****

**UNIVERSIDAD PRIVADA DE TACNA**

**FACULTAD DE INGENIERIA**

**Escuela Profesional de Ingeniería de Sistemas**

**TITULO**

**“Aplicación biométrica basada en App para la autenticación de usuarios”**

Curso: Seguridad Informática

Docente: Ing. Oscar Jimenez Flores

**Huillca Umpiri, Willian Arturo (2015053793)**

**Panty Sihuayro, Juan Carlos (2014040952)**

**Tacna – Perú 2020**



**Aplicación biométrica basada en App para la autenticación de usuarios**

1. Introducción

Un sistema biométrico en general consta de componentes tanto hardware como softwares necesarios para el proceso de reconocimiento. Dentro del hardware se incluyen principalmente los sensores que son los dispositivos encargados de extraer la característica deseada. Una vez obtenida la información del sensor, será necesario realizar sobre ella las tareas de acondicionamiento necesarias, para ello se emplean diferentes métodos dependiendo del sistema biométrico utilizado. Por ello se han descrito los principales tipos de sistemas biométricos existentes:

• Reconocimiento de la huella dactilar

• Reconocimiento de la cara

• Reconocimiento de iris/retina

• Geometría de dedos/mano

• Autentificación de la voz

• Reconocimiento de la firma

Para cada uno de estos sistemas se ha descrito su funcionamiento y algunas de las técnicas que se utilizan para procesar los datos obtenidos a partir de los sensores.

Los sistemas biométricos se han desarrollado como respuesta a la creciente demanda de seguridad existente en la actualidad y aunque algunos de ellos son altamente fiables, ningún sistema es efectivo al 100%, y estos sistemas también son susceptibles de ser engañados.

1. Concepto de Biometría

**Todos los seres humanos tenemos características morfológicas únicas que nos diferencian. La forma de la cara, la geometría de partes de nuestro cuerpo como las manos, nuestros ojos y tal vez la más conocida, la huella digital, son algunos rasgos que nos diferencian del resto de seres humanos.**

**El concepto biometría proviene de las palabras bio (vida) y metría (medida), por lo tanto**

**con ello se infiere que todo equipo biométrico mide e identifica alguna característica propia de la persona. Biometría es el conjunto de características fisiológicas y de comportamiento que pueden ser utilizadas para verificar la identidad del individuo, lo cual incluye huellas digitales, reconocimiento del iris, geometría de la mano, reconocimiento visual y otras técnicas.**

**La medición biométrica se ha venido estudiando desde tiempo atrás y es considerada en la actualidad como el método ideal de identificación humana.**

1. Evolución histórica

Si nuestro cerebro encuentra similitudes suficientes entre alguno de sus recuerdos y lo que está escuchando en ese momento, entonces reconocemos a la persona que nos ha llamado. Si no, asumimos que estamos ante alguien a quien no conocemos. Del mismo modo, los animales reconocen a otros animales, incluidos los seres humanos, por características biométricas tales como el olor, el tacto o el timbre de la voz.

Por tanto, aunque se podría pensar en la biometría como una ciencia-ficción futurista, los principios básicos de la biometría eran comprendidos y utilizados miles de años antes. Está comprobado, que en la época de los faraones, en el Valle del Nilo (Egipto) se utilizaban los principios básicos de la biometría para verificar a las personas que participaban en diferentes operaciones comerciales y judiciales.

Muchas son las referencias de personas que, en la antigüedad, han sido identificados por diversas características físicas y morfológicas como cicatrices, medidas, color de los ojos, tamaño de la dentadura. Esta clase de identificación se utilizaba, por ejemplo, en las zonas agrícolas, donde las cosechas eran almacenas en depósitos comunitarios a la espera de que sus propietarios dispusieran de ellas. Los encargados de cuidar estos depósitos debían identificar a cada uno de los propietarios cuando estos hicieran algún retiro de su mercadería, utilizando para esta tarea principios básicos de biometría como eran sus rasgos físicos.

Luego, en el siglo IXX hubo un pico de interés por parte de investigadores en criminología, cuando intentaron relacionar características físicas con tendencias criminales. Esto resulto en una variedad de equipos de medición y gran cantidad de datos recogidos. Los resultados no eran concluyentes, pero la idea de medir las características físicas de un individuo parecía efectiva y el desarrollo paralelo de la identificación de huellas digitales se convirtió en la metodología internacional para identificación utilizada por las fuerzas policiales de todo el mundo.

