SISTEMAS DE SEGURIDAD BASADOS EN BIOMETRÍA
SECURITY SYSTEMS BASED ON BIOMETRICS

Resumen.

Desde hace varios años, los sistemas de seguridad basados en biometría son un medio eficaz y eficiente para el reconocimiento del ser humano. Dentro de éstos, se destacan el reconocimiento facial o de rostro, el reconocimiento de la voz, el análisis del patrón del iris, el reconocimiento de huellas dactilares, el análisis del mapa de la retina del ojo, el olor corporal, el análisis de la forma del oído, el análisis de la forma de la mano, la geometría de los dedos, la forma de la cabeza, el análisis del mapa de venas de la mano.

Este artículo muestra algunas características a tener en cuenta en el momento de implementar un sistema de seguridad basado en adquisición de datos biométricos, haciendo énfasis en el reconocimiento de huellas dactilares a través de Punto Net.

Este trabajo forma parte de la investigación realizada por el grupo de robótica aplicada en la línea de investigación de visión artificial.

Palabras clave.
Biometría, control, huella dactilar, reconocimiento, tratamiento digital, visual Studio punto net.

M.Sc JIMY ALEXANDER CORTÉS OSORIO
Docente de Tiempo Completo de la Universidad Tecnológica de Pereira
Ingeniero Electricista
Magíster en Instrumentación Física
jacoper@utp.edu.co

M. Sc FRANCISCO ALEJANDRO MEDINA AGUIRRE
Docente Catedrático de la Universidad Cooperativa de Colombia
Docente Catedrático de la Universidad Libre sede de Pereira
Docente Medio Tiempo de la Universidad Tecnológica de Pereira
Ingeniero de Sistemas
Magíster en Instrumentación Física:
famedina@utp.edu.co

JOSÉ A. MURIEL ESCOBAR
Ingeniero Mecánico
Instructor Sena Industria.
Dosquebradas
jamuriel@sena.edu.co

Abstract.
For several years, security systems based on biometrics are an effective and efficient way for the recognition of human beings. Within them, highlights the face, facial recognition, voice recognition, the iris pattern analysis, fingerprint recognition, analysis of the map of the retina of the eye, body odor, the analysis of the shape of the ear, the analysis of hand shape, the geometry of the fingers, the shape of the head map analysis of hand veins.

This paper introduces some features to consider when implementing a security system based on biometric data acquisition, emphasizing the fingerprint recognition by means dot Net.

This work is part of the investigation by the robotics group in the research of artificial vision.

Keywords.
Biometrics, control, fingerprint, digital treatment, recognition, visual studio dot net.

1. INTRODUCCIÓN.

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

Según Jean-Marc Royer (2007) 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 cardiaco, la radiografía dental, el ADN, la forma de escribir a mano y la forma de digitar en el computador. El sistema más común en la práctica, es el reconocimiento de huellas digitales, y como en cualquier otro método siempre existirá un margen de error, siendo considerado menor en este. El método de las hullas digitales se encuentra entre las diez tecnologías emergentes que cambiarán el mundo según un informe realizado por el Massachussets Institute of Technology (2006). [7]

Mainguet Jean Francois (2006), investigador francés experto en biometría y creador del sensor para huellas FingerPrint, afirma que "una clave o llave no prueban que determinada persona es la que deba tener acceso a algo". La biometría llena ese bache, ya que un sistema de este tipo verifica algo que usted es, por lo que no hay forma de prestarlo o que se pierda.

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 registrados [2].

2. Técnicas de identificación biométrica.

En la actualidad, gracias a los avances de la tecnología, es fácil encontrar diferentes productos que permiten elaborar un reconocimiento biométrico del ser humano de una forma fácil y segura. algunos de los sistemas biométricos más utilizados se describen a continuación.

2.1. 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. El escaneo de la firma se analiza desde dos puntos de vista, siendo estos la firma en sí y el modo en que se efectúa. Los datos almacenados incluyen la velocidad, la presión, la dirección, el largo del trazado y las áreas donde el lápiz se levanta. El gran inconveniente de este método es que una persona nunca firma de manera idéntica dos veces.

