 10.1

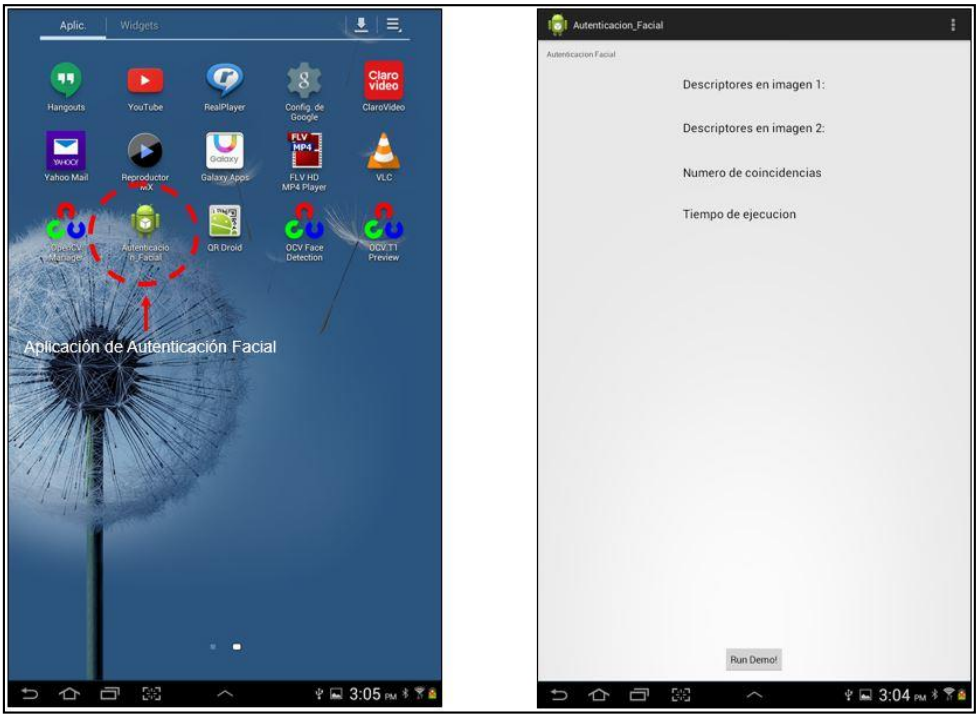
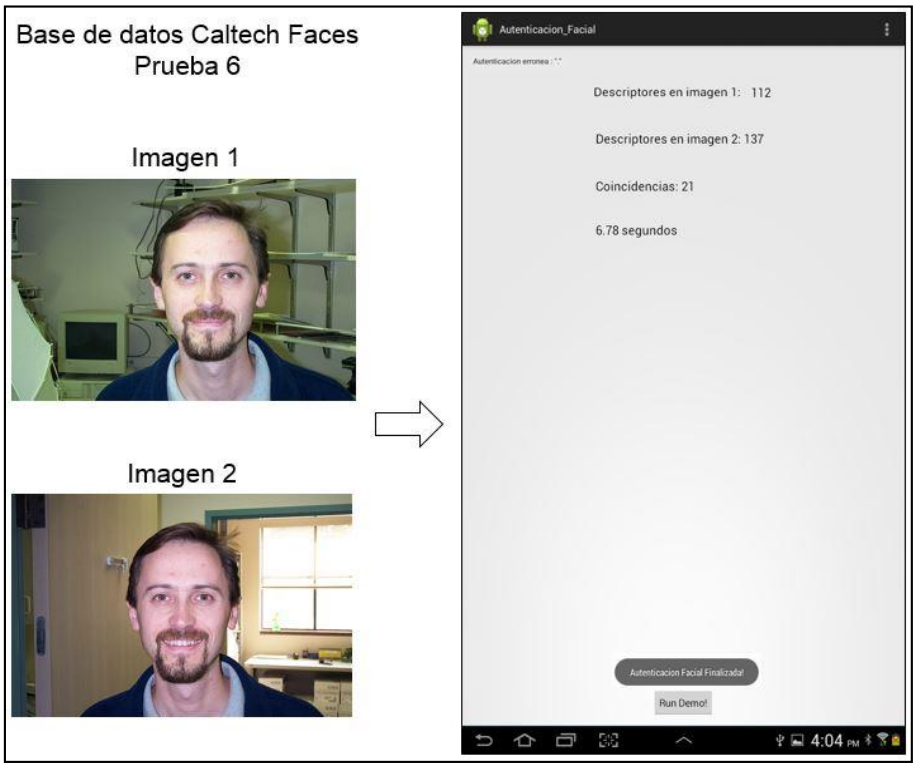


Figura 5-30 Ejemplo de autenticación facial en Tablet Samsung Galaxy Tab 4.

Figura 5-31 Ejemplo de autenticación facial en Tablet Samsung Galaxy Note 10.1

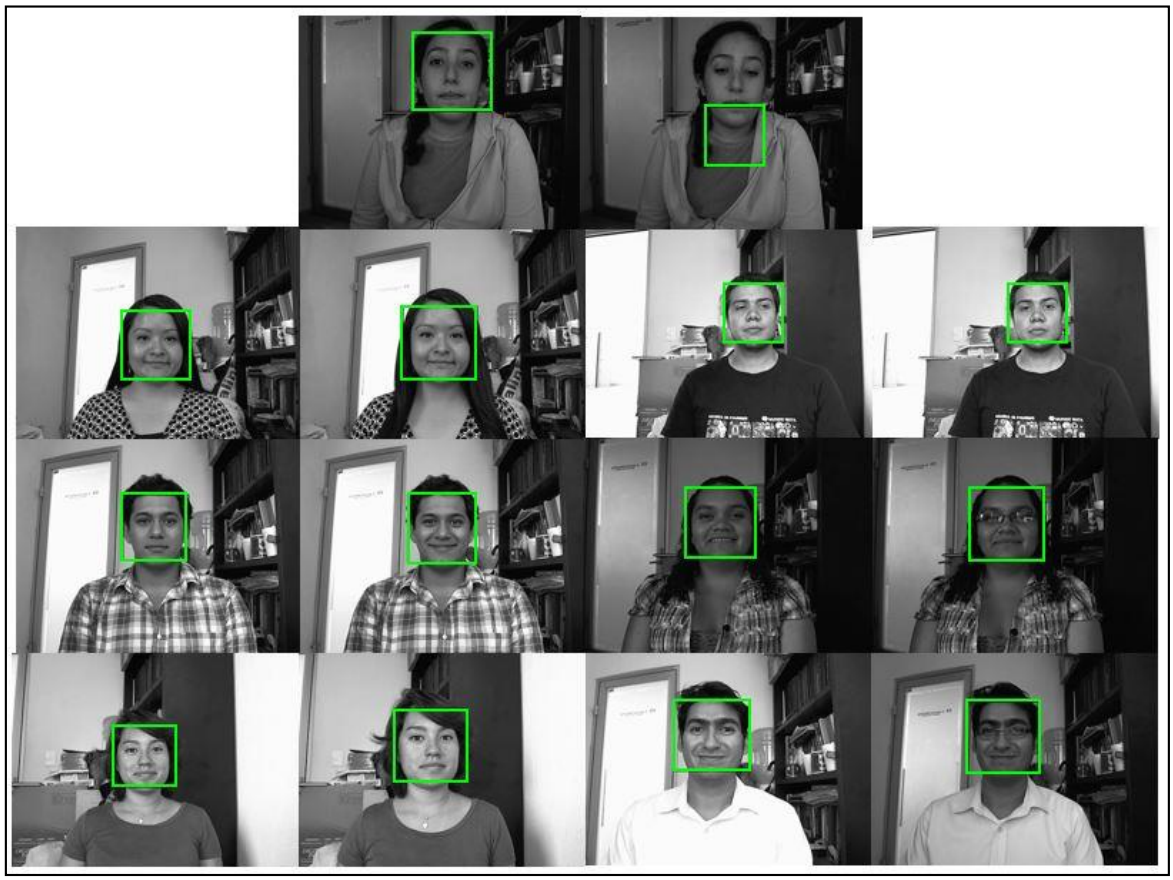


Posteriormente, se llevaron a cabo un conjunto de pruebas donde la metodología propuesta se ejecutó en cada uno de los seis dispositivos móviles y además se midió su tiempo de ejecución. A continuación se describen los resultados obtenidos en cada proceso.

Imágenes del rostro: Empleando la base de datos propia SURFace, se seleccionaron al azar dos imágenes de cada voluntario realizándose de dos a siete pruebas por cada uno de ellos, de esta manera se obtuvo un total de 70 pruebas de autenticación facial las cuales posteriormente fueron normalizadas a una resolución de 320x240 pixeles.

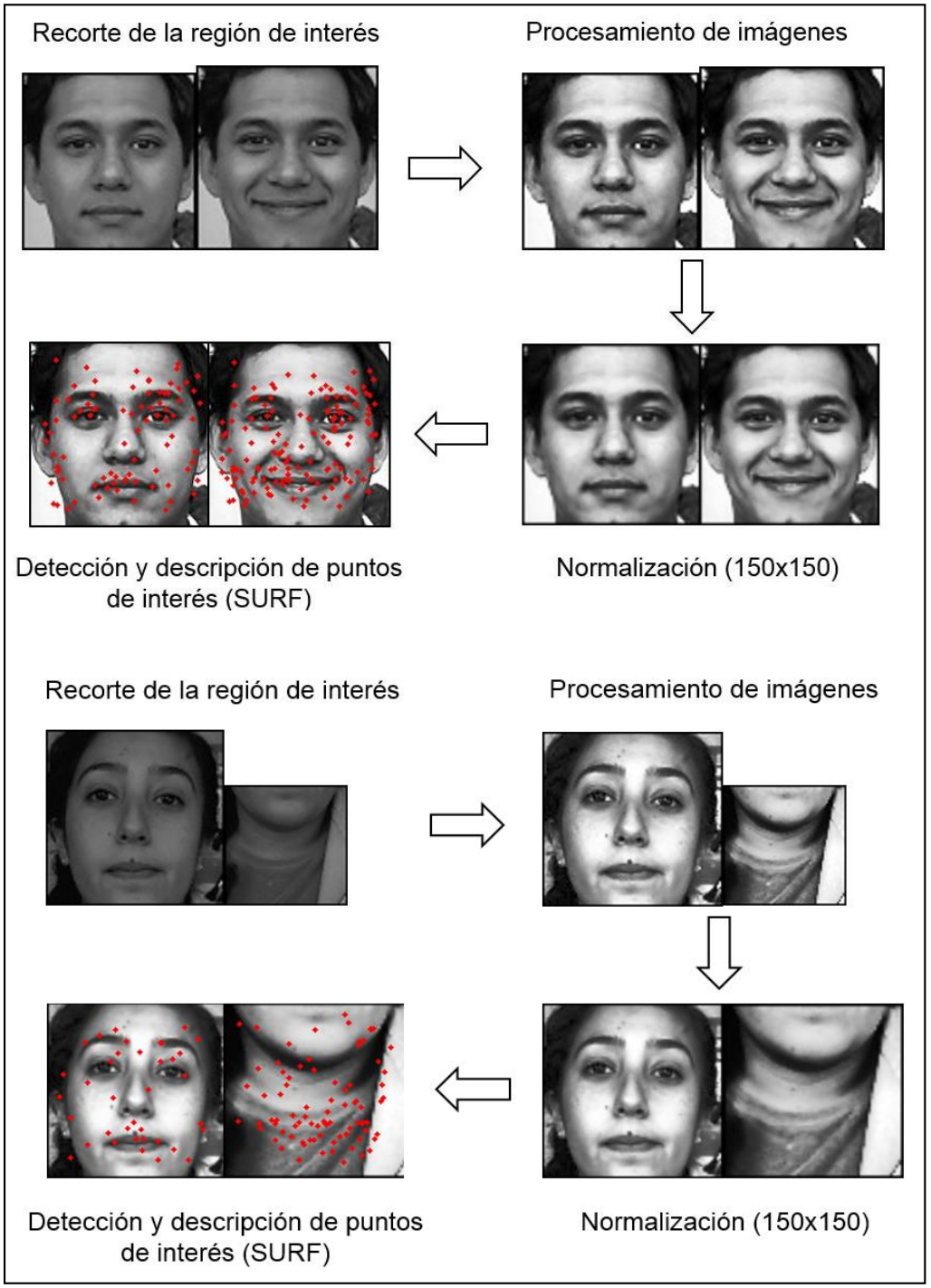
Detección del rostro: Se adquirió un 98% de resultados correctos de este proceso (69 rostros detectados en cada dispositivo móvil). La Figura 5-32 presenta algunos de los rostros que fueron detectados positivamente y el caso del rostro que no fue detectado.

