SISTEMA DE CONTROL DE ACCESO A RECINTOS UTILIZANDO EL RECONOCIMIENTO NEURONAL DE HUELLAS DACTILARES

ADRIANA MILENA CASTAÑO PADILLA **CÓDIGO: 9804013**

SILVIA PATRICIA MORALES CHAMORRO **CÓDIGO: 9804047**

UNIVERSIDAD TECNOLÓGICA DE BOLÍVAR

FACULTAD DE INGENIERÍA ELÉCTRICA, ELECTRÓNICA Y MECATRÓNICA

MINOR EN AUTOMATIZACIÓN INDUSTRIAL

CARTAGENA D.T. Y C.

2003

SISTEMA DE CONTROL DE ACCESO A RECINTOS UTILIZANDO EL RECONOCIMIENTO NEURONAL DE HUELLAS DACTILARES

ADRIANA MILENA CASTAÑO PADILLA

SILVIA PATRICIA MORALES CHAMORRO

Monografía presentada como requisito para el Minor en Automatización Industrial

Director

Eduardo Gómez
M.S.C en Ciencias Computacionales

Asesor

Javier Campillo
Ingeniero Electrónico

UNIVERSIDAD TECNOLÓGICA DE BOLÍVAR

FACULTAD DE INGENIERÍA

MINOR EN AUTOMATIZACIÓN INDUSTRIAL

CARTAGENA D.T. Y C.

2003

Nota de aceptación

_____

_____

_____

_____

_____

_____

_____

Firma del presidente del jurado

_____

Firma del jurado

_____

Firma del jurado

_____

A Dios y a mi familia

Adriana Milena Castaño Padilla

_____

A mi querido Dios

A mis padres

Nicanor Morales Paternina y Luz Estella Chamorro

A mis hermanas

Laura y Luz Angela.

A mi familia y amigos

. Silvia Patricia Morales Chamorro.

_____

TABLA DE CONTENIDO

Pág

LISTA DE FIGURAS

Pág

LISTA DE TABLAS

Pág

LISTA DE ANEXOS

Pág

INTRODUCCIÓN

Con la evolución de las tecnologías asociadas a la información, la sociedad está cada día más involucrada con el mundo electrónico. Labores que tradicionalmente eran realizadas por seres humanos son, gracias a las mejoras tecnológicas, realizadas por sistemas automatizados. Dentro de las posibles actividades que pueden automatizarse, aquellas relacionadas con la capacidad para establecer la identidad de los individuos han cobrado importancia y como consecuencia directa, la biometría se ha transformado en un área emergente. La biometría es la ciencia que se dedica a la identificación de individuos a partir de una característica anatómica o un rasgo de su comportamiento.

Un área de desarrollo de la biometría es la seguridad biométrica, que permite, como su mismo nombre lo indica, asegurar el acceso físico (lugares) o virtual (información) a un grupo de personas previamente autorizadas, verificando sus identidades por medio del reconocimiento de una característica biométrica. La verificación es la etapa mas importante de la aplicación, pues es la que se encarga de realizar la asociación entre la característica biométrica tomada del usuario y la que se encuentra almacenada en el servidor de una base de datos construida en una etapa anterior. Esta etapa generalmente se apoya en las

redes neuronales artificiales (RNAs), que son sistemas de inteligencia artificial que permiten reconocer patrones tales como una característica biométrica.

De los muchos sistemas biométricos disponibles, la tecnología de reconocimiento de la huella dactilar se convierte en la mejor opción por la aceptación, conveniencia, fiabilidad y precisión para el usuario.

En el presente documento mostraremos el reconocimiento de huellas dactilares como mecanismo biométrico para la identificación y autorización en un sistema de control de acceso físico. Para ello nos apoyaremos en el uso de las redes neuronales artificiales, la cual explicaremos en detalle mas adelante, debido a su alta capacidad de aprendizaje, robustez y tolerancia a fallos.

1. CONTROL DE ACCESO A RECINTOS

Desde la antiguedad, el hombre ha tratado de controlar el acceso a determinados lugares, o a determinada información. Los sobres lacrados con el sello real, el conocimiento de un santo y seña, la utilización de un determinado uniforme, la posesión de una determinada llave, han permitido desde siempre el acceso a lugares restringidos.