2.2. Reconocimiento facial o de rostro.

El reconocimiento de rostro, actualmente, es menos exacto que el análisis de huellas dactilares teniendo la gran ventaja de no se 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, o la longitud de la línea de la mandíbula. El análisis tridimensional de la cara elimina algunos inconvenientes que se pueden tener en un reconocimiento bidimensional, como son: la iluminación y las sombras, la orientación o pose de la cara, y la variación de expresiones faciales. En la actualidad existen muchos códigos fuentes ya desarrollados que permiten un análisis facial de forma simple como los implementados en la red social Facebook**.** [4]

2.3. 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 [1], este sistema de seguridad biométrica no es muy fiable ya que se ha comprobado que es susceptible a cambios producidos por irritaciones oculares. [1]

2.4. 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 [1]. Cada ojo es único y permanece estable con el paso del tiempo y en diferentes ambientes de clima.

En la figura 1 se muestran las partes externas de ojo humano.

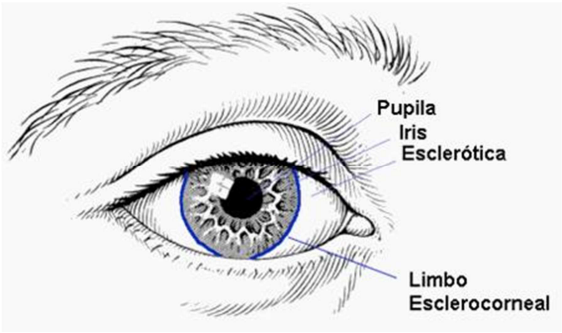

Figura 1: Partes externas del ojo humano

El escaneo de iris se realiza utilizando una videocámara y analizando los patrones de color de los surcos de la parte coloreada de los ojos.

2.5. Reconocimiento de la 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 [4]. El reconocimiento de voz funciona mediante la digitalización de diferentes palabras de una persona. Cada palabra se descompone en segmentos, de los cuales se obtienen 3 o 4 tonos dominantes que son capturados en forma digital y almacenados en una tabla o espectro, que se conoce con el nombre de plantilla de la voz (voice print).
La figura 2 muestra un ejemplo de cómo puede visualizarse el espectro de la voz humana [5].

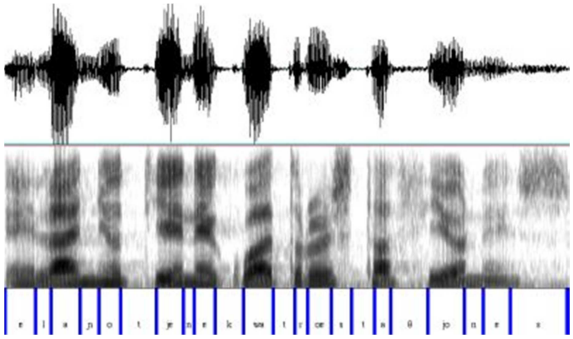

Figura 2: análisis del espectro de la voz humana

2.6. Reconocimiento de huellas dactilares.

El reconocimiento de huellas dactilares es otra de las técnicas más usadas a nivel mundial [1]. Está basado en el desarrollo realizado por John Evangelist Purkinje quien en 1823 realizó los primeros estudios de las huellas dactilares; años más tarde (1980) Sir Francis Galton comenzó sus observaciones para utilizar las huellas como identificadores personales. En el año de 1892 Galton publicó su libro "Fingerprints" en el que afirmaba que las huellas dactilares eran únicas y que no cambiaban a lo largo de la vida; Galton también estableció un sistema de clasificación de las huellas dactilares.

Una huella digital normalmente está conformada por una serie de líneas oscuras que representan las crestas y una serie de espacios blancos que representan los valles.

La identificación con huellas dactilares está basada principalmente en la ubicación y dirección de las terminaciones de crestas, bifurcaciones, deltas, valles y crestas.

La figura 3 muestra las diferentes líneas por las que puede estar conformada una huella digital.

Figura 3: Líneas de una huella dactilar

2.7. 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.

3. ARQUITECTURA DE UN SISTEMA BIOMÉTRICO.

Para realizar un análisis biométrico se debe cumplir con los siguientes requisitos [3]:

- 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.

Los dispositivos biométricos poseen tres elementos primordiales [3]:

- El primer elemento hace referencia a la adquisición análoga o digital de algún indicador biométrico de una persona (por ejemplo la adquisición de una huella dactilar utilizando un escáner).
- El segundo elemento establece: La compresión, procesamiento, almacenamiento y comparación de los datos adquiridos con los datos almacenados.
- Por último, se establece una interfaz con aplicaciones ubicadas dentro del mismo u otro sistema.