Figura 5-32 Detección del rostro en dispositivos móviles.



Extracción de características: La Figura 5-33 muestra un ejemplo del proceso de extracción de características en las imágenes de entrada el cual se considera desde el recorte de la región de interés hasta la detección y descripción de puntos de interés tanto para una detección de rostro correcta como incorrecta.

Figura 5-33 Extracción de características en dispositivos móviles (parte 2).



La Tabla 5-23 despliega los resultados obtenidos en este proceso además del número de características en promedio de cada imagen de entrada. Cabe resaltar que se adquirieron los mismos resultados en todos los dispositivos móviles.

Tabla 5-23 Número de características en dispositivos móviles (parte 2).

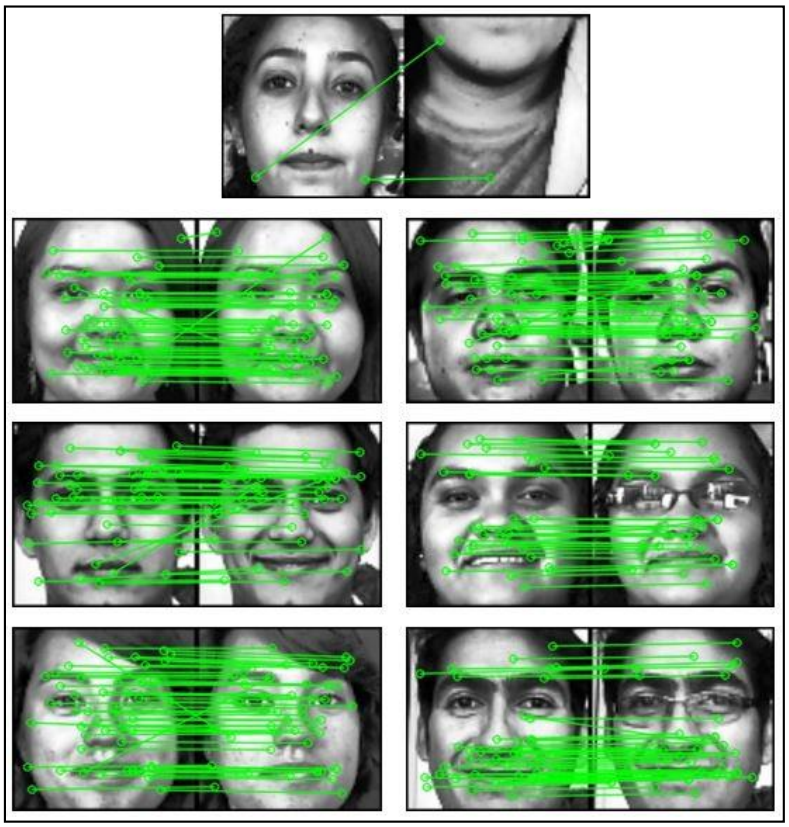
Prueba			Prueba		
	FImg1	FImg2		FImg1	FImg2
1	121	104	36	102	117
2	099	117	37	106	092
3	117	104	38	106	092
4	093	086	39	095	105
5	098	089	40	104	117
6	086	100	41	089	097
7	100	113	42	086	096
8	104	100	43	114	092
9	100	100	44	121	113
10	089	084	45	121	114
11	085	088	46	094	092
12	085	074	47	095	112
13	096	091	48	121	106
14	088	102	49	095	092
15	100	099	50	105	093
16	092	104	51	092	105
17	079	100	52	112	106
18	095	092	53	102	093
19	074	086	54	106	096
20	086	093	55	090	088
21	092	086	56	094	086
22	092	086	57	090	086
23	088	093	58	114	095
24	090	074	59	099	124
25	089	091	60	127	114
26	106	099	61	114	108
27	095	099	62	089	092
28	069	083	63	106	095
29	091	076	64	106	091
30	103	105	65	100	095
31	108	103	66	093	084
32	106	104	67	100	114
33	114	115	68	097	093
34	096	106	69	102	105
35	106	112	70	089	086
			Promedio	**098**	**097**

Coincidencias: La Tabla 5-24 presenta los resultados obtenidos en este proceso además del número de coincidencias en promedio. Por otro lado, la Figura 5-34 despliega algunos de los resultados tanto exitosos como erróneos del proceso de autenticación facial.

Tabla 5-24 Número de coincidencias en dispositivos móviles (parte 2).

Prueba	CImgs	Prueba	CImgs
1	39	36	41
2	43	37	32
3	25	38	32
4	41	39	39
5	32	40	34
6	24	41	31
7	41	42	36
8	48	43	34
9	47	44	48
10	27	45	60
11	46	46	49
12	34	47	31
13	44	48	37
14	36	49	38
15	44	50	47
16	32	51	48
17	33	52	40
18	31	53	32
19	38	54	35
20	48	55	21
21	39	56	44
22	39	57	36
23	39	58	33
24	24	59	44
25	37	60	35
26	31	61	41
27	40	62	39
28	35	63	35
29	29	64	39
30	48	65	30
31	46	66	02
32	48	67	38
33	40	68	49
34	45	69	41
35	36	70	30
		Promedio	**37**

Figura 5-34 Autenticación facial exitosa y errónea en dispositivos móviles (parte 2).



Decisión: Los resultados se presentan en la Tabla 5-25 donde se muestran los verdaderos positivos (TP), falsos negativos (FN) y el porcentaje de autenticidad de las imágenes evaluadas, con el cual se determina si esta fue exitosa o errónea. Estos resultados fueron los mismos para todos los dispositivos móviles.

Tabla 5-25 TP y FN en imágenes evaluadas en dispositivos móviles (parte 2).

Base de datos	TP	FN	Autenticidad
SURFace	90%	10%	90%

En las Figuras 5-35 a 5-45 se puede observar el icono de la aplicación de autenticación facial y la pantalla principal, así como la implementación de la metodología propuesta usando el mismo conjunto de imágenes de prueba en los seis dispositivos móviles.

Figura 5-35 Autenticación facial en Tablet Samsung Galaxy Tab S.

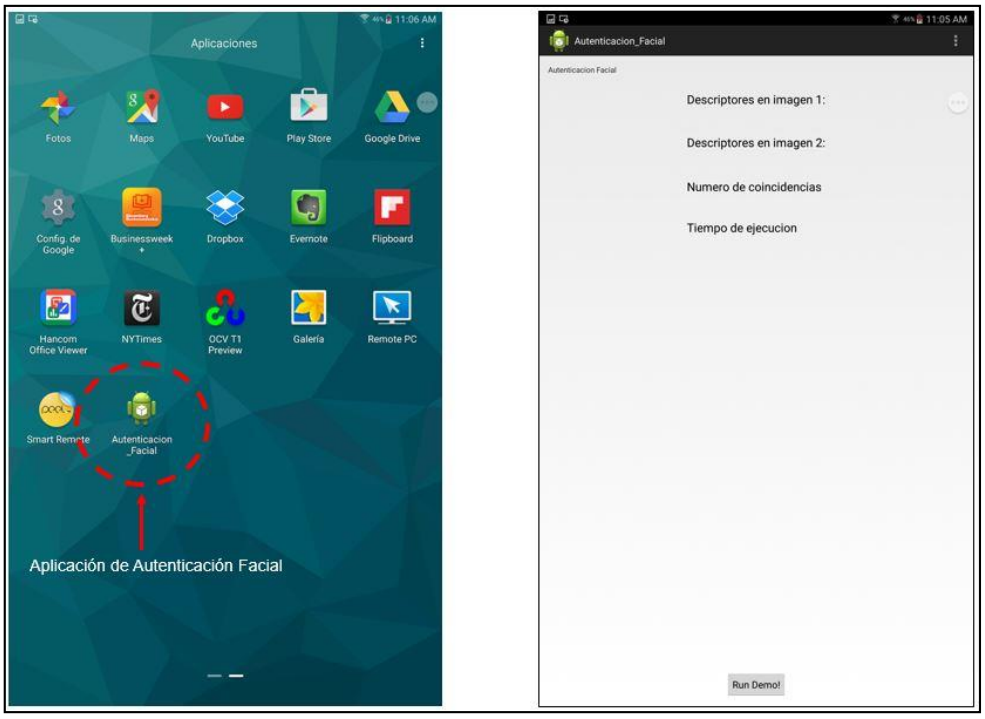


Figura 5-36 Autenticación facial en Smartphone LG Optimus L7.

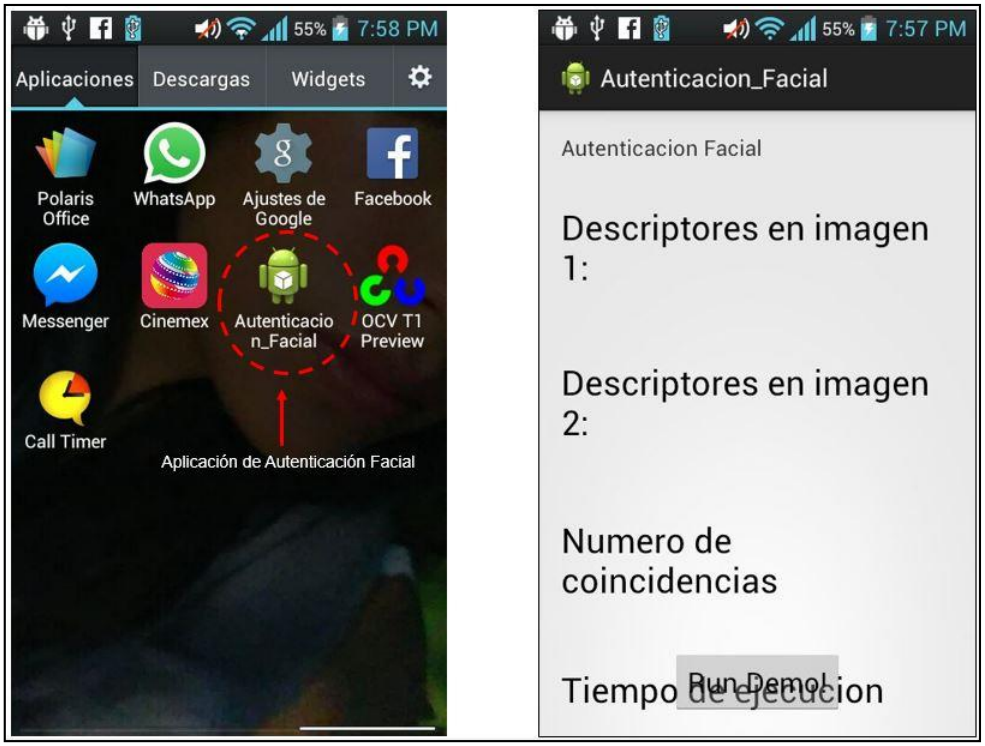


Figura 5-37 Autenticación facial en Smartphone Alcatel One Touch Pop C3.

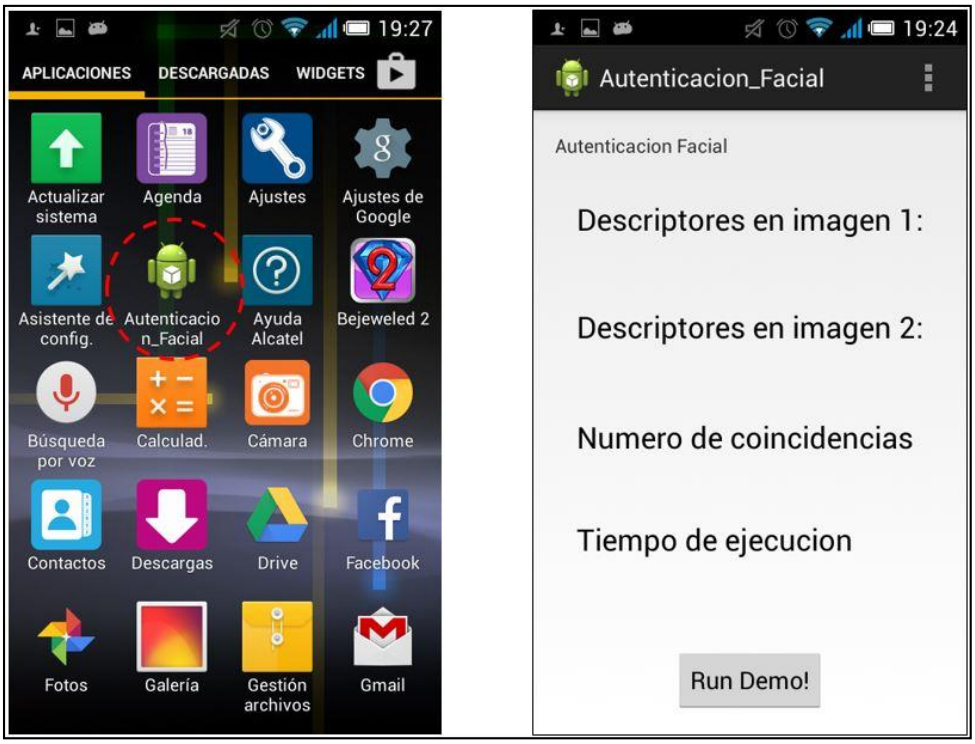


Figura 5-38 Autenticación facial en Smartphone Samsung GALAXY S II GT-I9100.