Si nos remontamos unas décadas atrás y pensamos en la forma en que se controlaba el acceso a los lugares de máxima seguridad, indudablemente aparecerá en nuestras mentes una visión muy remota de los métodos del pasado. En la época medieval, los pobladores de aquellos exorbitantes castillos rodeados por extensos lagos, controlaban el acceso por medio de fornidos guerreros parados en torres ubicadas arriba de los puentes que hacían las veces de portones de ingreso, dando el visto bueno según una inspección de los datos suministrados por el forastero. Para continuar citando ejemplos recordemos que en las más atractivas películas de espionaje, cuando se producía la llegada de una persona a la casa de cualquier detective o a la guarida del malhechor de turno, el invitado, indefectiblemente, tenía que pronunciar una frase en forma de contraseña, la cual era respondida del otro lado con la continuación de ese refrán.

En la sociedad digital, se han sustituido los objetos anteriores por contraseñas, números PIN, certificados digitales, firmas digitales. Sin embargo estos

objetos o datos pueden ser robados, falsificados, filtrados o deducidos. Es fácil conocer la contraseña de una persona o adivinar un numero PIN. Para permitir autenticar a una persona, ya sea para acceder a un lugar físico, para efectuar una transacción bancaria o para realizar una compra se deben buscar métodos que no dependan de una "llave" determinada, sino que la propia persona sea la llave que le permita autenticarse. Es aquí donde entra la biometría.

Tabla 1. Comparación entre el sistema de código de barra y los sistemas biométricos.

CONCEPTO	CODIGO DE BARRAS	BIOMETRIA	CONCLUSIONES
TECNOLOGÍA	Sistema de tecnología de punta que incluye comunicación por puerto ethernet, tiene capacidad de crecimiento en memoria	Sistema de tecnología de punta que incluye comunicación por puerto ethernet, tiene capacidad de crecimiento en memoria	Ambos sistemas cuentan con opción electrónica actualizada, sólo que el biométrico es un equipo distinto de reconocimiento, ya que identifica personas, lo cual lo hace más confiable que el código de barras
IDENTIFICACIÓN	Estos sistemas reconocen OBJETOS, Mediante el uso de credenciales con código de barras	Este sistema reconoce PERSONAS, mediante el uso de parámetros biométricos	Se controla mejor el acceso, reconociendo a las personas que les esta permitido la entrada que reconocer objetos que pueden ser usados por otras personas
FRAUDE	Con estos sistemas cualquier persona puede prestar o extraviar su credencial	Con este sistema, nadie puede suplantar a otra persona, ya que la credencial es la misma persona.	Con los sistemas biométricos los fraudes son menores del 5%

En la Tabla 1 se muestra una comparación entre uno de los sistemas tradicionales de control de acceso como lo es el código de barra y los sistemas biométricos.

1. BIOMETRÍA

La biometría es la ciencia que se dedica a la identificación de individuos a partir de una característica anatómica o un rasgo de su comportamiento. Una característica anatómica tiene la cualidad de ser relativamente estable en el tiempo, tal como una huella dactilar, la silueta de la mano, patrones de la retina o el iris. Un rasgo del comportamiento, por ejemplo la firma, es menos estable pues depende de la disposición psicológica de la persona. No todas las características anatómicas pueden ser utilizadas con éxito por un sistema biométrico. Para que esto sea posible debe cumplir con las siguientes características:

Universalidad: cualquier persona posee esa característica.
Unicidad: la existencia de dos personas con una característica idéntica tiene una probabilidad muy pequeña.
Permanencia: la característica no cambia en el tiempo.
Cuantificación: la característica puede ser medida en forma cuantitativa.

Hasta la fecha se han desarrollado numerosos métodos de reconocimiento biométrico, con diferentes grados de aceptación y prestaciones. Entre los más desarrollados actualmente se encuentran los siguientes:

- Huella dactilar
- Geometría de mano

- Rostro
- Patrones de la retina
- Voz
- Firma

Además de estos métodos existen muchos otros que, o bien se encuentran en fase de desarrollo o su uso está menos extendido, pero que resultan, cuanto menos, curiosos. Ejemplos de estos sistemas pueden ser los basados en el olor de una persona, la forma de sus orejas, su forma de caminar etc, que nos demuestran que existen numerosas características discriminantes entre personas que, aunque se escapan a nuestros propios sentidos, permiten diferenciarnos a unos de otros mediante métodos automáticos. Sin embargo, hasta hoy, la identificación por medio de la huella dactilar ha sido una de las más utilizadas en el mercado.

2.1 SISTEMAS BIOMÉTRICOS PARA EL RECONOCIMIENTO DE PERSONAS

Los sistemas biométricos son sistemas automatizados capaces de reconocer a un individuo mediante una característica personal, la cual es adquirida y verificada de manera automática.

