SISTEMA DE RECONOCIMIENTO DE HUELLAS DACTILARES PARA EL CONTROL DE ACCESO A RECINTOS

García Ortega Victor Hugo
Centro de Investigación en Computación
Laboratorio de Sistemas Digitales
Av. Juan de Dios Batiz s/n, Esq. Miguel Othón de Mendizabal
Unidad Profesional "Adolfo López Mateos"
Instituto Politécnico Nacional
México, D.F. C.P. 07738 Tel. (52)57296000 Ext. 56556
vgarcia@cic.edu.mx

RESUMEN. Este trabajo presenta el desarrollo de un AFAS (Automatic Fingerprint Authentification System), basado en la detección de bifurcaciones y terminaciones dentro de la huella para la verificación de personas.
Además se describe el diseño de un Sistema Digital el cuál realizará el procesamiento de la imagen. Dicho sistema esta basado en el Procesador Digital de Señales(DSP) TMS320C31 con interfaz al bus PCI de la PC.

1. INTRODUCCIÓN

Los sistemas tradicionales utilizados en el control de acceso a recintos se basan en los sistemas de tarjetas magnéticas, sistemas de tarjetas con código de barras, sistemas de captura de clave o combinación de ellos. Estos sistemas involucran el uso de una tarjeta que hay que llevar siempre consigo y la cual no está exenta de perderse, dañarse, ser robada o falsificada, con lo cual la seguridad del recinto se hace más vulnerable a fallas. Por esta razón, si se cuenta con un sistema más robusto y de mayor confiabilidad se pueden evitar los problemas antes mencionados.

Los sistemas biométricos se basan en características o rasgos físicos medibles ó personales de comportamiento, los cuáles son usados para reconocer o verificar la identidad de una persona a través de medios automáticos[1]. Estos sistemas biométricos han sido un área importante de investigación en los años recientes[2].

Estas características deben satisfacer los siguientes requerimientos[2]:

- Universalidad, lo cual significa que cada persona debe de tener esas características.
- Unicidad, lo cual significa que dos personas no deben de ser la misma en términos de las características.
- Permanencia, lo cual indica que las características deben ser invariantes con el tiempo.
- Colectibilidad, lo cuál indica que las características pueden ser medibles cuantitativamente.

Un sistema biométrico en particular es aquel que utiliza la huella dactilar. Esta huella representa un patrón único de identificación entre las personas, aun entre gemelos. Este patrón conserva la misma forma desde la formación del feto hasta la muerte de la persona con lo cual se satisface los requerimientos antes mencionados. Estas características representan un medio más robusto y confiable para un sistema de seguridad.

Con el incremento de cálculo de las computadoras se han ido desarrollando sistemas automatizados para realizar la clasificación e identificación de huellas dactilares. Básicamente los sistemas biométricos basados en huellas dactilares son de dos tipos[4]:

Automatic Fingerprint Authentification System(AFAS).
Automatic Fingerprint Identification System(AFIS).

En un AFAS la entrada es la identidad de la persona y la imagen de la huella dactilar de esa persona; y la salida es una respuesta de SI ó NO, indicando si la imagen de entrada pertenece a la persona cuya identidad es proporcionada.

En un AFIS la entrada es solo la imagen de la huella dactilar y la salida es una lista de identidades de personas que pueden tener la huella dada, además de una puntuación de cada identidad indicando el grado de similaridad entre ésta y la huella dada.

Ambos sistemas utilizan los detalles formados en las huellas dactilares. Estos detalles llamados "*ridges*" son definidos como un segmento de curva simple. La combinación de varios ridges forman un patrón de huella dactilar. Las pequeñas características formadas por el cruce y terminación de ridges son llamadas *minucias*.

Además de las minucias, las huellas dactilares contienen dos tipos especiales de rasgos llamados puntos *core* y *delta*(Fig 1.0). Estos puntos son referidos como los puntos de singularidad de una huella dactilar. El punto core es definido como el punto mas alto en el ridge curvo mas interior[6]. Este punto es generalmente usado como punto de referencia para la codificación de minucias.