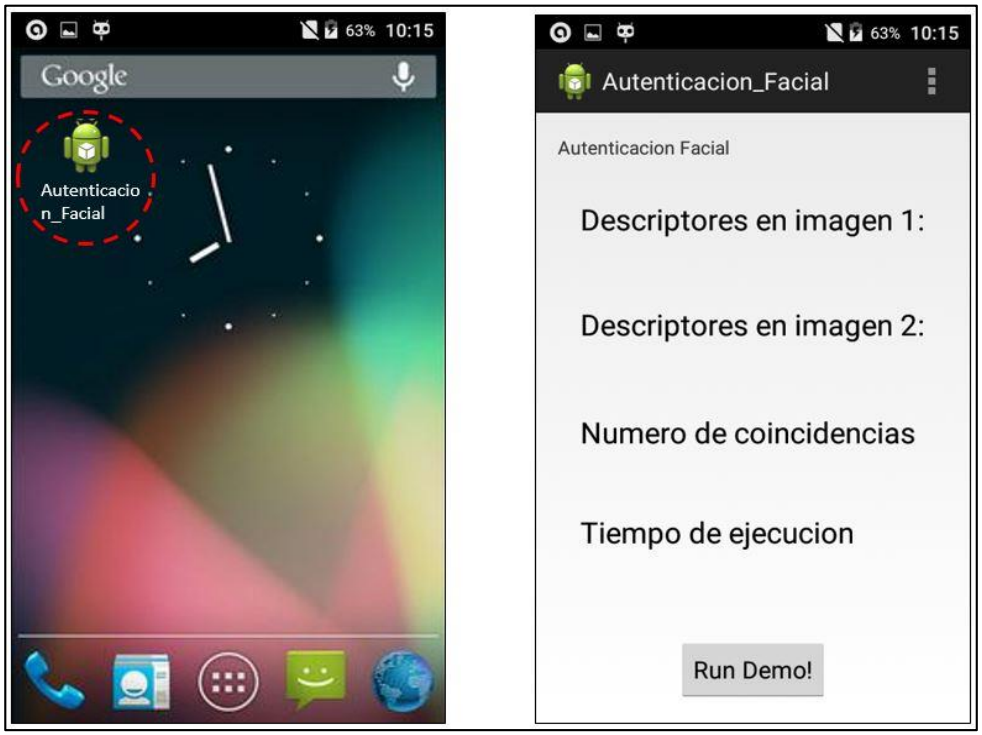


Figura 5-39 Ejemplo de autenticación facial exitosa en Tablet Samsung Galaxy Tab 4.

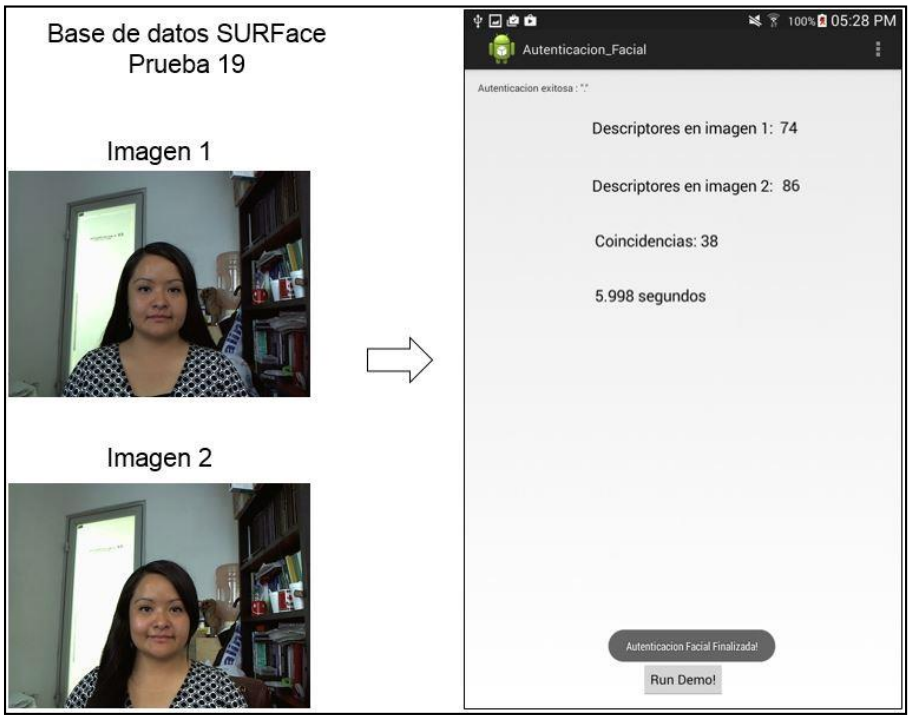


Figura 5-40 Ejemplo de autenticación facial exitosa en Tablet Samsung Galaxy Note 10.1.

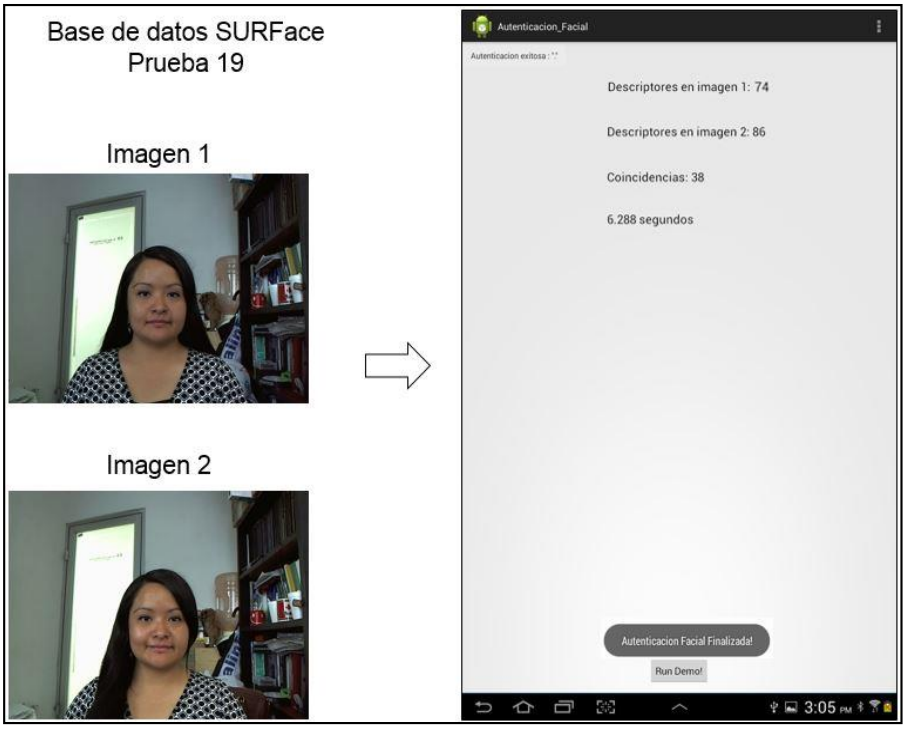


Figura 5-41 Ejemplo de autenticación facial exitosa en Tablet Samsung Galaxy Tab S.

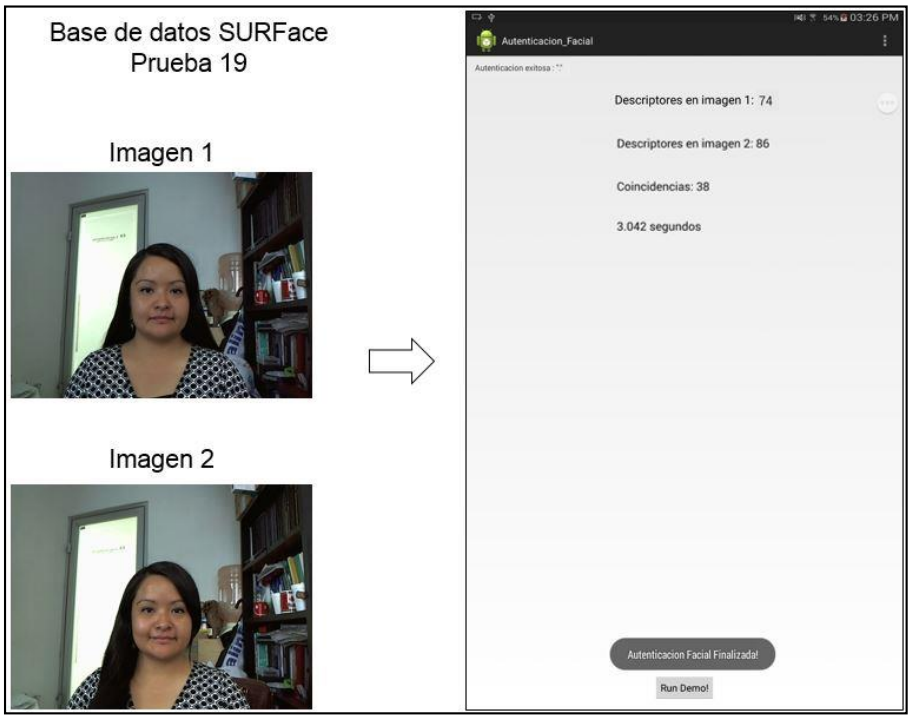


Figura 5-42 Ejemplo de autenticación facial exitosa en Smartphone LG Optimus L7.

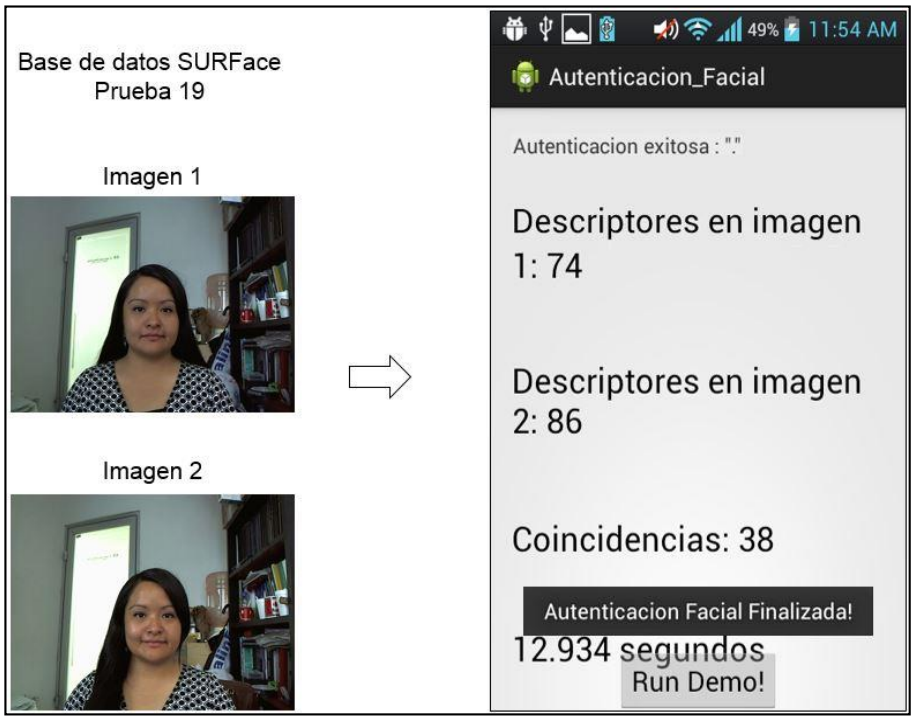


Figura 5-43 Ejemplo de autenticación facial exitosa en Smartphone Alcatel One Touch Pop.