1. Necesidad de Biometría y Objetivos

Durante todo el siglo pasado han sido muchas las empresas que han concentrado sus esfuerzos en desarrollar sistemas biométricos para garantizar su seguridad, así como lo han hecho los propios Departamentos de Defensa de varios países.

Encontrar un sistema infalible e inequívoco para reconocer personas es el objetivo último de la biometría.

Hoy en día contamos con una gran variedad de equipos capaces de identificar a las personas a partir de la información de alguna parte de su cuerpo como las manos, la retina, el iris, los dedos, las huellas dactilares, la voz, o la firma. Incluso se está investigando en la posibilidad de crear un sistema basado en el ADN.

Restringido a través de su historia por su costo elevado, una función cuestionable y proveedores transitorios, la identificación biométrica está experimentando ahora una aceptación creciente, no sólo en aplicaciones de alta seguridad tales como bancos e instalaciones gubernamentales, sino también en clubes de salud, la Villa Olímpica en Atlanta en 1996, control de clientes del seguro social y acceso a oficinas y plantas comerciales e industriales. Los costos han sido reducidos a un nivel razonable y la función y contabilidad de los dispositivos es hoy día satisfactoria.

De esta forma con los sistemas biométricos que reconocen las características singulares de las huellas digitales, por ejemplo, se logra evitar fraudes en la banca, en el sistema de salud por suplantación de pacientes, controlar el acceso en el desplazamiento de seres humanos al interior de las empresas, tiempos desperdiciados, accesos no deseados; sin necesidad de utilizar contraseñas, carnes, tarjetas magnéticas u otros medios de identificación vulnerables. Esto hace que los sistemas biométricos sean el medio más rápido y seguro mediante la utilización de la huella digital como validador de operaciones y de control de acceso.

1. Biometría Estática

**• HUELLA DACTILAR**

Las huellas digitales son características exclusivas de los primates. En la especie humana se forman a partir de la sexta semana de vida intrauterina y no varían en sus características a lo largo de toda la vida del individuo. Son las formas caprichosas que adopta la piel que cubre las yemas de los dedos. Están constituidas por rugosidades que forman salientes y depresiones. Las salientes se denominan crestas papilares y las depresiones surcos interpapilares. En las crestas se encuentran las glándulas sudoríparas. El sudor que éstas producen contiene aceite, que se retiene en los surcos de la huella, de tal manera que cuando el dedo hace contacto con una superficie, queda un residuo de ésta, lo cual produce un facsímil o negativo de la huella.



**Identificando patrones.**

A simple vista, el patrón que siguen las líneas y surcos de una huella se puede clasificar según tres rasgos mayores: arco, lazo y espiral. Cada dedo presenta al menos una de estas características. Por otro lado, en determinados puntos las líneas de la huella dactilar se cortan bruscamente o se bifurcan. Estos puntos reciben el nombre de minucias, y juntos suman casi el 80% de los elementos singulares de una huella.



Todo esto da lugar a un patrón complejo único para cada individuo, distinto incluso en gemelos idénticos. En concreto, se estima que la probabilidad de que dos personas tengan las mismas huellas dactilares es aproximadamente de 1 en 64.000 millones.

Cuando se digitaliza una huella, los detalles relativos a las líneas (curvatura, separación,...), así como la posición absoluta y relativa de las minucias extraídas, son procesados mediante algoritmos que permiten obtener un índice numérico correspondiente a dicha huella. En el momento en que un usuario solicita ser identificado, coloca su dedo sobre un lector (óptico, de campo eléctrico, por presión,...) y su huella dactilar es escaneada y analizada con el fin de extraer los elementos característicos y buscar su homóloga en la base de datos. El resultado es un diagnóstico certero en más del 99% de los casos. Las técnicas utilizadas para la comparación de la huella dactilar se pueden clasificar en dos categorías:

La técnica de puntos Minutia primero encuentran estas minucias y posteriormente procede a su colocación relativa en el dedo. Es difícil extraer los puntos de las minucias exactamente cuando la huella dactilar es de baja calidad. También este método no considera el patrón global de crestas y de surcos.

