RECONOCIMIENTO DE PATRONES EN HUELLAS DIGITALES UTILIZANDO MATLAB

Otoniel Silva Delgado[1,a], Oscar Juan Jiménez Flores[2,b]

RESUMEN

El objetivo de este estudio es el uso de huellas digitales para determinar la identidad de un individuo a través de extraer y procesar minucias. La herramienta por emplear es Matlab, en la que se procesa una imagen a modo de matriz y mediante bucles y máscaras se puede obtener las minucias de interés. El algoritmo, en primera instancia, binariza la imagen, de tonos grises a una imagen en blanco y negro. Una vez realizado lo anterior se hacen unas pequeñas correcciones en la imagen, por ejemplo usar el comando *bwmorph* junto con algunas de sus opciones; *clean,* que remueve los pixeles isolados con valor 1 rodeados de 8 vecinos de valor 0. *fill* remueve los pixeles isolados en la imagen, los pixeles de valor 0 rodeados de 8 vecinos de valor 1, y los convierte en 1. Y como última instancia la opción *thin* que adelgaza la línea que se dibuja con los pixeles de valor 1, y se genera una línea con el ancho de un pixel. En conclusión, se ha diseñado un algoritmo que es capaz de extraer los puntos de interés de una muestra y compararla con otra, contra un porcentaje de error menor de 30%, y el cual verifica si las muestras son del mismo individuo o de diferentes.

Palabras clave: *identidad, seguridad, sistema, biométrica, electrónica, tecnología, huellas dactilares.*

PATTERN RECOGNITION IN FINGER PRINTS USING MATLAB

ABSTRACT

The main objective of this study is the use of fingerprints to determine the identity of an individual through extracting and processing minutiae. Materials and Method.- The tool to be used is Matlab, in which process an image as a matrix and using loops and masks can get the minutiae of interest. Earnings.- algorithm in the first binarized image, gray image to a black and white tones. Once they have done the previous few small corrections are made in the image, such as using "bwmorph" command together with some of your options, "clean" which removes pixels with value 1 Isolados surrounded by 8 neighbors value of 0. " fill "Isolados removes pixels in the image, the pixel value 0 surrounded by 8 neighbors of value 1 and becomes 1. And ultimately the" thin "thin the line is drawn with pixels of value 1 and a line is generated with the width of a pixel. Conclusion.- has designed an algorithm that is able to extract the points of interest of a sample and compare it with another, against a percentage of error of less than 30%, which verifies whether the samples are from the same individual or different.

Keywords: *Identity, security, system, biometric, electronic, technology, fingerprint.*

[1.] Escuela profesional de Ingeniería de Sistemas e Informática. Universidad José Carlos Mariátegui. Moquegua, Perú
[a.] Ingeniero de Sistemas e Informática. Magíster en Docencia Universitaria e investigación, director de la Escuela Profesional ISI. ottoniel_silva@hotmail.com
[2.] Universidad Latinoamericana CIMA. Tacna, Perú.
[b.] Ingeniero de Sistemas e Informática. Magíster Administración y Gestión de Empresas, Consultor en Auditoría y Seguridad de la Información. oscar_qbiz@hotmail.com

Recibido: 19-11-2015 Aprobado: 15-12-2015

INTRODUCCIÓN

En la actualidad, determinar la identidad de un individuo se ha convertido en uno de los mayores desafíos para los sistemas de seguridad biométricos que, a su vez, cumplen una función importante en nuestra sociedad; algunos cuestionamientos son inevitables al momento de referirnos a identidad como: ¿es la persona que dice ser?, ¿este individuo debe tener accesos al sistema?, o ¿tiene este empleado la facultad para realizar dicha transacción?; muchas preguntas similares son hechas millones de veces al día por cientos de millones de organizaciones en servicios financieros, médicos, de comercio electrónico, telecomunicaciones, gobierno, etc. Con la rápida evolución de las tecnologías de información, las personas están cada vez más conectadas electrónicamente y, al mismo tiempo, menos seguras.