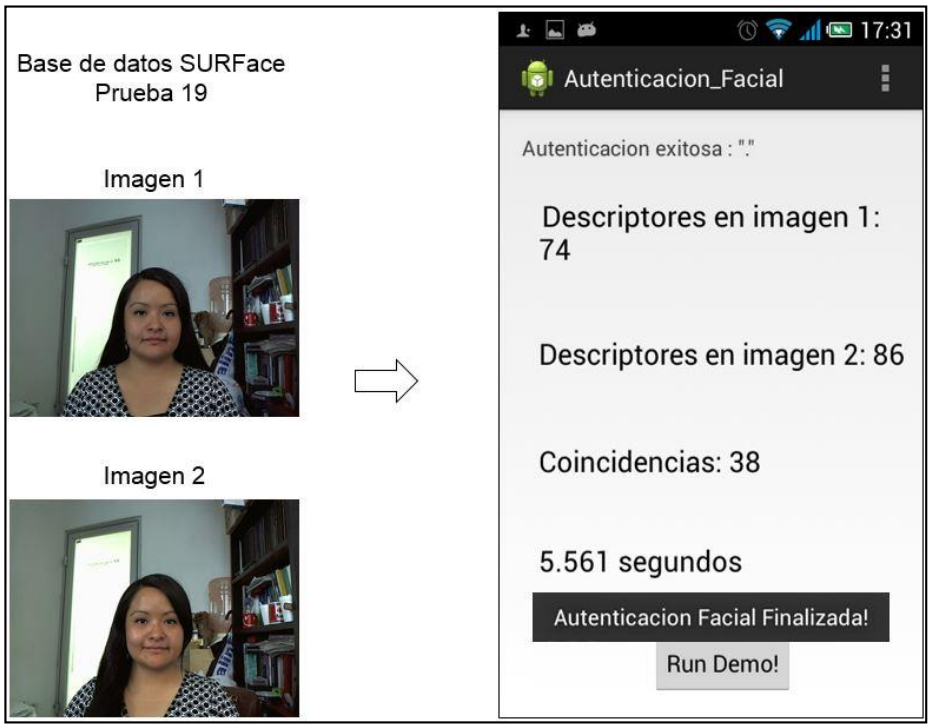


Figura 5-44 Ejemplo de autenticación facial exitosa en Smartphone Samsung GALAXY S II.

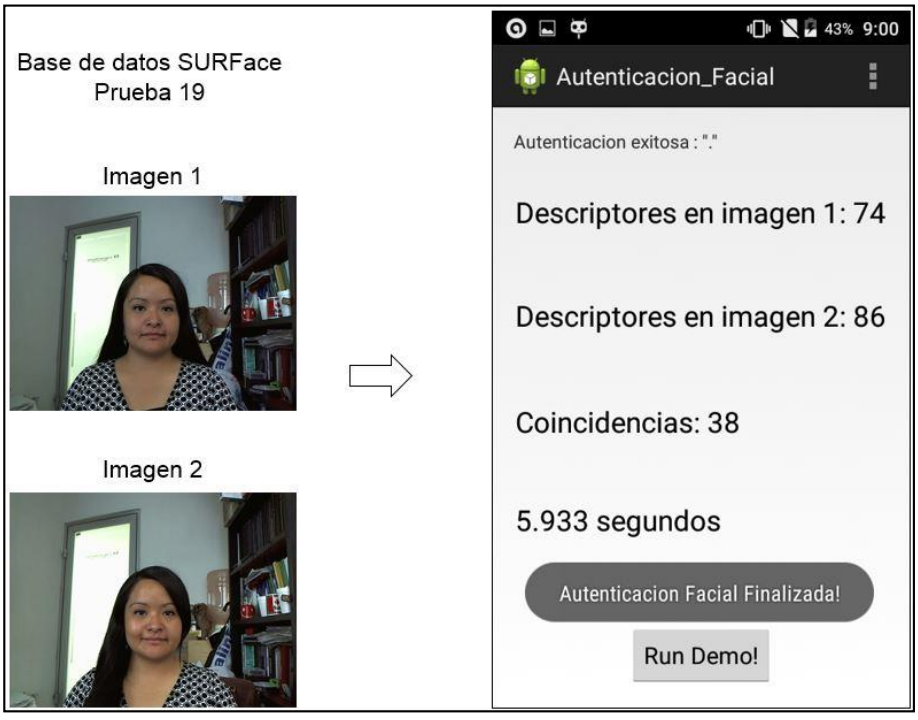
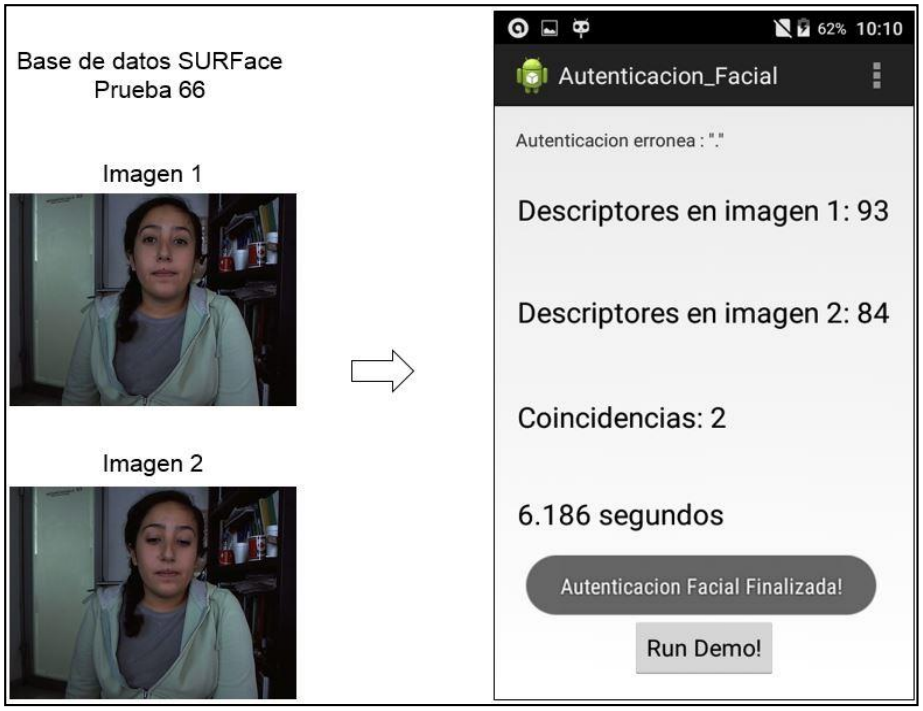


Figura 5-45 Ejemplo de autenticación facial errónea en Smartphone Samsung GALAXY S II.



A continuación se presentan los resultados obtenidos al realizar la autenticación facial de cada uno de los voluntarios de la base de datos SURFace contra otro de ellos, es decir, una imagen de entrada corresponderá a la persona que se desea autenticar mientras que la otra imagen hará referencia a otra persona que tenga algún parecido físico con la primera.

Cabe señalar que las imágenes de los voluntarios fueron seleccionadas al azar, empleando un total de 40 imágenes en 20 pruebas diferentes. Finalmente, la Tabla 5-26 despliega los resultados de este conjunto de pruebas las cuales se ejecutaron en la Tablet Samsung Galaxy Tab 4 y la Figura 5-46 muestra algunos ejemplos del proceso de autenticación.

Tabla 5-26 Número de características y coincidencias entre diferentes individuos.

Prueba	FImg1	FImg2	CImgs	Autenticación
1	117	108	02	Errónea
2	086	086	04	Errónea
3	100	100	14	Errónea
4	085	089	12	Errónea
5	096	093	08	Errónea
6	092	121	14	Errónea
7	093	096	15	Errónea
8	099	090	06	Errónea
9	083	105	01	Errónea
10	105	100	13	Errónea
11	106	074	13	Errónea
12	117	095	18	Errónea
13	111	113	07	Errónea
14	092	077	09	Errónea
15	095	099	08	Errónea
16	086	085	04	Errónea
17	099	103	11	Errónea
18	089	092	11	Errónea
Promedio	087	086	08	

Figura 5-46 Autenticación facial entre diferentes individuos.

Como se puede observar en los resultados de la Tabla 5-26 y considerando el número de coincidencias (falsos positivos) entre las imágenes de entrada, en ninguno de los casos se obtiene una autenticación exitosa ya que para que eso sea posible es necesario igualar o superar el umbral establecido en la metodología propuesta (número de coincidencias ≥ 30).

5.6. Tiempo de procesamiento

El siguiente parámetro que se tomó en cuenta fue el tiempo de procesamiento en cada dispositivo móvil. La Tabla 5-27 muestra los resultados obtenidos en las Tablets Samsung Galaxy Tab 4 y Galaxy Note 10.1 con algunas imágenes de las bases de datos The Extended Cohn-Kanade Dataset (CK+), Caltech Faces y FERET, donde se puede apreciar la diferencia en tiempo de procesamiento promedio entre ambos dispositivos.

Tabla 5-27 Tiempo de procesamiento con bases de datos públicas.

Prueba	**CK+ (s)**		**Caltech Faces (s)**		**FERET (s)**	
	Tab 4	**Note 10.1**	**Tab 4**	**Note 10.1**	**Tab 4**	**Note 10.1**
1	5.92	6.11	7.19	7.30	6.18	6.25
2	5.99	6.13	6.99	7.29	6.68	6.83
3	5.59	5.71	7.01	7.48	7.46	7.56
4	5.79	5.98	7.10	7.30	7.05	7.31
5	6.10	6.27	7.07	7.66	6.81	6.95
6	5.99	6.21	6.61	6.78	6.32	6.53
7	5.82	5.91	6.64	6.78	6.49	6.74
8	5.70	5.75	7.07	7.30	6.25	6.32
9	5.64	5.72	6.89	7.30	5.88	6.12
10	5.53	5.91	7.40	7.91	7.14	7.42
11	6.16	6.36	6.83	7.15	7.01	7.27
12	6.75	7.15	7.01	7.24	7.08	7.32
13	5.57	5.79	7.09	7.31	6.93	7.15
14	5.39	5.48	6.09	6.28	6.60	7.13
15	5.56	5.69	7.21	7.45	7.25	7.44
16	6.05	6.25	6.81	7.10	7.35	7.63
17	5.70	5.85	7.01	7.23	6.77	6.98
18	5.70	5.75	6.39	6.60	6.78	7.00
19	5.97	6.01	6.49	6.99	5.95	6.16
20	5.62	5.79	6.44	6.66	6.66	6.88
Promedio	**5.82**	**5.99**	**6.86**	**7.15**	**6.73**	**6.94**
Diferencia	**0.17**		**0.29**		**0.21**	

La Tabla 5-28 presenta el tiempo de procesamiento de la metodología propuesta considerando la base de datos propia SURFace para las Tablets: (d) Samsung Galaxy Tab 4, (e) Samsung Galaxy Note 10.1 y (f) Samsung Galaxy Tab S. Y la Tabla 5-29 despliega la misma información para los Smartphones: (g) LG Optimus L7, (h) Alcatel One Touch Pop C3 y (i) Samsung GALAXY S II GT.

Tabla 5-28 Tiempo de procesamiento para cada Tablet.

Prueba	d	e	f	Prueba	d	e	f
	(s)	(s)	(s)		(s)	(s)	(s)
1	6.45	6.51	3.84	36	6.77	7.12	3.66
2	6.50	6.80	3.47	37	6.77	7.01	3.40
3	6.29	6.65	3.35	38	6.58	6.89	4.52
4	5.88	6.21	3.11	39	6.70	7.04	3.62
5	5.75	5.94	3.01	40	6.79	7.09	3.71
6	5.86	6.11	3.10	41	6.42	6.61	3.36
7	6.37	6.68	3.41	42	6.18	6.55	3.31
8	6.31	6.55	3.29	43	6.17	6.35	3.25
9	6.26	6.53	3.30	44	6.77	7.12	3.67
10	5.77	6.11	3.05	45	6.49	6.71	3.52
11	6.10	6.32	3.29	46	6.13	6.42	3.23
12	6.08	6.29	3.18	47	6.50	6.81	3.45
13	6.35	6.66	3.34	48	6.84	7.06	3.59
14	6.26	6.51	3.25	49	5.48	5.69	2.88
15	6.35	6.49	3.31	50	5.51	5.81	2.95
16	6.28	6.54	3.30	51	5.47	5.67	2.93
17	6.14	6.50	3.35	52	5.63	5.80	3.11
18	6.19	6.45	3.28	53	5.52	5.66	2.91
19	5.99	6.28	3.04	54	5.52	5.74	2.93
20	6.13	6.41	3.23	55	5.65	5.93	3.00
21	6.28	6.64	5.14	56	5.66	5.88	2.96
22	6.28	6.70	3.24	57	5.69	5.89	3.01
23	6.17	6.37	3.19	58	6.14	6.48	3.26
24	5.95	6.26	3.12	59	6.14	6.43	3.27
25	6.11	6.35	3.18	60	6.43	6.74	3.46
26	6.20	6.42	3.24	61	6.26	6.64	3.35
27	6.06	6.47	3.18	62	6.15	6.42	3.39
28	5.74	6.07	2.99	63	6.33	6.65	3.42
29	5.85	6.08	3.06	64	6.29	6.69	3.29
30	5.67	5.81	3.03	65	6.28	6.64	3.37
31	5.92	6.05	3.04	66	6.23	6.55	3.31
32	5.90	6.12	3.14	67	6.37	6.68	3.36
33	6.04	6.42	3.26	68	5.65	5.89	3.09
34	5.85	6.09	3.13	69	6.77	7.09	3.67
35	6.01	6.18	3.31	70	6.08	6.37	3.12
				Promedio	**6.13**	**6.40**	**3.30**

Tabla 5-29 Tiempo de procesamiento para cada Smartphone.