El método correlación puede superar algunas de las dificultades de la comparación por puntos Minutia; sin embargo, tiene algunos inconvenientes propios. Las técnica de correlación requieren una localización precisa de un punto de registro y se ve afectada por el desplazamiento y rotación de la imagen.

Clasificación de la Huella La clasificación de las huellas dactilares es una técnica consistente en asignar a una huella uno de los varios tipos previamente especificados en la literatura y registrarla con un método de indexación de las direcciones. Una huella dactilar de entrada es primeramente clasificada a un nivel grueso en uno de los tipos:

● Whorl

● Lazo derecho

● Lazo izquierdo

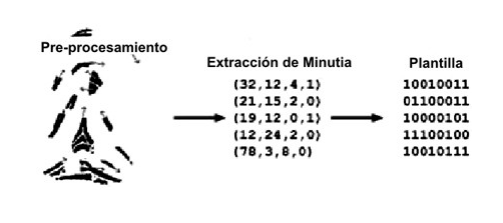
● Arco

● Tented el arco

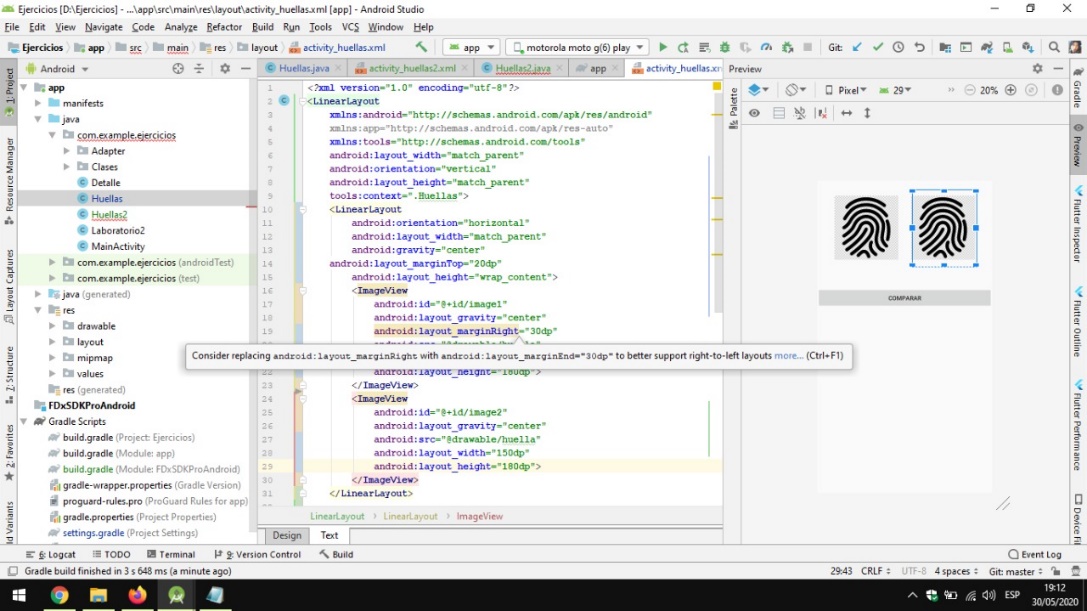
y entonces, en un nivel más fino, se compara con el subconjunto de la base de datos que contiene solamente ese tipo de huella dactilar. Se utilizan algoritmos desarrollados para identificar a cual de estos tipos de pertenece una huella en concreto.