Una amplia variedad de sistemas requieren esquemas de autenticación de personal, fiables para confirmar o determinar la identidad de las personas que solicitan sus servicios. El propósito de estos sistemas biométricos es asegurar que el servicio requerido sea asequible a un usuario legítimo, y no cualquier otra persona. Algunos ejemplos de estos sistemas son los que conceden accesos seguros a edificios, sistemas de cómputo, *laptops*, celulares y cajeros automáticos. En ausencia de sistemas de autentificación más robustos, estos serían simplemente vulnerables al paso de un impostor.

Tradicionalmente, *passwords* y tarjetas han sido usados para restringir el acceso a los sistemas. Las ventajas de estos sistemas tradicionales de identificación personal son la simplicidad de uso, la fácil integración y los costos bajos.

Además, estos alcances no están basados en ningún atributo propio del individuo para hacer una identificación personal, en lugar de tener un número de desventajas como que las tarjetas puedan ser robadas, olvidadas o ingresadas incorrectamente; un *password* o PIN puede ser olvidado o adivinado por algún impostor. La seguridad puede ser fácilmente burlada en estos sistemas cuando un *password* es divulgado a un usuario sin autorización o una tarjeta es robada; además *passwords* sencillos son fáciles de adivinar, y los más difíciles tal vez puedan resultar difíciles de recordar por el propio usuario.

Por otro lado, tenemos la biometría en el mundo de la seguridad computarizada, la cual se refiere a las técnicas de autenticación que recaen en las mediciones fisiológicas y características individuales que puedan ser automáticamente verificadas. En otras palabras, todos tenemos atributos únicos y personales que pueden ser usados para distinción de individuos, incluyendo huellas digitales, los patrones de retina, o características de la voz. La combinación de dos o más métodos de autentificación se está convirtiendo en un estándar en medios de seguridad. Algunas computadoras personales hoy en día pueden incluir un lector de huella digital donde el usuario coloca su dedo índice para probar su identidad. La computadora analiza la huella digital para determinar quién es y basado en la identidad sigue un código o *password* permitiéndo acceder a diferentes niveles de usuario. Los niveles de acceso pueden incluir el hecho de abrir y/manipular cierta información.

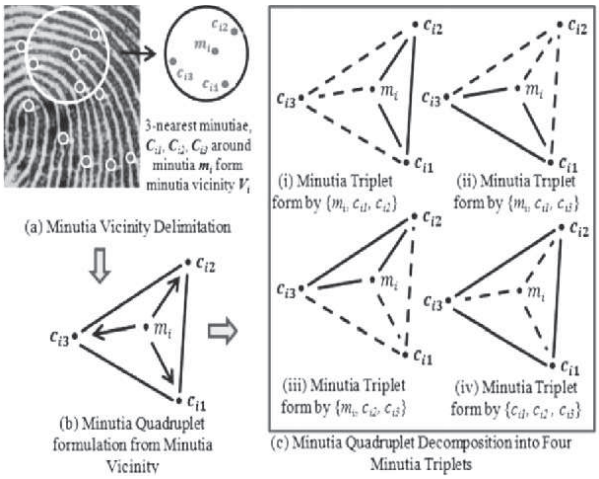
MARCO TEÓRICO

Un creciente número de tecnologías biométricas han estado siendo procesadas en el paso de los años, pero solo en los últimos 5 años son estos sistemas los que llevan la delantera, por ser altamente desarrollados. Algunas tecnologías son aplicadas de mejor manera según la aplicación, y otras son mejor aceptadas por los usuarios. Podemos mencionar siete tecnologías biométricas que llevan la delantera:

- Reconocimiento facial.
- Reconocimiento de huella digital.
- Geometría de la mano.
- Reconocimiento del iris.
- Reconocimiento de la firma.
- Reconocimiento de voz.

Reconocimiento de huella digital

Figura 1. Patrones que considerar en el análisis de huellas digitales.