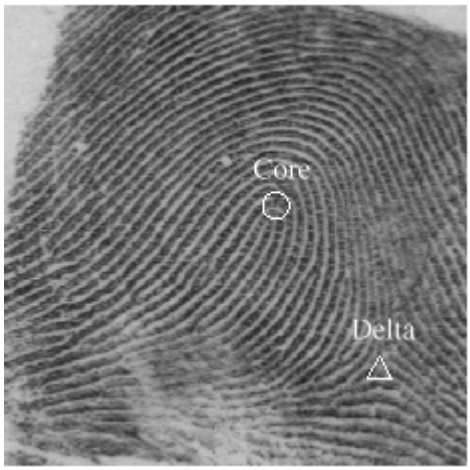

Fig. 1.0 Puntos singulares en una huella dactilar

2. DESCRIPCIÓN GENERAL DEL SISTEMA

El sistema completo se puede apreciar en la figura 2.0.

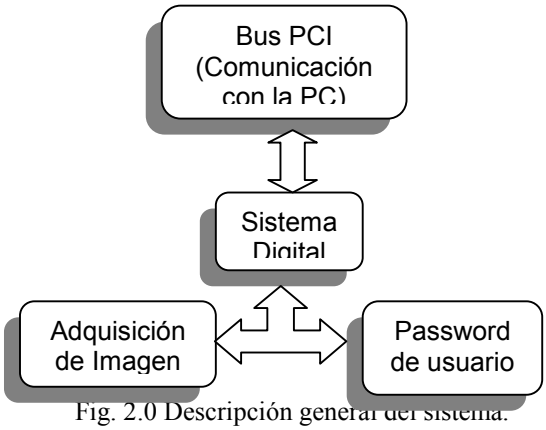

Fig. 2.0 Descripción general del sistema.

El sistema que se propone es un sistema de control de acceso utilizando reconocimiento de huellas dactilares en conjunción con el sistema mediante clave. Este sistema es un AFAS.

Una vez recibida la señal digitalizada de la huella dactilar y la clave de acceso, éstas son procesadas en un sistema digital basado en el DSP TMS320C31 de Texas Instruments, el cual tiene comunicación con la PC a través del bus PCI.

La base de datos del conjunto de patrones a reconocer se tendrá almacenada en la PC, con la finalidad de poder tener una capacidad mucho mayor de almacenamiento de usuarios, que la capacidad de la que se dispone con una determinada cantidad de memoria en la tarjeta, la cual limitaría de manera considerable la cantidad de usuarios del sistema. Además la clave capturada por el sistema sirve como índice de búsqueda en la base de datos, esto con la finalidad de hacer el reconocimiento con mayor rapidez.

3. DESCRIPCIÓN DEL SISTEMA DE RECONOCIMIENTO

El sistema de reconocimiento que se propone se muestra en la figura 3.0.

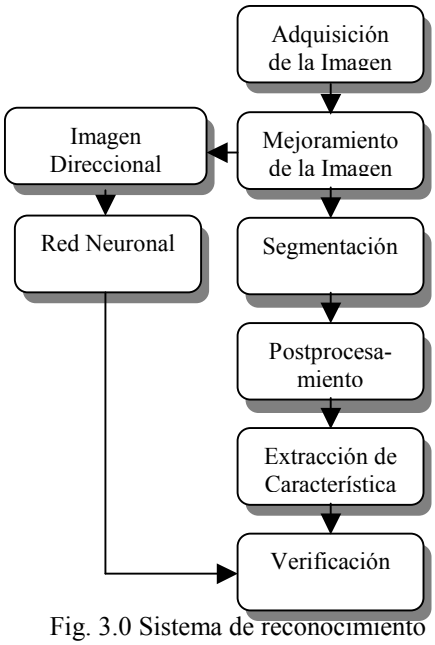

Fig. 3.0 Sistema de reconocimiento

3.1. Adquisición de la imagen.

Para la adquisición de la imagen se esta utilizando el *5th Sense Parallel Evaluation Kit*, el cuál es el Kit de desarrollo del sensor de huella dactilar FPS110. Dicho sensor es fabricado por la compañía Veridicom. El sensor es del tipo capacitivo, el cuál cuenta con una resolución de 500 dpi y con un tamaño de arreglo de pixeles de 300x300. Además, éste cuenta con un convertidor analógico/digital de 8 bits integrado, con lo que se tiene una imagen con una resolución en niveles de grises de 256 por píxel. En la figura 4.0 se puede observar una imagen obtenida con éste Kit.