La figura 4 presenta la arquitectura típica de un sistema biométrico. Este puede concebirse conceptualmente como dos módulos:

1. Módulo de inscripción
2. Módulo de identificación

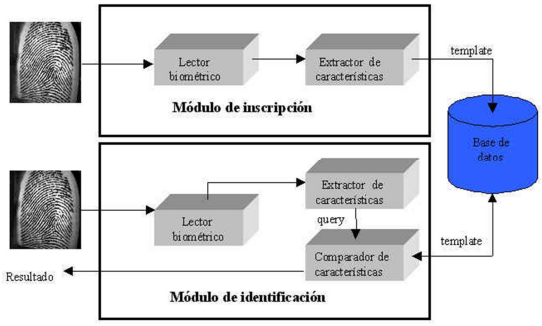

Figura 4: Arquitectura de un sistema biométrico para identificación personal, aquí ejemplificado con huellas dactilares.

El módulo de inscripción es el encargado de adquirir y almacenar la señal proveniente del lector biométrico con el fin de poder comprobar la señal capturada con la proporcionada en ingresos posteriores al sistema. Las tareas producidas por el módulo de inscripción son posibles gracias a la acción del lector biométrico y del extractor de características.

El lector biométrico, se encarga de adquirir datos relativos del indicador biométrico elegido y entregar una representación en formato digital de éste. El extractor de características toma las particularidades representativas del indicador a partir de la salida del lector. El conjunto de características será almacenado en una base de datos central y se conoce con el nombre de *template*; los *templates* se usan en labores de identificación al ser comparados con la información proveniente del indicador biométrico en un punto de acceso.

El módulo de identificación es aquel que se encarga del reconocimiento de individuos: El proceso de identificación inicia cuando el lector biométrico captura la característica del individuo a ser verificado y la convierte a formato digital para que, a continuación, el extractor de características entregue una representación compacta con el mismo formato de los *templates*. La representación resultante se conoce con el nombre de *query* y se envía al comparador de características que se encarga de confrontar el *query* con uno o varios *templates* para establecer la identidad de la persona.

4. IMPLEMENTACIÓN DE UN LECTOR DE HUELLA UTILIZANDO VISUAL STUDIO PUNTO NET

4.1 Lector de huella dactilar Biométrico.

Para la implementación del lector biométrico se usó un lector de huella dactilar marca U.are.U 2000 (modelo No. URU2S-U) fabricado por la empresa DigitalPersona. Este dispositivo se conecta al computador vía puerto USB y es compatible con una gran serie de versiones del sistema operativo Windows. Este resulta sencillo de instalar y posee un diseño compacto y moderno que facilita su uso.La empresa DigitalPersona, fundada en 1996, desde su creación es un proveedor global de soluciones de protección y seguridad, usando productos biométricos de autenticación simple, práctica y asequible para todo tipo de empresas.

La figura 5 muestra el lector de huella U.are.U 2000 implementado en este trabajo.

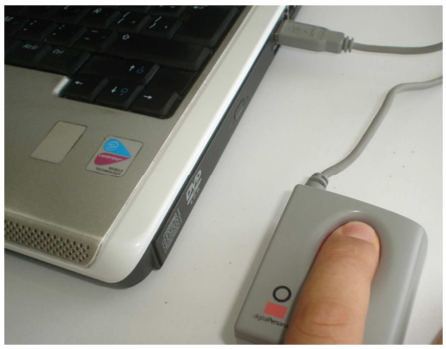

Figura 5: Lector de huella U.are.U 2000

4.2. Desarrollo del software

Para el procesamiento de la huella digital se utilizó el *One Touch for Windows SDK .NET Edition* desarrollado por la empresa digitalpersona: Esta aplicación es una herramienta de desarrollo de software que permite a los programadores integrar la biometría de la huella dactilar a un amplio conjunto de aplicaciones para el sistema operativo Windows [6]. La herramienta permite realizar las operaciones básicas biométricas para el tratamiento de una huella digital como lo son, su captura a través del lector U.are.U 2000 de DigitalPersona, la extracción de las características de las huellas dactilares capturadas y el almacenamiento de los datos resultantes en una plantilla o *template* para la comparación posterior de la huella digital con otras ya existentes.