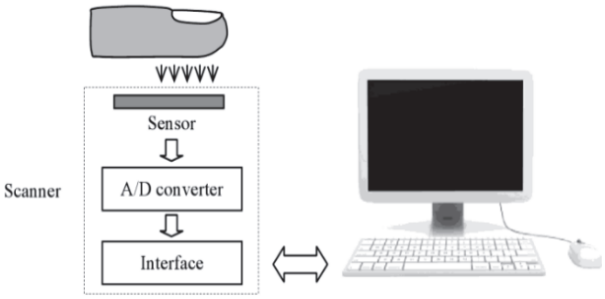


Fuente Artículo: A two-dimensional random projected minutiae vicinity decomposition-based cancellable fingerprint template. Zhe Jin, Bok-Min Goi, Andrew Teoh, Yong Haur Tay. Year 2013, Page 4.

Aunque no se ha establecido científicamente, se cree que las huellas digitales son únicas en cuanto a las personas así como únicas en cuanto a todos los dedos de la misma persona. Inclusive, gemelos idénticos, quienes tienen un ADN similar, tienen huellas digitales diferentes. Tradicionalmente, los patrones de estas han sido extraídos creando una impresión de tinta de la huella digital sobre papel.

La era electrónica ha iniciado una serie de sensores compactos que proporcionan imágenes digitales de estos patrones. Estos sensores pueden ser fácilmente incorporados en periféricos de computación existentes, como el mouse o el teclado. Esto ha dirigido el incremento del uso automático de identificación por huella digital, en ambos sistemas civiles y legales

Figura 2. Diagrama de reconocimiento de huella digital mediante escáner al computador.



Fuente Libro: Handbook of fingerprint recognition. Maltoni, Maio, Jain, Prabhakar. Year 2009, Page 58.

PROPUESTA

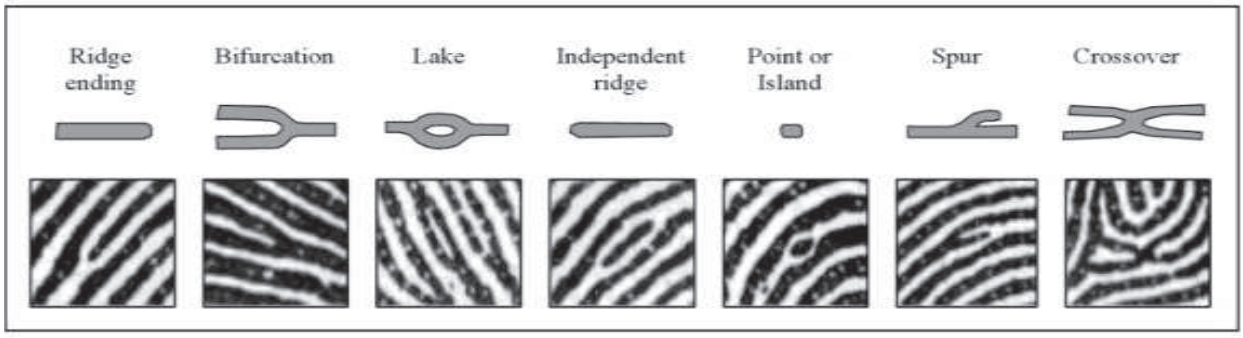
La singularidad de una huella digital es determinada por la topografía en los relieves de la yema de los dedos, y la presencia de ciertas anomalías llamadas minucias. Típicamente, la configuración global definida por estas anomalías, es usada para determinar la clase o el tipo de huella digital, mientras que la distribución de las minucias es usada para comparar y establecer la similitud entre dos huellas digitales. Por otro lado, tenemos las minucias, en términos de huellas digitales, son los puntos de interés, como bifurcaciones y terminaciones, entre otros.

Una vez analizado y comprendido cómo se identifica una huella digital, los usos industriales, legales o civiles que tiene, se debe realizar una interfaz donde podamos comparar una huella digital, con las que tengamos en una base de datos, o contra cualquier otra que se ingrese. Esto se logra una vez obteniendo la imagen de interés, para generar su procesamiento.