Prueba	g	h	i	Prueba	g	h	i
	(s)	(s)	(s)		(s)	(s)	(s)
1	12.41	8.80	6.06	36	13.52	6.28	6.59
2	12.33	6.34	6.42	37	13.16	6.07	6.48
3	15.30	5.81	6.12	38	10.82	6.67	6.39
4	09.45	5.47	5.64	39	12.80	6.45	6.58
5	08.53	5.17	5.68	40	11.13	6.26	6.50
6	08.23	5.38	5.92	41	11.24	6.00	6.22
7	08.71	5.74	6.37	42	09.91	5.82	6.20
8	10.13	5.84	6.01	43	11.85	5.79	6.03
9	15.03	5.79	6.21	44	12.74	6.16	6.56
10	14.15	5.41	5.72	45	12.45	5.96	6.45
11	12.10	5.66	6.04	46	09.13	5.67	5.98
12	12.93	5.55	5.97	47	08.97	5.97	6.37
13	10.70	5.81	6.20	48	09.31	6.23	6.64
14	14.34	5.92	6.06	49	07.57	5.00	5.48
15	14.16	5.76	6.33	50	07.54	5.08	5.48
16	15.50	5.75	6.01	51	12.14	4.97	5.56
17	11.66	5.67	5.88	52	09.34	5.15	5.56
18	11.93	5.61	5.99	53	11.25	5.04	5.55
19	12.93	5.56	5.93	54	11.24	5.04	5.55
20	11.27	5.70	5.95	55	10.02	5.22	5.70
21	12.63	5.84	6.38	56	10.00	5.14	5.56
22	08.75	5.94	6.06	57	10.15	5.09	5.64
23	11.71	5.73	6.10	58	11.70	5.60	5.99
24	13.29	5.67	6.16	59	09.90	5.61	6.06
25	17.67	5.62	5.98	60	11.30	5.94	6.36
26	11.52	5.62	6.41	61	11.72	5.67	6.27
27	10.10	5.67	6.08	62	11.24	5.76	6.05
28	13.80	5.25	5.49	63	11.68	5.84	6.20
29	12.52	5.36	5.70	64	16.16	5.76	6.27
30	10.43	5.13	5.44	65	13.35	5.78	6.21
31	09.26	5.25	5.77	66	12.48	5.78	6.18
32	12.40	5.32	5.87	67	12.85	5.93	6.52
33	11.04	5.57	5.94	68	11.07	5.08	5.46
34	10.16	5.42	5.66	69	12.73	6.45	6.54
35	10.74	5.54	6.13	70	09.05	5.56	5.90
				Promedio	**11.56**	**5.70**	**6.03**

Como se puede observar en las Tablas 5-28 y 5-29, los dispositivos que tuvieron en promedio el menor tiempo de procesamiento fueron la Tablet Samsung Galaxy Tab S y el Smartphone Alcatel One Touch Pop C3, por el contrario, aquellos que tuvieron en promedio el mayor tiempo de procesamiento fueron la Tablet Samsung Galaxy Note 10.1 y el Smartphone LG Optimus L7.

6. CONCLUSIONES Y TRABAJO FUTURO

Se propuso una metodología novedosa para autenticación facial basada en un método que toma como referencia el algoritmo SURF. La novedad radica en la adición de una etapa de preprocesamiento de imágenes, cuya imagen de salida será la que utilice el algoritmo SURF como inicio del proceso de autenticación.

Con la implementación de la etapa de preprocesamiento de imágenes, la propuesta del umbral heurístico ≥ 30 para la autenticación de dos imágenes del rostro de una persona y del uso del algoritmo SURF dentro de la fase de extracción de características en dispositivos móviles, se obtuvo el 90% de resultados correctos positivos en promedio entre 6.13 s y 6.40 s en el proceso de autenticación facial[4], el cual comparado con el 90% en 6.54 s en promedio obtenido por (Ye *et al.,* 2015) permite concluir que la metodología propuesta presenta un buen desempeño de autenticación, principalmente en dispositivos con procesador superior al Dual-Core 1.2GHz.

Por otro lado, gracias al desarrollo de este proyecto de investigación se obtuvo una base de datos de rostros propia denominada SURFace, con la cual se logró realizar un conjunto de pruebas de autenticación facial en diversos dispositivos móviles para obtener el porcentaje de resultados correctos positivos y el tiempo de procesamiento en cada uno de ellos, sin embargo este último factor depende de los recursos físicos con los que cuente cada dispositivo (procesador, RAM, etc.).

Asimismo, con el desarrollo de la metodología indicada en la Figura 5-22 y los resultados obtenidos en las Tablas 5-16 a 5-18, se puede llegar a la implementación de un sistema de autenticación facial de bajo costo en tarjetas de desarrollo Raspberry Pi.

[4] Considerando características similares entre los dispositivos utilizados en este trabajo y el empleado por (Ye *et al*., 2015).

Finalmente, como trabajo futuro se pretende implementar la metodología propuesta como medio de acceso a los dispositivos móviles, además de utilizar la cámara frontal de estos mismos de tal manera que se pueda adquirir una imagen en tiempo real de la persona que se desea autenticar para se compare no solo con una imagen sino con más imágenes de la persona las cuales se encontraran en la base de datos SURFace, para finalmente determinar si esta puede o no acceder al dispositivo móvil.

REFERENCIAS

Abeni, P., M. Madalina, and R. D'Alessandro. 2006. Implementing Biometrics-Based Authentication for Mobile Devices. In Global Telecommunications Conference. GLOBECOM '06, p. 1–5.

Anviz. 2013. Recuperado de http://www.anviz.com (consultado el 16 de Marzo de 2015).

Bay, H., T. Tuytelaars, and L. Van Gool. 2006. SURF: Speeded Up Robust Features. In Computer vision–ECCV. Springer, p. 404–417.

Bay, H., A. Ess, T. Tuytelaars, and L. Van Gool. 2008. Speeded-up robust features (SURF). In Computer vision and image understanding, 110(3), p. 346–359.

Bhattacharyya, D., R. Ranjan, F. Alisherov A., and M. Choi. 2009. Biometric Authentication: A Review. In International Journal of u- and e- Service, Science and Technology, Vol. 2, No. 3, p. 13–28.

Bigun, J., J. Fiérrez Aguilar, J. Ortega Garcia, and J. Gonzalez Rodriguez. 2005. Combining biometric evidence for person authentication. In Advanced Studies in Biometrics, Springer Berlin Heidelberg, p. 1–18.

Boehm, A., D. Chen, M. Frank, L. Huang, C. Kuo, T. Lolic, I. Martinovic, and D. Song. 2008. SAFE: Secure Authentication with Face and Eyes. In Proceedings of International Conference on Security and Privacy in Mobile Information and Communication Systems, p. 1–8.

Boullosa, Ó. 2011. Estudio comparativo de descriptores visuales para la detección de escenas cuasi-duplicadas. Universidad Autónoma de Madrid, Madrid, España.

Bouris, D., A. Nikitakis, and I. Papaefstathiou. 2010. Fast and efficient FPGA-based feature detection employing the SURF algorithm. In Field-Programmable Custom Computing Machines, 18th IEEE Annual International Symposium on, p. 3–10.

Brumnik, R., I. Podbregar, and T. Ivanuša. 2011. Reliability of Fingerprint Biometry (Weibull Approach). In Biometric Systems, Design and Applications, p. 1. Recuperado de http://www.intechopen.com/books/biometric-systems-design-and-applications/reliability-of-fingerprint-biometry-weibull-approach-. ISBN: 978-953-307-542-6 (consultado el 11 de Noviembre de 2014).

CareerDiva. 2009. smile-scan. Recuperado de http://www.evetahmincioglu.com/web/blog/wp-content/uploads/2009/07/smile-scan.jpg (consultado el 16 de Marzo de 2015)

Chao, W.-L. 2010. Face Recognition. GICE, National Taiwan University, Taiwan.

Chen, S., A. Pande, and P. Mohapatra. 2014. Sensor-Assisted Facial Recognition: An Enhanced Bio-metric Authentication System for Smartphones. In Proceedings of the 12th annual international conference on Mobile systems, applications, and services, p. 109–122.

Derpanis, K. 2007. Integral image-based representations. Department of Computer Science and Engineering, York University, p. 1–6.

Deza, M. M., and E. Deza. 2009. Encyclopedia of Distances. Springer, Berlin.

DIGINFO. 2012. Recuperado de http://www.diginfo.tv/v/12-0209-r-en.php (consultado el 16 de Marzo de 2015)

Duc, N. M., and B. Q. Minh. 2009. Your face is NOT your password. Face Authentication ByPassing Lenovo – Asus – Toshiba. Black Hat Briefings. Ha Noi University of Technology, Vietnam.

Falcao, X. 2003. Recuperado de http://www.ic.unicamp.br/~cpg/material-didatico/mo815/9802/curso/img65.png (consultado el 25 de Febrero de 2015)

Florencia, A. N. 2004. Modelado de Sistemas de control de un robot manipulador basado en procesamiento digital de Imágenes. Tesis de grado de Maestría en Ciencias. Universidad de las Américas de Puebla, Puebla, México. Recuperado de http://catarina.udlap.mx/u_dl_a/tales/documentos/msp/florencia_y_an/

Fong, L. L., and W. C. Seng. 2009. User authentication on mobile phones – What is the best approach?. University of Malaya, Kuala Lumpur, Malaysia. Recuperado de http://www.cigital.com/wp-content/uploads/downloads/2012/11/mobile-authentication.pdf

Gámez, C. V. 2009. Diseño y Desarrollo de un Sistema de Reconocimiento de Caras. Proyecto de grado de Ingeniería de Telecomunicación. Escuela Politécnica Superior. Madrid.

Gartner. 2014. Forecast: PCs, Ultramobiles and Mobile Phones, Worldwide, 2011-2018, 3Q14 Update. Recuperado de http://www.gartner.com/document/2848418 (consultado el 03 de Marzo de 2015).

Gibson, M. 2015. Recuperado de https://itunes.apple.com/us/app/faceshine-powerful-social/id967868541?mt=8 (consultado el 16 de Marzo de 2015)

González R. C. y R. E. Woods. 2002. Digital Image Processing. New Jersey, United States. Prentice-Hall, Inc.

Gui, Y., A. Su, and J. Du. 2013. Point-pattern matching method using SURF and Shape Context. In Optik - International Journal for Light and Electron Optics, p. 1869–1873.

Hadid, A., J. Y. Heikkild, O. Silven, and M. Pietikdinen. 2007. Face and eye detection for person authentication in mobile phones. In Distributed Smart Cameras. ICDSC'07. First ACM/IEEE International Conference on, p. 101–108.

Han, J.H., S. Yang, and B.U. Lee. 2011. A novel 3-D color histogram equalization method with uniform 1-D gray scale histogram. IEEE Transactions on Image Processing, 20(2), p. 506–512.

Hanvon. 2009. Recuperado de http://www.hanvon.com/en/products/index.html (consultado el 16 de Marzo de 2015)

Iglesias, G. 2007. Sistema de Autenticación para Dispositivos Móviles basado en Biometría de comportamiento de Tecleo. Tesis de grado de Ingeniería en Sistemas Computacionales. Instituto Tecnológico de Morelia. México, D.F. Recuperado de http://delta.cs.cinvestav.mx/~francisco/tesisIglesias.pdf

Izenman, A. J. 2008. Linear discriminant analysis. In Modern Multivariate Statistical Techniques. Springer New York, p. 237–280.

Jafri, R., and H. R. Arabnia. 2009. A Survey of Face Recognition Techniques. In Journal of Information Processing Systems, 5(2), p. 41–68.

Jiménez, E. 2009. Medición de distancias por medio de procesamiento de imágenes y triangulación, haciendo uso de cámaras de video. Tesis de grado de Ingeniería en Electrónica y Comunicaciones. Universidad de las Américas de Puebla, Puebla, México. Recuperado de http://catarina.udlap.mx/u_dl_a/tales/documentos/lem/jimenez_c_e/portada.html

Junered, M. 2010. Face Recognition in Mobile Devices. Master Thesis. Luleå University of Technology, Luleå, Suecia. Recuperado de http://pure.ltu.se/portal/files/31162078/LTU-EX-10040-SE.pdf

Kremić, E., and A. Subaşi. 2011. The Implementation of Face Security for Authentication Implemented on Mobile Phone. In The International Arab Journal of Information Technology, p. 414–419.