**Realce de la Huella**

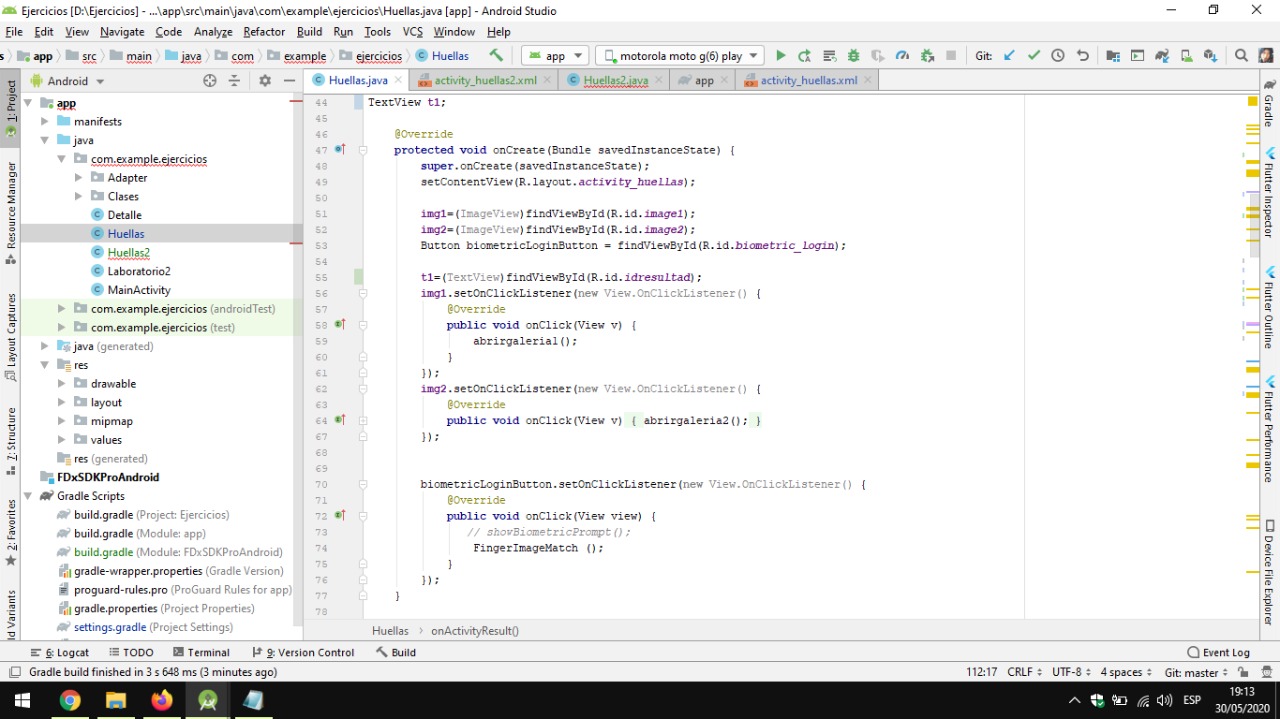
Un paso crítico en la clasificación automática de la huella dactilar está en extraer mediante un algoritmo las minucias de las imágenes de la huella dactilar de la entrada. El funcionamiento de un algoritmo de extracción de las minucias confía totalmente en la calidad de las imágenes de la huella dactilar de la entrada. Para asegurarse de que el funcionamiento de un sistema automático de identificación/verificación de huella dactilar sea robusto con cierta independencia de la calidad de las imágenes de la huella dactilar, es esencial incorporar un algoritmo del realce de la huella dactilar en el módulo de la extracción de las minucias. De este modo se puede mejorar de forma adaptativa la claridad de las estructuras de la cresta y del surco de las imágenes de las huellas dactilares de entrada.