Fig. 4.0 Huella obtenida con el 5th Sense Parallel Evaluation Kit

3.2. Mejoramiento de la Imagen.

La información direccional de la imagen de un bloque específico de la imagen esta contenido en la magnitud de la Tranformada de Fourier del bloque[7]. Al igual que en [7] la imagen es dividida en bloques de 32x32 pixeles, los cuales son mejorados utilizando la magnitud de la Transformada de Fourier del bloque. El mejoramiento es realizado sobre un área de 256x256 pixeles. La Transformada de Fourier es calculada de acuerdo a:

$$F(u,v) = \frac{1}{MN}\sum_{x=0}^{M-1}\sum_{y=0}^{N-1} f(x,y)\exp\left\{-j2\pi\left(\frac{ux}{M}+\frac{vy}{N}\right)\right\} \quad (1)$$

La imagen mejorada g(x,y) en cada bloque es obtenida por:

$$g(x,y) = F^{-1}\left\{F(u,v)x\left|F(u,v)\right|^{k}\right\} \quad (2)$$

Donde F(u,v) es la Transformada de Fourier de un bloque de 32x32 pixeles y F^{-1} es la Transformada Inversa de Fourier obtenida de acuerdo a:

$$f(x,y) = \sum_{u=0}^{M-1}\sum_{v=0}^{N-1} F(u,v)\exp\left\{j2\pi\left(\frac{ux}{M}+\frac{vy}{N}\right)\right\} \quad (3)$$

Experimentalmente se encontró que un valor de k = 1.2 fue el óptimo para el mejoramiento de la imagen. Este método presenta un problema en los bordes de cada bloque por lo se necesito un traslape de 26 pixeles entre cada bloque para eliminar este efecto. La figura 5.0 muestra la imagen mejorada de la imagen de la figura 4.0

Fig. 5.0 Huella mejorada a través de la Transformada de Fourier

3.3. Imagen Direccional

De acuerdo con la clasificación de Henry[9], la estructura global de las huellas se pueden clasificar en *right loop, left loop, whorl, arch y tented arch*. De esta forma la estructura de la huella dactilar de algún usuario pertenece a alguna de éstas clases.

La imagen direccional nos da información de la estructura global de la imagen de la huella dactlilar. Por lo que una primera fase de identificación es verificar que la imagen de la huella pertenezca a su clase.

Después del mejoramiento de la imagen se procede a calcular la orientación local de cada pixel. Una aproximación común para encontrar las direcciones de los ridges es descrito en [4][9], en donde se propone el uso de *"slits"*. Para cada pixel se calculan 8 diferentes slits. La dirección asignada al pixel C esta dada por:

$$dir(C) = \begin{cases} i \mid S_i = S_{max} \Rightarrow 4C + S_{min} + S_{max} > \frac{3}{8}\sum_{i=1}^{8} S_i \\ i \mid S_i = S_{min} \Rightarrow deotraforma \end{cases} \quad (4)$$

Después de obtener la dirección de cada pixel se realiza un promediado de éstas tomando bloques de 15x15 pixeles. De esta imagen solo se toma la región central de la imagen de 240x240 pixeles.

3.4. Red Neuronal

La región central de la imagen esta formada por 16x16 bloques, cada uno de 15x15 pixeles, estos bloques representan la entrada a una red neuronal no supervisada. En este trabajo se propone un Mapa Autoorganizado(SOM) para hacer la separación de clases derivada de la estructura global de la huella dactilar. El algoritmo de entrenamiento es el algoritmo de Kohonen[10]. La arquitectura que se propone es un mapa bidimensional de 10x10 neuronas.

En esta etapa se hace la extracción del punto Core de la imagen de acuerdo a [4]. Este punto es necesario para hacer la comparación correcta de dos huellas dactilares al usar el mapa autoorganizado, así como para realizar la extracción de las minucias descritas en la sección 2.7.