Kumar, S., and H. Kaur. 2012. Face recognition techniques: Classification and comparisons. In International Journal of Information Technology and Knowledge Management, 5(2), p. 361–363.

Lowe, D. G. 2004. Distinctive Image Features from Scale-Invariant Keypoints. In International journal of computer vision, 60(2), p. 91–110.

Lu, X. 2003. Image Analysis for Face Recognition. Michigan State University, East Lansing, Míchigan, Estados Unidos.

Lucey, P., J.F. Cohn, T. Kanade, J. Saragih, Z. Ambadar, and I. Matthews. 2010. The Extended Cohn-Kanade Dataset (CK+): A complete expression dataset for action unit and emotion-specified expression. Proceedings of the Third International Workshop on CVPR for Human Communicative Behavior Analysis, San Francisco, USA, p. 94–101.

Luxand. 2015. Recuperado de http://www.luxand.com/blink/LuxandBlinkProScreenshot1.jpg (consultado el 16 de Marzo de 2015)

Marqués, I. 2010. Face Recognition Algorithms. Universidad del país Vasco, Euskal Herria, España.

Maxine, C. 2007. Biometrics Market Development: Mega Trends and Meta Drivers. In Acuity Market Intelligence. Recuperado de http://www.acuity-mi.com/hdfsjosg/euyotjtub/Biometrics 2007 London.pdf

Mendoza-Martinez, C., J. C. Pedraza-Ortega, and J. M. Ramos-Arreguin. 2014. A Novel Approach for Face Authentication Using Speeded Up Robust Features Algorithm. In Human-Inspired Computing and Its Applications, p. 356–367. Springer International Publishing.

Mukherjee, S., A. Gangopadhyay, Z. Chen, and S. Russell. 2008. A Secure Face Recognition System for Mobile-devices without The Need of Decryption. citeseerx. Recuperado de http://citeseerx.ist.psu.edu/viewdoc/summary?doi=10.1.1.164.3345

Murali, Y., and M. MITS. 2012. Image mosaic using speeded up robust feature detection. In International Journal of Advanced Research in Electronics and Communication Engineering, 1(3), p. 40–45.

NeoFace. 2014. neoface. Recuperado de http://jpn.nec.com

Oyallon, E., and J. Rabin. 2013. An analysis and implementation of the SURF method, and its comparison to SIFT. In Image Processing On Line, ISSN 2105–1232.

Pabbaraju, A., and S. Puchakayala. 2009. Face Recognition for Mobile Devices. web.eecs. Recuperado de http://web.eecs.umich.edu/~silvio/teaching/EECS598_2010/progress_report/Aditya_Srujan.pdf

Paik, J.K. 2011. Image processing method and system using gain controllable clipped histogram equalization. U.S. Patent No 7, 885, 462, p. 1–15.

Phillips, P.J., H. Moon, S.A. Rizvi, and P.J. Rauss. 2000. The FERET Evaluation Methodology for Face-Recognition Algorithms. IEEE Transactions on Pattern Analysis and Machine Intelligence, vol. 22, no. 10, p. 1–15.

Pinto, B., and P. R. Anurenjan. 2011. Video stabilization using speeded up robust features. In Communications and Signal Processing, International Conference on, p. 527–531.

Raspberry. Disponible en: http://www.raspberrypi.org (consultado el 16 de Marzo de 2015).

Ren, J., X. Jiang, and J. Yuan. 2013. A complete and fully automated face verification system on mobile devices. In Pattern Recognition, 46(1), p. 45–56.

Rivera, A. 2013. Recuperado de http://totem.com.ec/blog/wp-content/uploads/2013/12/reconocimiento-facial-300x176.jpg (consultado el 18 de Marzo de 2015).

Ruiz, S., S. Lee, S. R. Soekadar, A. Caria, R. Veit, T. Kircher, and R. Sitaram. 2013. Acquired self-control of insula cortex modulates emotion recognition and brain network connectivity in schizophrenia. Human brain mapping, 34(1), p. 200–212.

Sainz, J. 2014. Recuperado de http://juanst.com/wp-content/uploads/2014/12/facephi-tecnologia-reconocimiento-facial.jpeg (consultado el 18 de Marzo de 2015).

Svab, J., T. Krajnik, J. Faigl, and L. Preucil. 2009. FPGA based speeded up robust features. In Technologies for Practical Robot Applications. IEEE International Conference on, p. 35–41.

Tao, Q., and R. Veldhuis. 2010. Biometric Authentication System on Mobile Personal Devices. In Instrumentation and Measurement, IEEE Transactions on, 59(4), p. 763–773.

Terriberry, T. B., L. M. French, and J. Helmsen. 2008. GPU accelerating speeded-up robust features. In Proceedings of 3DPVT, Vol. 8, p. 355–362.

Thakoor, K. A., S. Marat, P. J. Nasiatka, B. P. McIntosh, F. E. Sahin, A. R. Tanguay, J. D. Weiland, and L. Itti. 2013. Attention biased speeded up robust features (AB-SURF): A neurally-inspired object recognition algorithm for a wearable aid for the visually-impaired. In Multimedia and Expo Workshops, IEEE International Conference on, p. 1–6.

Travieso, C., M. del Pozo, and J. R. Ticay. 2011. Cuaderno Red de Cátedras Telefónica. Sistemas Biométricos. Recuperado de http://www.rcysostenibilidad.telefonica.com/blogs/documentoscatedras/files/2012/07/Catedra_telefonica_Sistemas_Biometricos.pdf

Valstar, M., J. Girard, T. Almaev, G. McKeown, M. Mehu, L. Yin, and J. Cohn. 2015. Fera 2015-second facial expression recognition and analysis challenge. Proc. IEEE ICFG.

Viola, P., and Jones. M. 2001. Rapid Object Detection Using a Boosted Cascade of Simple Features. In Proceedings of the Computer Vision and Pattern Recognition, Kauai, p. I-511–I-518.

Viola, P., and M. Jones. 2002. Robust real-time object detection. In International Journal of Computer Vision, vol. 57, no. 2, p. 137–154.

Visidon. 2014. Recuperado de http://www.visidon.fi

Wang, Y. T., C. T. Chi, and Y. C. Feng. 2014. Robot mapping using local invariant feature detectors. In Engineering Computations: International Journal for Computer-Aided Engineering and Software 31(2), p. 297–316.

Weber, M. 2000. Unsupervised Learning of Models for Object Recognition. PhD. Thesis, California Institute of Technology, Pasadena, California.

Ye, P., M. Yu, and M. Wu. 2015. Implementation: Mobile Face Identity Authentication System on Android Platforms. International Journal of Security and Its Applications, 9(1), p. 51–60.

Yin, Q., Tang, X., and Sun, J. 2011. An associate-predict model for face recognition. In Computer Vision and Pattern Recognition (CVPR), 2011 IEEE Conference on. IEEE, p. 497–504

Zheng, X., S. Cui, G. Wang, and J. Li. 2015. Video Stabilization System Based on Speeded-up Robust Features. In International Industrial Informatics and Computer Engineering Conference, p. 1995–1998.

Zhuang, X. 2013. Front camera technique and facial recognition in mobile Cs5760.

ANEXOS

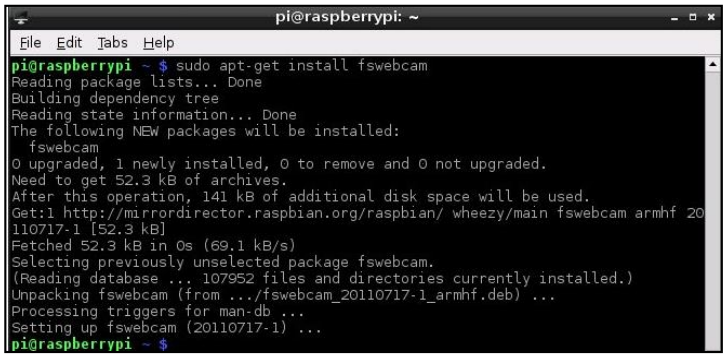
ANEXO I

Configuración de webcam en Raspbian

Instalación

Para usar una webcam es necesario la instalación de fswebcam. Por lo tanto, en la consola de Raspbian se debe escribir el siguiente comando (ver Figura I-1): **sudo apt-get install fswebcam**

Figura I-1 Instalación de fswebcam en la consola de Raspbian.



Uso básico del comando fswebcam

En la consola de Raspbian se debe escribir fswebcam seguido del nombre de la imagen y su extensión, el siguiente paso es presionar la tecla Enter y una fotografía será tomada con la cámara web y salvada con el nombre que se le especificó anteriormente. Un ejemplo de la captura de una imagen se puede apreciar en la Figura I-2.

Figura I-2 Captura de una imagen desde una cámara web con fswebcam.

Configurando la resolución de una imagen

La cámara web usada en este ejemplo tiene una resolución de 352x288, sin embargo si se requiere especificar una resolución diferente se debe usar el comando “-r” seguido de la nueva resolución de la imagen tal y como se aprecia en los ejemplos de las Figuras I-3 y I-4.

Figura I-3 Especificación de diferentes resoluciones de una imagen.

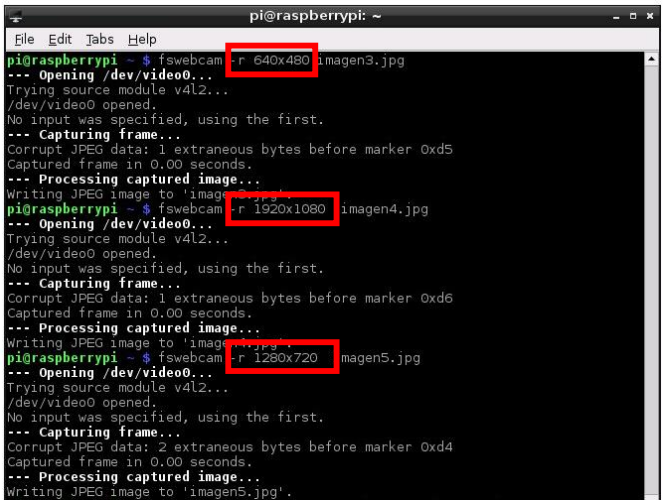
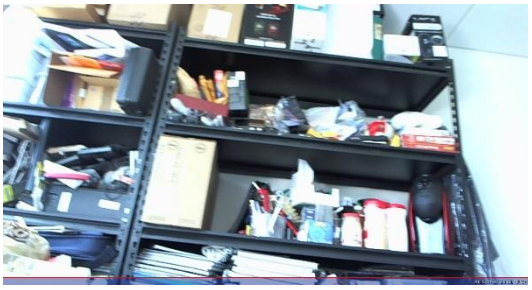


Figura I-4 Ejemplos de diferentes resoluciones.



Especificar sin pie de imagen (banner)

Para poder adquirir una imagen sin el banner que aparece en la parte inferior de la imagen, se debe agregar el siguiente comando “--no-banner”. El resultado de usar este comando se puede apreciar en la Figura II-5.

Figura I-5 imagen sin banner con el comando “--no-banner”.

ANEXO II

Selección del dispositivo móvil en Eclipse.

Figura II-1 Tablet Samsung Galaxy Tab 4 con versión 4.4.2 del sistema operativo Android.

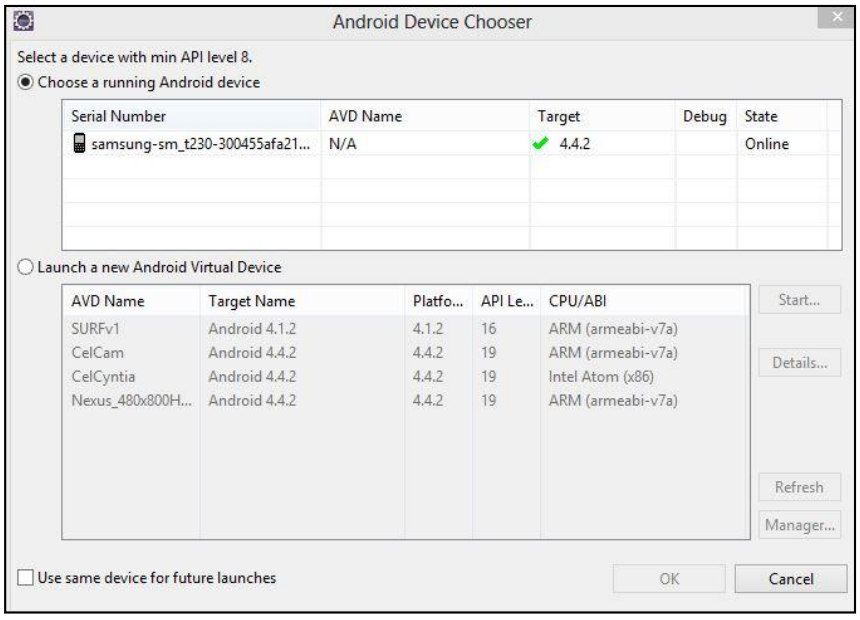


Figura II-2 Tablet Samsung Galaxy Note 10.1 con versión 4.1.2 del sistema operativo Android.