El programa implementado realiza los siguientes procesos y funcionalidades:

- Proceso de inscripción de la huella. Este proceso captura la huella dactilar de una persona cuatro veces. Después de capturada la huella se realiza un proceso de extracción de las características de las huellas digitales; posteriormente se crea una plantilla o *template* de huella dactilar capturada, y por ultimo realiza el almacenamiento del *template* para la comparación posterior.

- Verificación de la huella. Es el proceso de comparación de una huella digital capturada con un *template* de huellas dactilares para determinar si ambas coinciden.

- Desmatriculación de una huella. Es el proceso de eliminación de un *template* de huella digital asociada a una huella dactilar previamente inscrita.

La figura 6 muestra el formulario diseñado en Visual Studio punto Net para el proceso de inscripción de una huella dactilar.

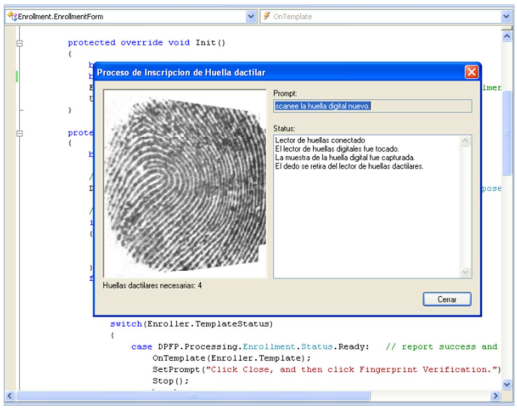

Figura 6: proceso de inscripción de una huella dactilar

6. CONCLUSIONES Y/O RECOMENDACIONES

Este trabajo fue desarrollado por el grupo de investigación de Robótica Aplicada en la línea de visión artificial. Este resulta ser una aproximación a los sistemas biométricos, y hace énfasis en el reconocimiento de huellas dactilares> A lo largo del artículo se puede apreciar cómo se aplican las diferentes etapas que se deben tener en cuenta durante la adquisición de un dato biométrico y su posterior reconocimiento.

Utilizando librerías como las ofrecidas por la empresa Digitalpersona es muy sencillo implementar sistemas biométricos basados en el reconocimiento de huellas dactilares. La librería *One Touch for Windows SDK .NET Edition* de esta empresa, ofrece seguridad, simplicidad y eficiencia de autenticación de huellas digitales e identificación de usuarios en el momento de desarrollar aplicaciones comerciales.

Es de suma importancia continuar con la investigación de sistemas biométricos alternativos y el mejoramiento de los algoritmos propios que faciliten la tarea de identificación de patrones biométricos tanto humanos como animales.

7. BIBLIOGRAFÍA

[1] Tutorial biometría, [En línea] disponible en: http://tutorial-biometria.galeon.com/pages/sistemas.html (Consultado el 3 de noviembre de 2010)

[2]]Sensores biométricos [en línea] disponible en: http://neutron.ing.ucv.ve/revista-e/No6/Olguin%20Patricio/SEN_BIOMETRICOS.html (Consultado el 4 de noviembre de 2010)

[3]Sistemas biométricos: Matching de huellas dactilares mediante transformada de Hough generalizada [en línea] disponible en: http://www2.ing.puc.cl/~iing/ed429/sistemas_biometricos.htm (Consultado el 4 de noviembre de 2010)

[4] Web electrónica club SE [en línea] disponible en: http://www.webelectronica.com.ar/news18/nota09.htm (Consultado el 4 de noviembre de 2010)

[5] Club de lo insólito [en línea] disponible en: http://blogs.elcomercio.pe/elclubdeloinsolito/2008/12/es-posible-identificar-una-voz.html (Consultado el 5 de noviembre de 2010)

[6]One Touch® for Windows® SDK .NET Edition Versión 1.6 en [en línea] disponible en: http://www.digitalpersona.com/Biometrics/SDK-Products/One-Touch-for-Windows-SDK/One-Touch-for-Windows-Software-Development-Kit/ (Consultado el 6 de noviembre de 2010)

[7] Jean-Marc Royer (2007) Seguridad en la informática de empresa: riesgos, amenazas, prevención y soluciones (2007) Ediciones ENI