RESULTADOS

El algoritmo, en primera instancia, binariza la imagen, o dicho en otras palabras, la transforma de una imagen de tonos grises a una imagen en blanco y negro. Una vez realizado lo anterior se hacen unas pequeñas correcciones en la imagen,

Figura 3. Ejemplo de minucias.



Fuente Libro: Handbook of fingerprint recognition. Maltoni, Maio, Jain, Prabhakar. Year 2009, Page 99.

como es usar el comando *bwmorph* junto con algunas de sus opciones; *clean* , que remueve los pixeles isolados con valor 1 rodeados de 8 vecinos de valor 0. *Fill,* remueve los pixeles isolados en la imagen, los pixeles de valor 0 rodeados de 8 vecinos de valor 1, y los convierte en 1. Y como última instancia la opción *thin* adelgaza la línea que se dibuja con los pixeles de valor 1, y se genera una línea con el ancho de un pixel. El algoritmo funciona identificando las frecuencias de ciertas minucias en la huella digital, para realizar esto, sometemos a nuestra imagen a ser comparada pixel por pixel, en sus 8 vecinos, identificando de esta manera si un pixel es un punto final de una línea, una bifurcación, o una cresta hacia arriba o hacia abajo. Las frecuencias se comparan contra las de otra imagen tendiendo un rango de aceptación de 30%.