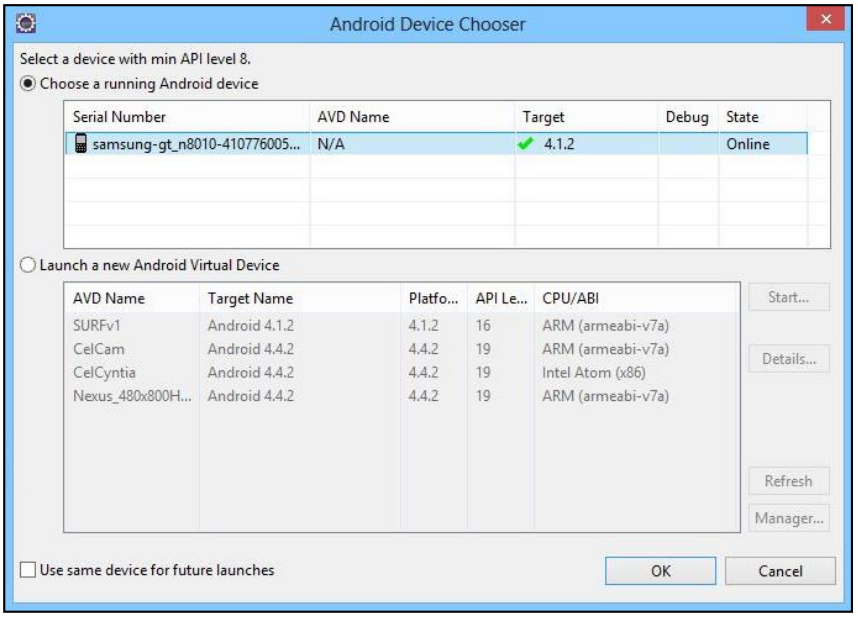


Figura II-3 Tablet Samsung Galaxy Tab S con versión 4.4.2 del sistema operativo Android.

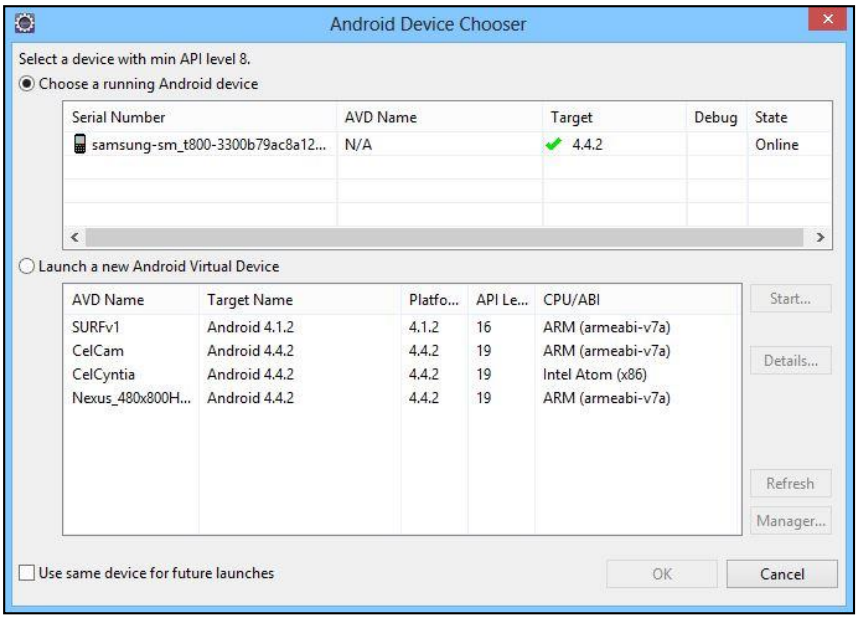


Figura II-4 Smartphone LG Optimus L7 con versión 4.0.3 del sistema operativo Android.

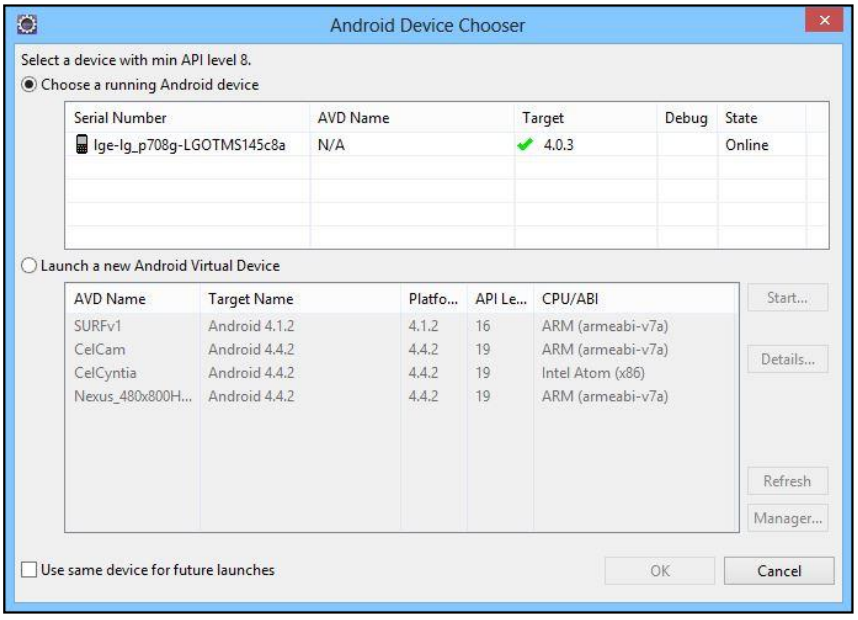


Figura II-5 Smartphone Alcatel One Touch Pop C3 con versión 4.2.2 del sistema operativo Android.

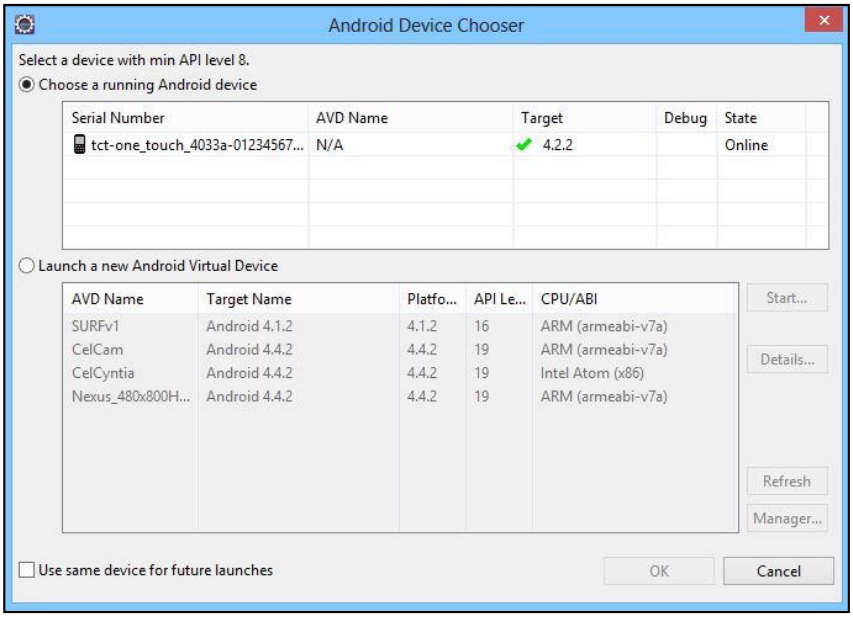
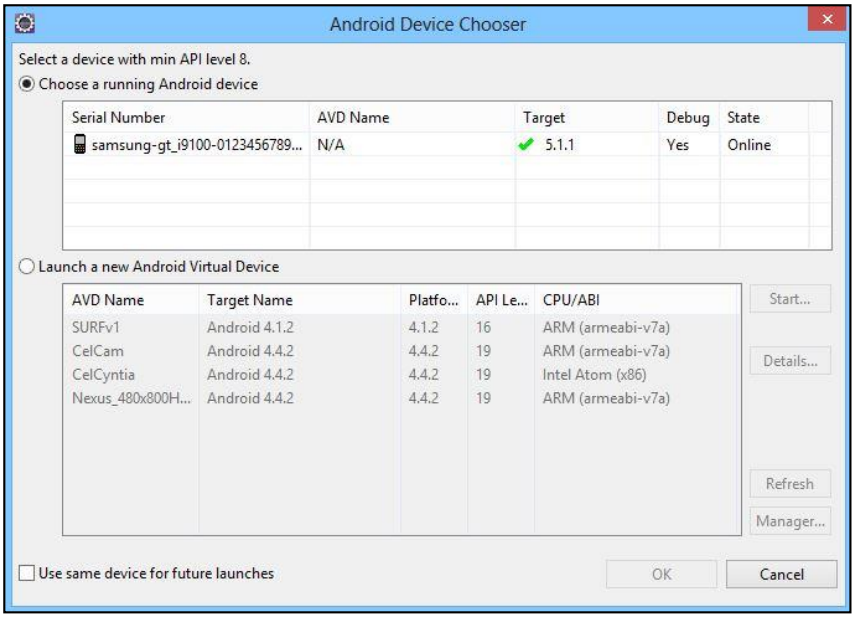


Figura II-6 Smartphone Samsung GALAXY S II GT-I9100 con versión 5.1.1 del sistema operativo Android.



ANEXO III

Artículos

A Novel Approach for Face Authentication Using Speeded Up Robust Features Algorithm

Cyntia Mendoza-Martinez*, Jesus Carlos Pedraza-Ortega, and Juan Manuel Ramos-Arreguin

Universidad Autonoma de Queretaro, Queretaro, Mexico
isc_cmendoza@hotmail.com

Abstract. In this paper, we propose a modified face authentication method based on the image preprocessing (histogram equalization, HE) and with SURF algorithm (Speeded Up Robust Features) in the feature extraction step. In particular, our methodology aims at determining a person's authenticity when he/she has a few facial expressions, different backgrounds or a variance in lighting. We evaluated the performance of this method using public face databases like The Extended Cohn-Kanade Dataset (CK+) and Caltech Faces. We made some test using sixty images (thirty per database), Equal (E) or Different (D) and according to the match between images (for example Image 1 and Image 2) and a defined threshold, our method determines if a person is authenticated or not. The results showed that with the database CK+ was obtained 93% and with Caltech Faces 86% of accuracy in the authentication process, these results were compared with those obtained by some algorithms like LDA, PCA, SIFT and SURF (without preprocessing) and we can conclude that the authentication rate was improved.

Keywords: Biometrics, Computer vision, Face authentication, Image processing, OpenCV, Python, SURF.

1 Introduction

Biometrics refers to the identification of a person on the basis of their physical and behavioral characteristics. Some biometric systems include features of fingerprints, hand geometry, voice, iris, etc., and can be used for identification. Most biometric systems are based on the collection and comparison of biometric characteristics which can provide identification [1]. In the recent years, a number of recognition and authentication systems based on biometric measurements have been proposed. Algorithms and sensors have been developed to acquire and process many different biometric traits. Moreover, the biometric technology is being used in novel ways, with potential commercial and practical implications to our daily activities [2]. Today's world security issues are the most important segment among all. Therefore, a segment of authentication and face recognition plays a major role. When a person or a system checks the person's identity against another person then we are in process of authentication. That means the one who is authenticated can confirm that he/she is the person with whom is compared.

* Corresponding author.

A. Gelbukh et al. (Eds.): MICAI 2014, Part I, LNAI 8856, pp. 356–367, 2014.

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.