3.5. Segmentación.

En el procesamiento de las imágenes de huellas dactilares es usualmente necesario remover las partes que no llevan información válida. La segmentación es útil para este propósito.

Una buena técnica de segmentación debe ser insensible al contraste de la imagen original y debe ser independiente a si la imagen es mejorada o no. El *método compuesto* propuesto en [8] que combina los métodos de segmentación basados en la información de *dirección* y *varianza* es altamente eficiente para determinar regiones inválidas. Para este trabajo fue suficiente con utilizar la método de la varianza[8].

En este método se calcula la varianza de los niveles de gris de un bloque. La varianza de un bloque(k,l) es calculada por:

$$V(k,l) = \frac{1}{XY}\sum_{i=0}^{Y}\sum_{j=0}^{X}\left[i(kY+i,lX+j)-\mu\right]^2 \quad (5)$$

Donde X y Y son la dimensión del bloque, μ es la media aritmética de los niveles de gris del bloque (k,l) e *i* es la imagen. En este trabajo X = Y = 15.

Una vez obtenidos los bloques válidos de la imagen estos se binarizan usando un umbral global de 125, el cuál fue obtenido experimentalmente.

La figura 6.0 muestra la imagen segmentada de la imagen de la figura 5.0

Fig. 6.0 Huella Binarizada

3.6. Postprocesamiento

Una vez obtenida la imagen binaria de la huella dactilar es más fácil obtener las minucias partir del esqueleto de la imagen, por lo que un algoritmo de esqueletización es aplicado a fin de obtener dicha imagen[3]. La figura 7.0 muestra el esqueleto de la imagen de la figura 6.0

Fig. 7.0 Huella Esqueletizada

Después de esqueletizar la imagen en ocasiones se suelen obtener falsas minucias dependiendo si el usuario presionó excesivamente o suavemente la superficie del sensor. Por esta razón, a la imagen esqueletizada se le aplica un algoritmo de detección de este tipo de falsas minucias. Una vez detectadas las falsas minucias, se eliminan de la imagen.

3.7. Extracción de Características.

Dentro de la imagen de una huella dactilar se pueden encontrar las minucias descritas en la tabla 1[5].

Tabla 1. Tipos de Minucias.

Características	
	Terminación
	Bifucarción
	Laguna
	Borde independiente
	Punto o isla
	Aguijón
	Cruce

Los dos tipos de minucias mas importantes son las bifurcaciones y terminaciones, ya que los demás tipos de minucias se forman con una combinación de estas dos. Por esta razón, en la etapa de extracción de características se detectan estos dos tipos de minucias.

.

3.8. Verificación.

Una vez detectadas las bifurcaciones y terminaciones dentro de la imagen, se forma una plantilla, la cuál contiene el tipo de minucia detectada, posición, distancia a sus cinco vecinos mas cercanos, y ángulo de orientación de la minucia. Con esta plantilla que se obtiene para cada minucia, se forma una base de conocimiento para cada individuo. Si la imagen pertenece a su clase de acuerdo con la estructura global de la huella dactilar del individuo, ésta base de conocimiento se compara con la imagen del individuo a fin de poder decidir si pertenece o no al individuo.

4. DESCRIPCIÓN DEL SISTEMA DIGITAL

El sistema digital consta de las etapas mostradas en la figura 8.0

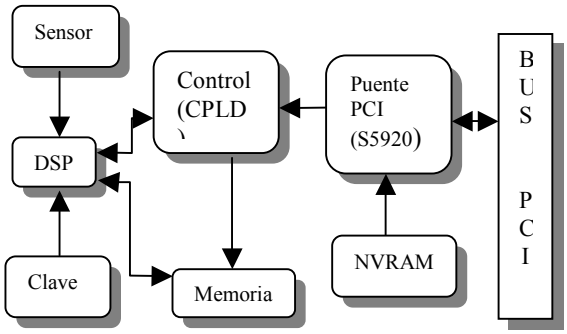

Fig. 8.0 Sistema Digital

4.1. Adquisición de Datos

Esta etapa esta formada por la adquisición de la imagen llevada a cabo mediante el sensor de Veridicom y la captura de la clave de usuario.