Codificación base en matlab para las pruebas de la investigación

```
function varargout = HuellaDigital1(varargin)
gui_Singleton = 1;
gui_State = struct('gui_Name',       mfilename, ...
                   'gui_Singleton',  gui_Singleton, ...
                   'gui_OpeningFcn', @HuellaDigital1_OpeningFcn, ...
                   'gui_OutputFcn',  @HuellaDigital1_OutputFcn, ...
                   'gui_LayoutFcn',  [] , ...
                   'gui_Callback',   []);
if nargin && ischar(varargin{1})
    gui_State.gui_Callback = str2func(varargin{1});
end

if nargout
    [varargout{1:nargout}] = gui_mainfcn(gui_State, varargin{:});
else
    gui_mainfcn(gui_State, varargin{:});
end

function HuellaDigital1_OpeningFcn(hObject, eventdata,
handles, varargin)
handles.output = hObject;
guidata(hObject, handles);

function varargout = HuellaDigital1_OutputFcn(hObject,
eventdata, handles)
varargout{1} = handles.output;

function cargarimagen_Callback(hObject, eventdata, handles)
[FileName Path]=uigetfile({'*.jpg;*.bmp;*.png'},'Seleccionar
Huella');
if isequal(FileName,0)
return
else

huella1=imread(strcat(Path,FileName));
[i j]=size(huella1);

%Binarizar
for j=1:j
    for i=1:i
        if huella1(i,j)>=25 %umbral en escala de gris
            huella1(i,j)=0;
        else
            huella1(i,j)=1;
        end
    end
end

%Limpiar y rellenar la imagen
huella1=bwmorph(huella1,'clean');
huella1=bwmorph(huella1,'fill');

%Maximizar el adelgazamiento de la linea
huella1=bwmorph(huella1,'thin');
huella1=bwmorph(huella1,'thin');
huella1=bwmorph(huella1,'thin');

imshow(huella1,'Parent',handles.axes1);

end
handles.huella1=huella1;
guidata(hObject,handles)

function cargarimagen2_Callback(hObject, eventdata, handles)
[FileName        Path]=uigetfile({'*.jpg;*.bmp;*.png'},'Seleccionar
Huella');
if isequal(FileName,0)
return
else

huella3=imread(strcat(Path,FileName));
[i j]=size(huella3);

%Binarizar
for j=1:j
    for i=1:i
        if huella3(i,j)>=25 %umbral en escala de gris
            huella3(i,j)=0;
        else
            huella3(i,j)=1;
        end
    end
end
%Limpiar y rellenar la imagen
huella3=bwmorph(huella3,'clean');
huella3=bwmorph(huella3,'fill');

%Maximizar el adelgazamiento de la linea
huella3=bwmorph(huella3,'thin');
huella3=bwmorph(huella3,'thin');
huella3=bwmorph(huella3,'thin');

imshow(huella3,'Parent',handles.axes2);

end
handles.huella3=huella3;
guidata(hObject,handles)

function autenticar_Callback(hObject, eventdata, handles)

huella1=handles.huella1;
huella3=handles.huella3;

%Procesamiento de cada imagen

%Primera Huella
%Agregar marco, filas y columna
[i j]=size(huella1);
huella2=zeros(i+2,j+2);
[n m]=size(huella2);
huella2(2:n-1,2:m-1)=huella1(1:i,1:j);

%Puntos de interés, para reconocimiento
endpoint1=0;
branchpoint1=0;
bottompoint1=0;
toppoint1=0;

%Generación de patrones/vectores de reconocimiento
for m=2:m-1
    for n=2:n-1
        %Generar una máscara de 3x3 para cada pixel
        mascara=huella2(n-1:n+1,m-1:m+1);
        contador=0; %contador que cuenta números 1

        %Bucle, se cuentan los 1 en cada máscara
        for j=1:3
            for i=1:3
                if mascara(i,j)==1
                  contador=contador+1;
                end
            end
        end

        %Condicionantes para contar puntos de interés
        if contador==2 && mascara(2,2)==1 %si existen
solamente dos 1, es un punto final
            endpoint1=endpoint1+1;
```

```
      elseif contador==4 && mascara(2,2)==1 %si existen
cuatro 1, es una bifurcación
         branchpoint1=branchpoint1+1;
      end

      if mascara==[1 0 1;0 1 0;0 0 0] %Se cuentan los valles
         bottompoint1=bottompoint1+1;
      elseif mascara==[0 0 0;0 1 0;1 0 1] %Se cuentan las
crestas
         toppoint1=toppoint1+1;
      end

   end
end

%Segunda Huella
%Agregar marco, filas y columna
[i j]=size(huella3);
huella4=zeros(i+2,j+2);
[n m]=size(huella4);
huella4(2:n-1,2:m-1)=huella3(1:i,1:j);

%Puntos de interés, para reconocimiento
endpoint2=0;
branchpoint2=0;
bottompoint2=0;
toppoint2=0;

%Generación de patrones/vectores de reconocimiento
for m=2:m-1
   for n=2:n-1
      %Generar una máscara de 3x3 para cada pixel
      mascara=huella4(n-1:n+1,m-1:m+1);
      contador=0; %contador que cuenta números 1

      %Bucle, se cuentan los 1 en cada máscara
      for j=1:3
         for i=1:3
            if mascara(i,j)==1
               contador=contador+1;
            end
         end
      end

      %Condicionantes para contar puntos de interés
      if contador==2 && mascara(2,2)==1 %si existen
solamente dos 1, es un punto final
         endpoint2=endpoint2+1;
      elseif contador==4 && mascara(2,2)==1 %si existen
cuatro 1, es una bifurcación
         branchpoint2=branchpoint2+1;
      end

      if mascara==[1 0 1;0 1 0;0 0 0] %Se cuentan los valles
         bottompoint2=bottompoint2+1;
      elseif mascara==[0 0 0;0 1 0;1 0 1] %Se cuentan las
crestas
         toppoint2=toppoint2+1;
      end

   end
end

%Comparación
v1=[toppoint1 bottompoint1 branchpoint1 endpoint1];
v2=[toppoint2 bottompoint2 branchpoint2 endpoint2];

vmax=max(v1,v2);
vmin=min(v1,v2);
vhuella=(vmin*100)./vmax;
if v1(1,1)==v2(1,2) && (vhuella(1,2)>=70 && vhuella(1,3)>=70
&& vhuella(1,4)>=70)
   identidad1
elseif v1(1,2)==v2(1,2) && (vhuella(1,1)>=70 &&
vhuella(1,3)>=70 && vhuella(1,4)>=70)
   identidad1
elseif v1(1,3)==v2(1,3) && (vhuella(1,1)>=70 &&
vhuella(1,2)>=70 && vhuella(1,4)>=70)
   identidad1
elseif v1(1,4)==v2(1,4) && (vhuella(1,1)>=70 &&
vhuella(1,2)>=70 && vhuella(1,3)>=70)
   identidad1
elseif vhuella(1,1)>=70 && vhuella(1,2)>=70 &&
vhuella(1,3)>=70 && vhuella(1,4)>=70
   identidad1
else
   identidad2
end
```

