

SEGURIDAD EN SISTEMAS BIOMÉTRICOS



BIOMETRÍA

El concepto biometría viene de las palabras bio (vida) y metría (medida), y consiste en técnicas que miden e identifican las características físicas únicas de organismos vivos o patrones de su comportamiento, que permiten identificar a los diferentes individuos, como por ejemplo, las clásicas huellas digitales.

MÉTODOS UTILIZADOS

La biometría consiste en medir una de las características del cuerpo humano con el fin de identificar un individuo. Para esto se debe elegir una característica dotada de una fuerte variabilidad de un individuo a otro. Dentro de los principales métodos utilizados en la biometría se encuentran: la cara, la huella, la geometría de la mano, el iris, la voz, las venas, las orejas, el pulso cardíaco, la radiografía dental, el ADN, la forma de escribir a mano y la forma de digitar en el computador.

FUNCIONAMIENTO

Para su funcionamiento, un sistema biométrico requiere una parte física (hardware) que incluye la mayoría de las veces algunos sensores que llevan a cabo las mediciones y una parte de software que lleva ejecuta las comparaciones con los datos previamente registrado.

ARQUITECTURA

Para realizar un análisis biométrico se debe cumplir con los siguientes requisitos:

- **Universalidad:** Esta característica está presente en todos los individuos.
- **Unicidad:** la probabilidad de que existan dos personas con una característica idéntica es muy pequeña.
- **Permanencia:** la característica es prácticamente estática, es decir, no cambia con el tiempo.
- **Cuantificación:** la característica puede medirse en forma cuantitativa.



TÉCNICAS DE IDENTIFICACIÓN BIOMÉTRICA



RECONOCIMIENTO DE FIRMAS

Es la tecnología biométrica menos problemática, en la actualidad resulta la más difundida en el mundo ya que, entre otras ventajas, es muy económica si se requiere implementar. Un sistema de este tipo solo necesita una tableta de escritura conectada al computador.

MAPA DE LA RETINA DEL OJO

Mide el patrón de venas en el fondo del ojo, que se obtiene proyectando una luz infrarroja a través de la pupila, este sistema de seguridad biométrica no es muy fiable ya que se ha comprobado que es susceptible a cambios producidos por irritaciones oculares.

RECONOCIMIENTO FACIAL

El reconocimiento de rostro es menos exacto que el análisis de huellas dactilares teniendo la gran ventaja de no ser un método invasivo. Los sistemas basados en reconocimiento facial clasifican la apariencia de la persona e intenta medir algunos puntos nodales del rostro como la distancia entre los ojos, el ancho de la nariz, la distancia del ojo a la boca, etc.

PATRÓN DEL IRIS

Es uno de los sistemas biométricos más confiables debido a que el iris posee alrededor de 266 puntos únicos mientras que la mayoría de sistemas biométricos poseen alrededor de 13 a 60 características distintas. Cada ojo es único y permanece estable con el paso del tiempo y en diferentes ambientes de clima.

RECONOCIMIENTO DE VOZ

El análisis de la voz inicia a mediados de la década de los años 60. El habla se considera como uno de los sistemas biométricos más eficaces, debido a su naturalidad. Se ha podido comprobar que los patrones con que una persona dice una palabra son únicos. El reconocimiento de voz funciona mediante la digitalización de diferentes palabras de una persona.



GEOGRAFÍA DE MANO

Es un método mucho más eficiente que el reconocimiento por huellas dactilares, ya que al leer la mano de forma completa, permite capturar muchas más variables como imágenes individuales de algunos dedos y extraer datos como longitudes, anchuras, alturas, posiciones relativas y articulaciones entre otras.

BIBLIOGRAFÍA

Sistemas biométricos: Matching de huellas dactilares mediante transformada de Hough generalizada [en línea] disponible en:

http://www2.ing.puc.cl/~iing/ed429/sistemas_biometrico_s.htm (Consultado el 09 de Septiembre de 2020)