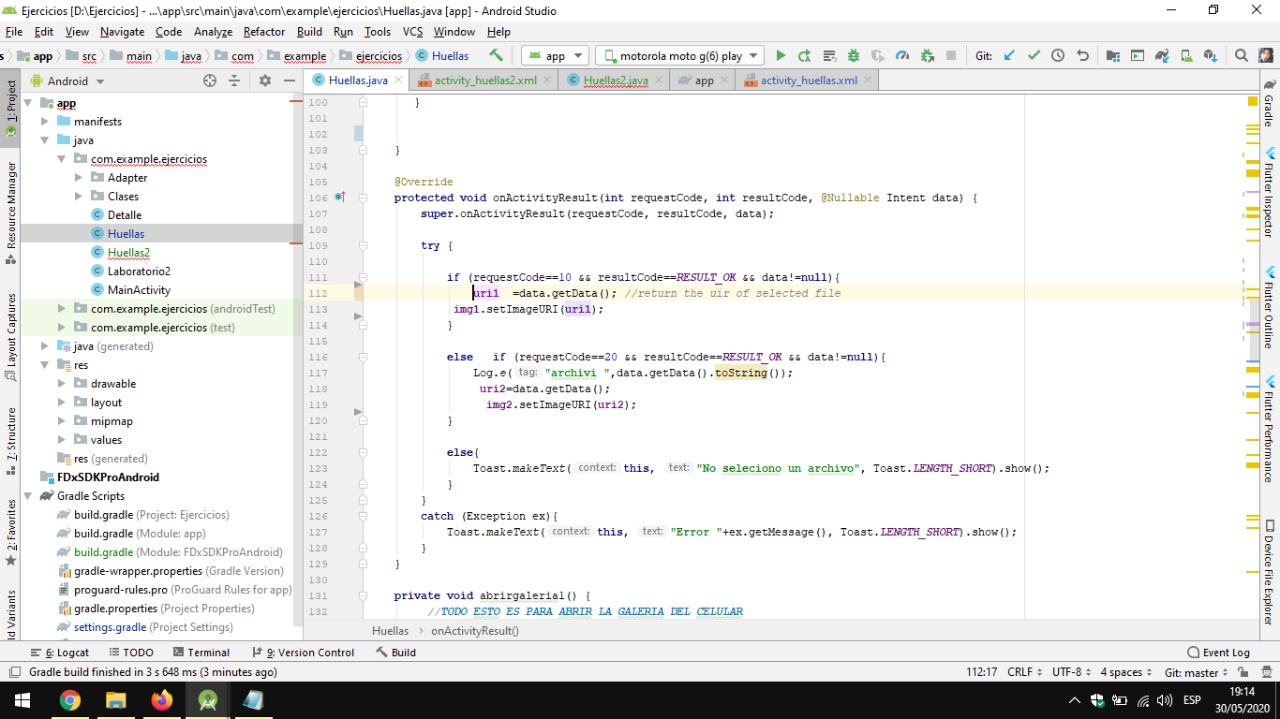
1. Prototipos:



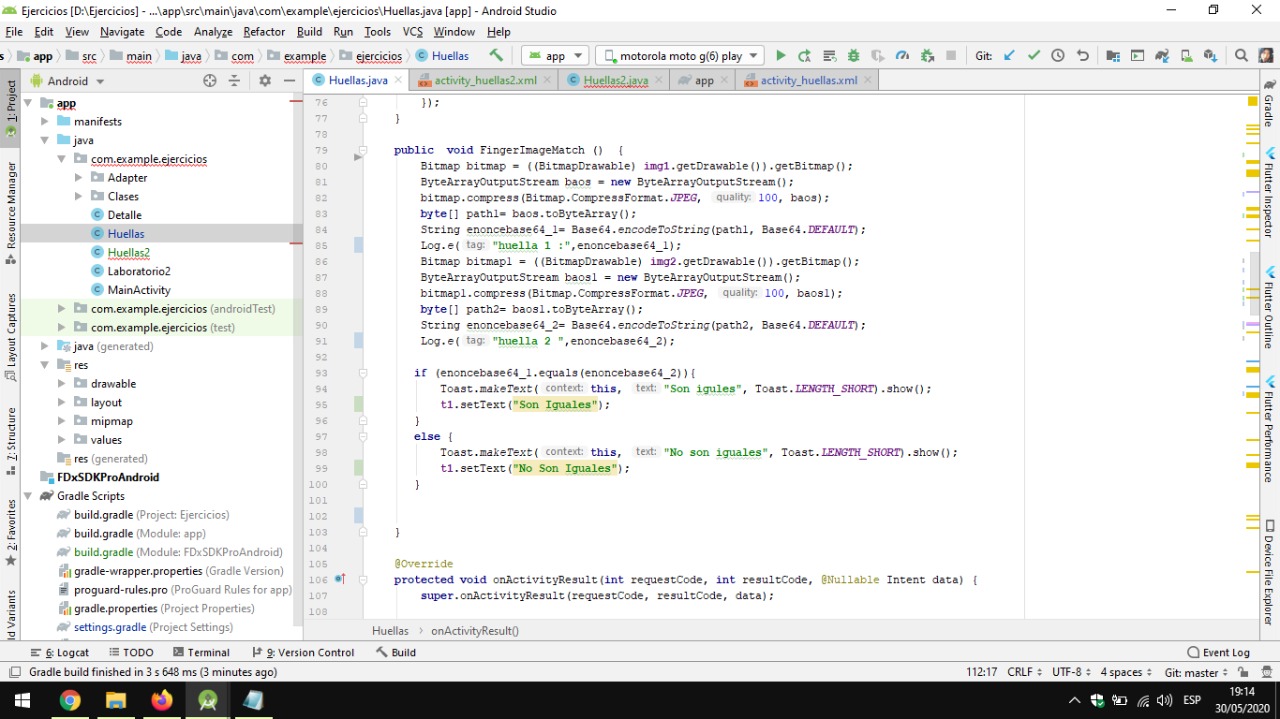
Declaración de las herramientas



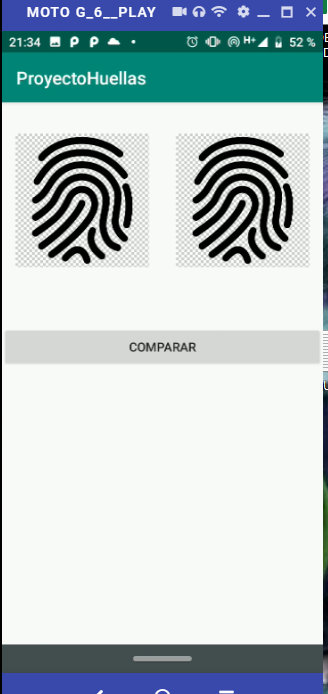
Recibimos las huellas y la ponemos en el imageView



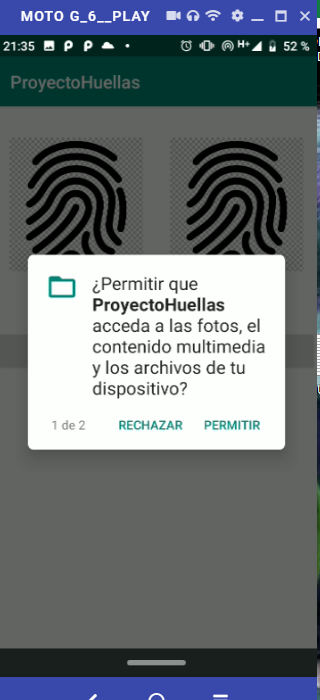
Y aquí convertimos las dos imágenes a base 64 y la comparamos



1. FUNCIONAMIENTO DE LA APLICACION:



Primero iniciamos la aplicación



Aceptamos los permisos para que podamos buscar las imágenes



Abrimos la galería para buscar a la imagen



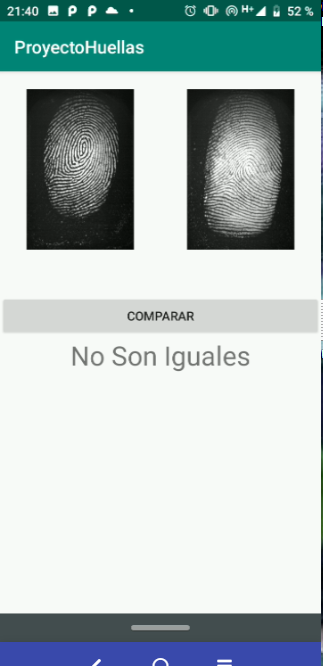
Seleccionamos la foto que deseamos comparar