Resultados de la interfaz gráfica

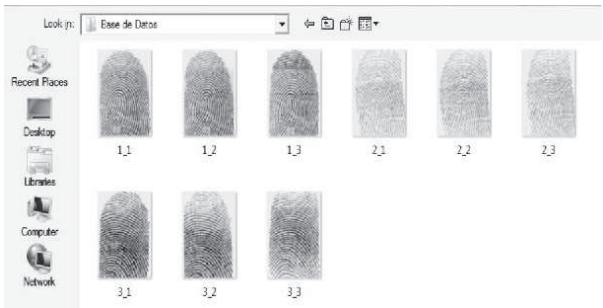
Para efectos de comprobar el nivel de eficiencia del algoritmo realizado en Matlab, la interfaz gráfica requiere que se carguen dos huellas digitales para su comparación y evaluación.

Figura 4. Interfaz principal

Fuente: Propia - Captura de imagen del software de reconocimiento de patrones de huellas digitales.

Buscamos las huellas digitales en nuestra base de datos y las seleccionamos.

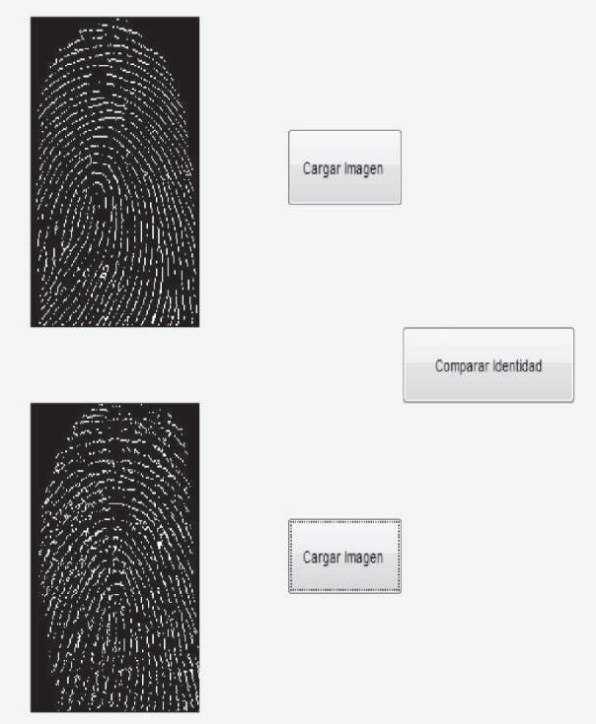
Figura 5. Base de imágenes de huellas digitales en formato PNG



Fuente: Propia - Captura de imagen del software de reconocimiento de patrones de huellas digitales.

Cuando cargamos las huellas digitales, el algoritmo las transforma en una imagen en blanco y negro.

Figura 6. Precarga de imágenes con reconocimiento



Fuente: Propia - Captura de imagen del software de reconocimiento de patrones de huellas digitales.

Finalmente, el algoritmo evalúa las minucias / patrones para poder determinar si el individuo es quien dice ser, mostrando los siguientes mensajes.

Figura 7. El algoritmo identifica que el individuo NO corresponde con la huella digital.

Fuente: Propia - Captura de imagen del software de reconocimiento de patrones de huellas digitales.

Figura 8. El algoritmo identifica que el individuo SI corresponde con la huella digital.

Fuente: Propia - Captura de imagen del software de reconocimiento de patrones de huellas digitales.