4.2. Procesamiento.

Aquí se utiliza el DSP TMS320C31, el cuál realizará el procesamiento de la imagen. Este DSP es un procesador de punto flotante, con 32 bits en el bus de datos y 24 bits en el bus de direcciones así mismo trabaja con una frecuencia de reloj de 30 MHz, al dividir internamente su frecuencia de oscilador de 60 MHz en un factor de dos. El

procesador es usado en modo microcomputador[11] por lo que el programa de reconocimiento es cargado por medio de la interfaz PCI. Este procesador tiene asociado a él, la memoria CYM1841 de la compañía Cypress, cuya organización es de 256Kx32 con un tiempo de acceso de 15 ns. Con estas características el DSP de 60MHz, trabaja con cero estados de espera, con lo que se obtiene el máximo desempeño en cuanto a velocidad del procesador. Además, el tamaño de palabra de 32 bits de la memoria permite una interfaz directa con el bus de datos del procesador que es de 32 bits también.

4.3. Control.

Todo el control del sistema digital se hace en un Dispositivo Lógico Programable Complejo(CPLD) de la compañía Xilinx[12]. Aquí se hace la detección de escritura o lectura del bus PCI hacia la aplicación que se encuentra en el bus Add-On del puente PCI[13]. Aquí se generan las direcciones de la memoria para accesar a las primeras localidades de la misma al momento de cargar el programa mediante el "*boot-loader*" que maneja el DSP. También se realiza la decodificación de direcciones de los periféricos.

4.4. Interfaz PCI.

Una vez procesada la huella dentro del DSP, se procede a enviar las plantillas de características hacia la computadora personal(PC) donde se encuentra el sistema digital, mediante la señal de interrupción asociada al puente S5920 de AMCC. Este puente realiza la interfaz entre la aplicación y las señales de control que maneja el bus PCI. Para esto se hace uso de una de las cuatro regiones Pass-Thru que se pueden usar con este puente[13]. Para cargar con un valor deseado los registros de configuración del dispositivo, se utiliza una memoria serial de configuración[13].

5. RESULTADOS

Existen numerosas técnicas para el procesamiento de huellas dactilares, en este trabajo se utilizan algunas de ellas para la verificación de personas. Actualmente se estan realizando pruebas del sistema en las etapas finales de verificación.

El sistema de hardware que se presenta pretende realizar la identificación de personas mediante su huella dactilar utilizando un DSP como célula de procesamiento con interfaz al bus PCI. Este sistema se encuentra en su etapa de construcción teniendo el diseño del mismo en un 100%.

De esta manera se pretende tener un sistema completo, con un software de reconocimiento en conjunción con un hardware específico para la aplicación.

6. REFERENCIAS

[1] http://www.mytec.com/02/bio-02-01.shtml
[2] B. Miller, "*Vital signs of identity", IEEE Spectrum,* 31(2), 1994, pp. 22-30.
[3] R. C. Gonzalez y R. E. Woods, Tratamiento digital de imágenes, 1996
[4] L. C. Jain, U. Halici, I. Hayashi, S. B. Lee, Intelligent biometric techniques in fingerprint and face recognition, 1999.
[5] H. C. Lee, and R. E. Gaensslen, Advances in fingerprint technology, 1994
[6] V. S. Srinivasan and N. N. Murthy, "Detection of singularity point in fingerprint images", Pattern Recognition, vol 25, pp. 139-153, 1992.
[7] A.J. Willis and L. Myers, "A cost-effective fingerprint recognition system for use with low-quality prints and damage fingertips", Pattern Recognition, vol. 34, No 2, pp. 255-270, February 2001.
[8] B.M. Mehtre and B. Chatterjee, "Segmentation of fingerprint images-A composite method", Pattern Recognition, vol. 22, pp. 381-385, 1989.
[9] U. Halici, G. Ongun, "Fingerprint classification through Self-Organizing features maps modified to treat uncertainties", The Proceedings of the IEEE, vol. 84, No 10, pp 1497-1512, 1996
[10] Simon Haykin, Neural Networks A comprehensive foundation, 1999
[11] Texas Instruments, TMS320C3X User's Guide
[12] Xilinx Company, Databook, 1999
[13] AMCC Company, PCI Products Data Book, 1998