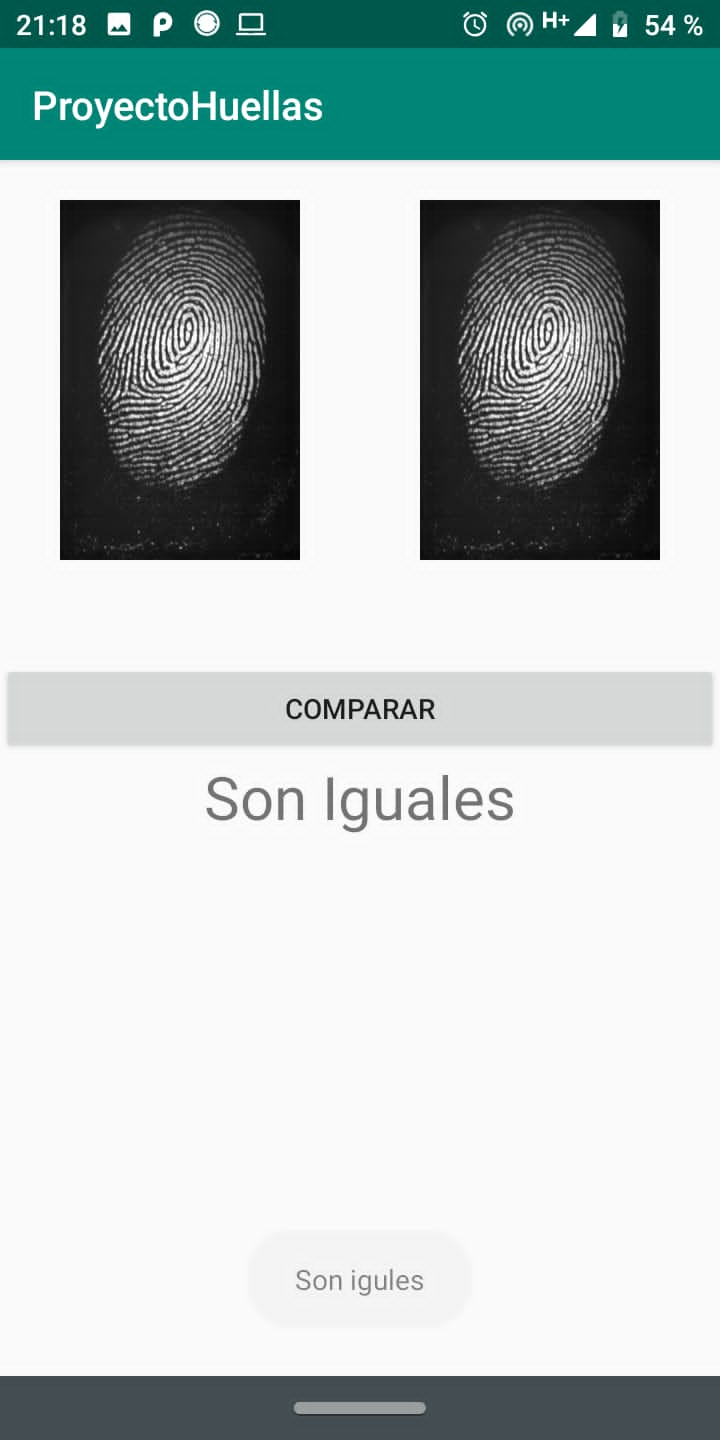
Y nos aparecerá en el primer imageview



Luego buscamos otra huella de la misma forma que la primera



Luego hacemos click en el botón para verificar si las huellas coinciden en este caso las huellas son diferentes y nos muestra que no son iguales



1. RESULTADOS

A través de esta aplicación pudimos detectar las huellas dactilares y poder hacer diferentes comparaciones con las imágenes que nos brindaron en los cuales pudimos detectar que algunos casos las huellas son iguales es porque coinciden los códigos en base 64 al momento de hacer la comparación con las otras imágenes en caso contrario al hacer la comparación si se detecta que el código en base 64 son diferentes determinaría la comparación no son iguales esos serían los resultados tomados en esta aplicación.

1. CONCLUSIONES

Para concluir con esta [investigación](https://www.monografias.com/trabajos11/norma/norma.shtml) sobre el uso de las huellas dactilares debemos mencionar que son procesos efectivos pero en aplicaciones básicas y pudieran ser utilizados como lo son controlar la asistencia del [personal](https://www.monografias.com/trabajos11/fuper/fuper.shtml) o de alumnos, etc.

La identificación huella dactilar desde hace muchos años se ha convertido en la técnica biométrica más usada debido a la gran investigación que se hace realizado en las huellas dactilares y análisis de huella dactilar como fuentes de autenticación en sistemas de seguridad.

Sin embargo en el futuro se está planeando el uso de la huella dactilar para tener acceso a información más detallada como lo son los historiales clínicos cabe decir que esto sería un proceso nivel mundial, por lo que los sistemas o base de datos que guarden la información deberán ser de gran capacidad para albergar toda la información y así también deberá contar con un [procesador](https://www.monografias.com/trabajos5/sisope/sisope.shtml) de alto rendimiento para no tener saturaciones.