CONCLUSIONES

1. La biometría en la huella digital se seguirá mejorando en su técnica de evaluación de patrones/minucias, y según algunos investigadores algún día será nuestra identificación oficial alrededor de todo el mundo.
2. Los parámetros que sirven como medición se vuelven casi invariables en el tiempo, claro que existen sus excepciones en los individuos, ya sea que estos trabajen en laboratorios u obras de construcción donde sus manos son sometidas a procesos químicos o un desgaste de fricción muy alto, que puede provocar cambios en sus huellas digitales o incluso borrarlas por completo con el paso de los años.
3. La lectura de este tipo de biometría es bastante sencilla, ya que no es invasiva y ha sido aceptada por los usuarios. La tecnología para extraer dicha información es bastante económica comparada con otras. El costo se eleva si el sistema de reconocimiento de huellas digitales tiene el menor porcentaje posible de error, lo que se conoce como niveles de fiabilidad.
4. Cada vez son más las empresas que llevan a cabo el reconocimiento de sus empleados por medio de huellas digitales, para poder darles privilegios en ciertas tareas. Los registros legales y criminalísticas también están muy interesados en el desarrollo de esta tecnología, ya que se consideran los primeros en usarla, y probablemente nunca dejen de hacerlo.
5. Aunado a todo esto, cada vez existen más dispositivos (celulares, laptops) que cuentan con un sistema de bloqueo e identificación de huella digital, tal vez se pueda decir que la información que guardan estos dispositivos usados solo con un fin de ocio, no guarden información vital ni muy valiosa, pero cada vez más, los usuarios desean mantener su información privada, de forma inaccesible.

REFERENCIAS BIBLIOGRÁFICAS

1. Handbook of fingerprint recognition. Maltoni, Maio, Jain, Prabhakar. Año 2009
2. Automated Fingerprint Identification Systems. Peter Komarinski, Año 2005
3. Advances in Fingerprint Technology. Henry C. Lee & R.E.Gaensslen. Año 2001
4. Combining Fingerprint Classifiers. R. Cappelli, D. Maio, and D. Maltoni, Año 2000
5. Fingerprint Recognition in low quality Images. L. Coetzee and E. C. Botha. Año 1993
6. FVC2000: Fingerprint Verification Competition. D. Maio, D. Maltoni, R. Capelli, J. L. Wayman and A. K. Jain. Año 2002
7. MCYT Baseline corpus: A bimodal biometric database, Año 2003
8. Algoritmo para la identificación de personas basado en huellas dactilares. J. López. Año 2009
9. Uso de Dispositivos de Huella Digital para el Sistema de Control de Ingreso y Salida del Personal Docente de la Escuela de Ingeniería de Sistemas de la PUCESA. N. Vera, V. Chuncha . Año 2008
10. Implementación de un sistema de acceso electrónico mediante la huella dactilar y una clave de acceso. I. Cóndor, C. Paredes. Año 2009
11. A two-dimensional random projected minutiae vicinity decomposition-based cancellable fingerprint template. Zhe Jin, Bok-Min Goi, Andrew Teoh, Yong Haur Tay. Año 2013
12. Fingerprint Based Gender Classification Using Minutiae Extraction. S. S. Gornal, Basavanna M., Kruthi R., Año 2015.
13. Efficient Fingerprint Matching Based Upon Minutiae Extraction. Chiranjeeb Roy Chowdhury, Banani Saha. Año 2015.
14. Improved cancelable fingerprint templates using minutiae-based functional transform. Daesung Moon, Jang-Hee Yoo, Mun-Kyu Lee. Año 2014
15. Hough Transform Based Fingerprint Matching Using Minutiae Extraction. Nitika Saroha, Nasib Singh Gill. Año 2013
16. Fingerprint Recognition Using a Hybrid of Minutiae- and Image-Based Matching Techniques. Renee Ka Yin Chin, Jin Fei Lim. Año 2007
17. Fingerprint Feature Extraction Using Hough Transform and Minutiae Extraction. Nitika, Dr. Nasib Singh Gill. Año 2013

Foto 02: Ceremonia de Grados y Títulos de la Universidad José Carlos Mariátegui en el Auditorio "El Amauta"

Cortesía: Oficina de Comunicación e Imagen Institucional