GUÍA 8: PROCESOS DE AUTENTICACIÓN

Ejercicio 1:

La identificación por huella dactilar es una de las biometrías más conocidas y publicitadas. La creación del primer método de clasificación de ficheros de huellas dactilares por parte del argentino Juan Vucetich, permitió reemplazar el uso de la antropometría por la clasificación de huellas dactilares. Gracias a su unicidad y constancia en el tiempo las huellas dactilares han sido usadas para la identificación por más de un siglo.

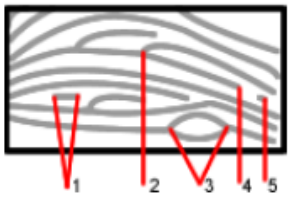
La computación provee ahora mecanismos para automatizar dichos procesos. EL AFIS (Automated Fingerprint Identification System) efectúa dos funciones principales:

a) *almacenar todas las huellas dactilares recolectadas en formato de template*
b) *compara las huellas enviadas desde las estaciones locales o remotas contra las almacenadas en el sistema.*

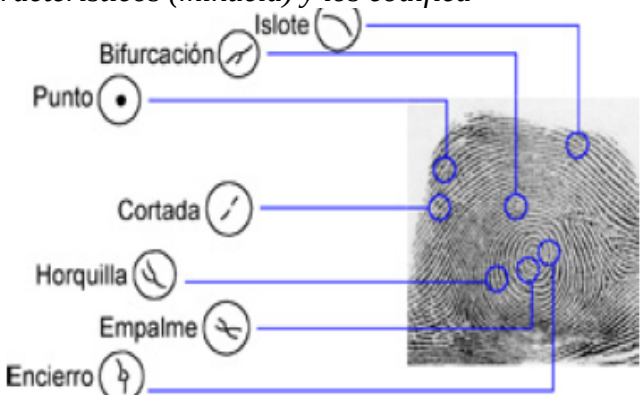
Hay entonces tres operaciones fundamentales: enrolamiento, verificación e identificación. En el enrolamiento, la tarea principal es la de insertar una nueva huella en el AFIS. En la verificación, una persona presenta sus huellas y se las compara contra las ya alojadas en el AFIS. En la identificación, cuando se conoce una huella pero ningún otro dato, entonces se compara contra todas las huellas ya registradas en el sistema.

Para efectuar dichos procesos, las huellas dactilares son captadas por un escáner. Los sensores extraen puntos de la imagen que se genera de la huella.

El software detecta los rasgos característicos (minucia) y los codifica



Puntos -minucias- en la huella
1.- Cresta corta
2.- Bifurcación
3.- Cercamiento
4.- Fin de la cresta
5.- Punto



Con este conjunto de puntos, el software biométrico de huella digital genera un modelo en dos dimensiones. El mismo se almacena en una base de datos con la debida referencia de la persona que ha sido objeto del estudio. La ubicación de cada punto característico o minucia se representa mediante una combinación de números (x.y) dentro de un plano cartesiano que sirven como base para crear un conjunto de vectores que se obtienen al unir las minucias entre sí mediante rectas cuyo ángulo y dirección generan el trazo de un prisma de configuración única e irrepetible.

		
El dedo es leído por un captor de huellas.	El dedo es codificado por el captor.	El captor guarda y reconoce un conjunto de números que solo podrán ser reconocidos como una plantilla.

Para llevar a cabo el proceso inverso o verificación dactilar se utilizan estos mismos vectores, no imágenes. (Aunque puede ser recomendable que también se guarde la imagen comprimida)

La identificación biométrica tiene un grado de seguridad muy alto. Es muy difícil copiar o reproducir los elementos usados en ella ya que son elementos inherentes a su portador, sin embargo puede estar sujeta a errores de:

- *Falsa aceptación - Cuando se acepta a alguien que No es la persona correcta*
- *Falso rechazo - Consiste en no aceptar a alguien que Sí es la persona correcta*

Fuentes: www.biometria.gov.ar y www.biocom.com

a) Identifica los 5 componentes de un SISTEMA DE AUTENTICACIÓN basado en huellas digitales:
   - información de autenticación (A)
   - información complementaria (C)
   - funciones de complementación (F)
   - funciones de autenticación (L)
   - funciones de selección (S)

b) Da dos ejemplos de falsa aceptación que podrían darse en un sistema de autenticación por huellas digitales.

c) Da dos ejemplos de falso rechazo que podrían darse en un sistema de autenticación por huellas digitales.

d) ¿Podría ocurrir un robo de identidad en un sistema de autenticación biométrico? Justificar.

Ejercicio 2:

El encargado de seguridad informática de una organización sugiere que las passwords que se usen sean de 8 caracteres de longitud. Asumiendo que un atacante puede probar 16mil passwords por segundo, cuál es la probabilidad de que todas las passwords se hayan adivinado en el lapso de un año para los siguientes alfabetos:

a) los caracteres deben ser dígitos. (“0” al “9”)
b) los caracteres deben ser alfanuméricos, pero sólo se usan letras mayúsculas (26 letras “A”…”Z” y “0” a “9”)
c) Se agregan 10 bits de SALT a los casos anteriores.