2014 11th International Conference on Electrical Engineering, Computing Science and Automatic Control (CCE)

Automatic Segmentation of Mammograms Using a Scale-Invariant FeatureTransform and K-Means Clustering algorithm

Luis. A. Salazar-Licea*, C. Mendoza, M.A. Aceves, J.C. Pedraza
Facultad de Informática,
Universidad Autónoma de Querétaro
Queretaro, Mexico
*Corresponding author: l.antonyo.al@gmail.com

Alberto Pastrana-Palma
División de Estudios de Posgrado
Facultad de Contaduría y Administración,
Universidad Autónoma de Querétaro
Queretaro, Mexico

Abstract— **In this work, a Scale-Invariant Feature Transform method, together with a K-means clustering is used in order to find regions of interest (ROI's) in mammograms. This paper focuses on presenting a tool that can improve the search of suspicious areas that contain abnormalities, leaving the final decision to the radiologist. The methodology is divided into three sections: first, a pre-processing step that consist in acquiring image and reduction its size erasing the background leaving only the breast area and eliminating noise. The second step is to improve the image quality through image thresholding and histogram equalization limited contrast (CLAHE). Last step of the methodology is the location of regions of interest in the image and is done using Scale-Invariant Feature Transform (SIFT) as the main tool and is complemented with Binary Robust Independent Elementary Features (BRIEF) to find descriptors and as classifier K-Means Clustering. Finally in the results are presented the location of ROI's and they are compared with the position of abnormalities diagnosed by the Mammographic Image Analysis Society.**

Keywords—mammogram; image processing; segmentation; SIFT.

I. INTRODUCTION

Breast cancer consists in a disordered and abnormal growth of breast cells. The World Health Organization estimates that about 84 million people will die because this disease between 2005 and 2015. In Mexico, since 2006 breast cancer is the second highest cause of death in the age group 30 to 54 years, and ranks as the first cause of mortality from malignant tumors in women [2]. A mammogram is a radiographic test non-invasive of the mammary gland that can detect cancer up to two years before it can be felt and can reduce mortality up to 30% [3].

Among the disadvantages of this technique to make a diagnosis are: low differentiation in the appearance of cancerous tissue compared with normal parenchymal tissue; varied morphology of the findings; similarity between the morphologies of the findings; varied size of the findings; deficiencies in the skill to make the radiograph and visual fatigue or distraction of the radiologist. [4]

Typical steps of computer-assisted diagnosis are (Fig.1) [5]: Pre-processing which aim is to increase the image quality and reduce noise; Segmentation step its objective is to find regions of interest (ROI's) suspicious of containing anomalies; Detection step selects the best set of features in the region of interest and finally, based on the detection, is carried out the reducing of false positive and lesion classification.

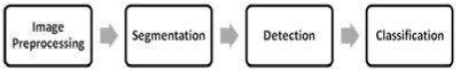


Fig. 1. Typical steps of the computer diagnostic

II. METHODS AND MATERIALS

This section is divided into three main sub sections: image preprocessing, image enhancement and location of regions of interest where are described all the methods used to create this work but first there is a part that described the materials and tools used.

A. Materials

The mammographic images analyzed in this work belong to the mini-MIAS (Mammographic Image Analysis Society) database from the UK National Breast Screening Programme [6]. This database contains 322 images; each image has a 200 micron pixel edge and 1024x1024 pixels of size. All developed algorithms were implemented entirely using open source tools such as Python language programming, Eclipse IDE and OpenCV libraries.

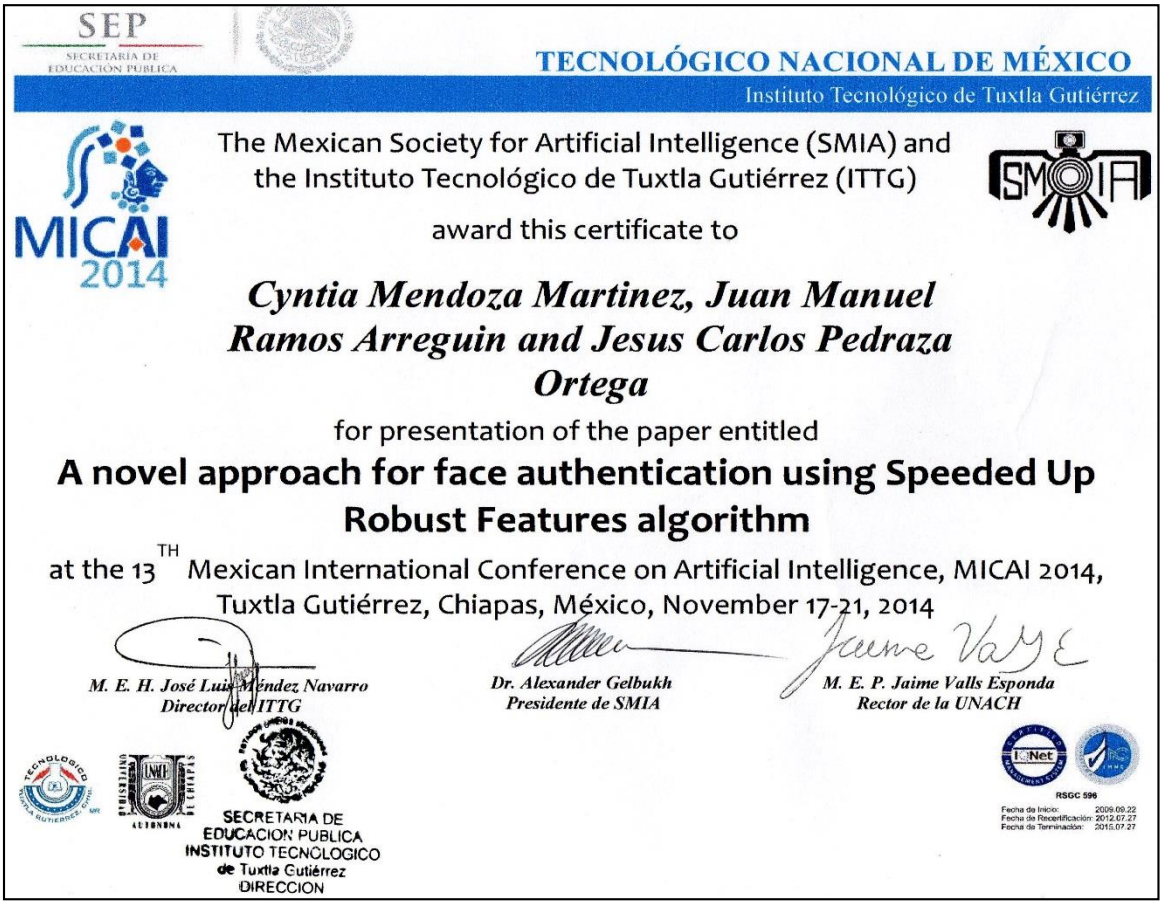
B. Image Preprocessing

This stage consists of perform an image pre-segmentation to acquire and select only the breast area and to eliminate noise in order to reduce processing time. The corner detector

978-1-4799-6230- 3/14/$31.00 ©2014 IEEE

ANEXO IV

Ponente en el congreso internacional MICAI 2014



SEP
SECRETARÍA DE EDUCACIÓN PÚBLICA

TECNOLÓGICO NACIONAL DE MÉXICO
Instituto Tecnológico de Tuxtla Gutiérrez

MICAI 2014

The Mexican Society for Artificial Intelligence (SMIA) and the Instituto Tecnológico de Tuxtla Gutiérrez (ITTG)

award this certificate to

Cyntia Mendoza Martinez, Juan Manuel Ramos Arreguin and Jesus Carlos Pedraza Ortega

for presentation of the paper entitled

A novel approach for face authentication using Speeded Up Robust Features algorithm

at the 13TH Mexican International Conference on Artificial Intelligence, MICAI 2014, Tuxtla Gutiérrez, Chiapas, México, November 17-21, 2014

M. E. H. José Luis Méndez Navarro
Director del ITTG

Dr. Alexander Gelbukh
Presidente de SMIA

M. E. P. Jaime Valls Esponda
Rector de la UNACH

SECRETARIA DE EDUCACION PUBLICA
INSTITUTO TECNOLOGICO de Tuxtla Gutiérrez
DIRECCION

RSGC 596
Fecha de Inicio: 2009.09.22
Fecha de Recertificación: 2012.07.27
Fecha de Terminación: 2015.07.27

ANEXO V

Actividades complementarias

Presentación de artículo en congreso internacional CCE 2014

Centro de Investigación y de Estudios Avanzados
del
Instituto Politécnico Nacional

Cinvestav

The Organizing Committee of the 2014 11th International Conference on Electrical Engineering, Computing Science and Automatic Control (CCE 2014) awards the present RECOGNITION TO:

CCE

Luis Antonio Salazar Licea, Cyntia Mendoza-Martínez, Marco Antonio Aceves Fernandez, Alberto Pastrana Palma and Jesus Carlos Pedraza Ortega

For the presentation of the paper entitled:

Automatic Segmentation of Mammograms Using a Scale-Invariant FeatureTransform and K-Means Clustering algorithm

Ciudad del Carmen, Campeche, México
September 29 – October 3, 2014

Dr. Carlos Coello Coello
Co-Chair of CCE 2014

Dr. José Antonio Moreno Cadenas
Co-Chair of CCE 2014

Dr. Alexander Poznyak Gorbatch
Co-Chair of CCE 2014

Estancia de investigación en la Universidad Autónoma de Baja California

Universidad Autónoma de Baja California

FACULTAD DE INGENIERÍA
CAMPUS MEXICALI

Mexicali, Baja California, 23 de julio del 2015

Dr. Jesús Carlos Pedraza Ortega
Coordinador de la Maestría en Ciencias de la Computación
Presente

Por este medio me permito enviarle un cordial saludo. Así mismo, hago de su conocimiento que fue terminada exitosamente la estancia académica realizada por la Ing. Cyntia Mendoza Martínez. Durante su estancia en la Facultad de Ingeniería de la Universidad Autónoma de Baja California, Cyntia realizó cabalmente las actividades programadas.

Desarrolló una aplicación demostrativa de tratamiento de imágenes para iOS y la instaló en su teléfono iPhone. Los participantes del taller que impartió Cyntia aprendimos mucho durante el curso. Cyntia estructuró muy bien el contenido del curso, sus presentaciones fueron claras y se destacó por su dominio del tema y su profesionalismo.

Considero que fue una estancia provechosa para ambas partes. Sin más por el momento, me despido.

Atentamente

Dra. Cecilia Margarita Curlango Rosas
Investigadora UABC
Correo electrónico: curlango@uabc.edu.mx
Teléfono: +52 (686) 566-4270 ext. 1340

Instructor del Curso

“Procesamiento de Imágenes y Reconocimiento de objetos”

UNIVERSIDAD AUTÓNOMA DE BAJA CALIFORNIA
FACULTAD DE INGENIERÍA

Otorga la presente

Constancia

A la ISC

Cyntia Mendoza Martínez

Por impartir el curso

“Procesamiento de Imágenes y Reconocimiento de Objetos”

a profesores y alumnos de la Facultad de Ingeniería, durante los días 3 al 11 de junio de 2015

Mexicali, Baja California, a 11 de junio de 2015
“POR LA REALIZACIÓN PLENA DEL HOMBRE”

UNIVERSIDAD AUTONOMA DE BAJA CALIFORNIA
FACULTAD DE INGENIERIA

M.C. Jorge Eduardo Ibarra Esquer
Responsable del P.E. Ing. en Computación

Dr. Daniel Hernández Balbuena
Director

Colaboración como miembro del comité organizador en el 13er Congreso Nacional de Mecatrónica 2014

Asociación Mexicana de Mecatrónica A.C.

EN EL MARCO DE SU:

13° CONGRESO NACIONAL DE MECATRÓNICA

Otorga el presente

Reconocimiento a:

ASOCIACIÓN MEXICANA DE MECATRÓNICA A C

ISC. MENDOZA MARTÍNEZ CYNTHIA

ASOCIACIÓN MEXICANA DE MECATRÓNICA A.C.

POR SU PARTICIPACIÓN COMO MIEMBRO DEL COMITÉ ORGANIZADOR, EN EL 13 CONGRESO NACIONAL DE MECATRÓNICA, CON SEDE EN EL CENTRO DE NEGOCIOS, UAQ.

QUERÉTARO, QRO., DEL 30 DE OCTUBRE AL 1 DE NOVIEMBRE DEL 2014

DR. JUAN MANUEL RAMOS ARREGUÍN
PRESIDENTE DE LA ASOCIACIÓN MEXICANA DE MECATRÓNICA

Curso de entrenamiento de digitalización 3D VISI Series

VISI Series México

VISI Series México, S.A. de C.V.

Otorga el presente

Diploma

A: I.S.C. Cyntia Mendoza Martínez

Por su participación en el :

CURSO DE ENTRENAMIENTO DE DIGITALIZACIÓN 3D VISI Series

Con duración de 36 horas. Impartido en

UNIVERSIDAD AUTÓNOMA DE QUERÉTARO

Ing. Elías Hernández Moreno
Instructor

Ing. Raúl Moreno Espinosa
Director General

Certificación Microsoft