2.1.1 Características de un sistema biométrico para el reconocimiento de personas. Un sistema biométrico para la identificación de personas se considera útil y óptimo cuando posee las siguientes características:

El desempeño, que se refiere a la exactitud, la rapidez y la robustez alcanzada en la identificación, además de los recursos invertidos y el efecto de factores ambientales y operacionales.

La aceptabilidad, que indica el grado en que la gente está dispuesta a aceptar un sistema biométrico en su vida diaria. Es claro que el sistema no debe representar peligro alguno para los usuarios y debe inspirar confianza a los mismos.

La fiabilidad, que refleja cuán difícil es burlar al sistema. El sistema biométrico debe ser inmune a cualquier intento de engaño que pueda poner en riesgo la seguridad del sistema protegido, por ejemplo, debe ser capaz de diferenciar entre las características biométricas de una persona viva de una muerta.

2.1.2 Arquitectura de un sistema biométrico para la identificación de personas Los dispositivos biométricos poseen tres componentes básicos. El primero se encarga de la adquisición análoga o digital de algún indicador biométrico de una persona, como por ejemplo, la adquisición de la imagen de una huella dactilar mediante un escáner. El segundo maneja la compresión, procesamiento, almacenamiento y comparación de los datos adquiridos con los

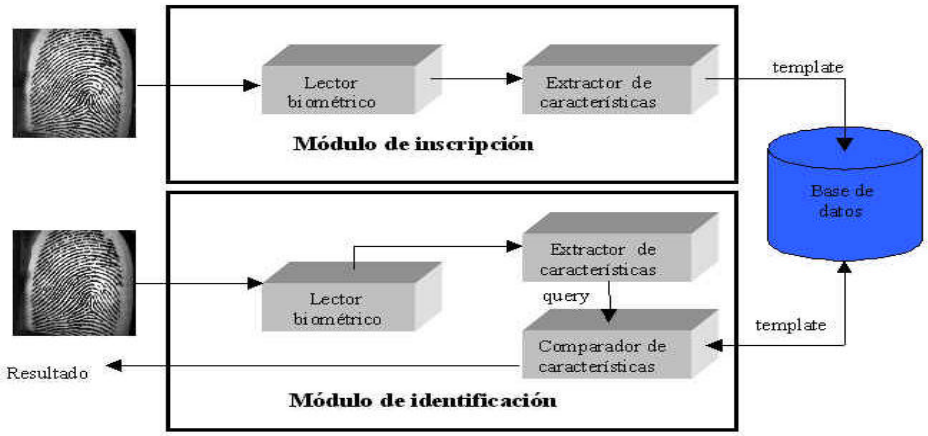
datos almacenados. El tercer componente establece una interfaz con aplicaciones ubicadas en el mismo u otro sistema.

La arquitectura típica de un sistema biométrico se presenta en la figura 1. Esta puede entenderse conceptualmente como dos módulos:

Módulo de inscripción (enrollment module)
Módulo de identificación (identification module).

El módulo de inscripción se encarga de adquirir y almacenar la información proveniente del indicador biométrico con el objeto de poder compararla con las que serán ingresadas posteriormente al sistema. Las labores ejecutadas por el módulo de inscripción son posibles gracias a la acción del lector biométrico y del extractor de características. El primero se encarga de adquirir datos relativos al indicador biométrico elegido y entregar una representación en formato digital de éste. El segundo extrae, a partir de la salida del lector, características representativas del indicador. El conjunto de características anterior, será almacenado en una base de datos central u otro medio como una tarjeta magnética y recibirá el nombre de plantilla (template). En otras palabras una plantilla es la información representativa del indicador biométrico que se encuentra almacenada y que será utilizada en las labores de identificación al ser comparada con la información proveniente del indicador biométrico en el punto de acceso.

Figura 1. Arquitectura de un sistema Biométrico



El módulo de identificación es el responsable del reconocimiento de individuos, por ejemplo en una aplicación de control de acceso. El proceso de identificación comienza cuando el lector biométrico captura la característica del individuo a ser identificado y la convierte a formato digital, para que a continuación el extractor de características produzca una representación compacta con el mismo formato de las plantillas. La representación resultante se denomina query y es enviada al comparador de *características* que confronta a éste con uno o varias plantillas para establecer la identidad.

El conjunto de procesos realizados por el módulo de inscripción recibe el nombre de *fase de inscripción*, mientras que los procesos realizados por el módulo de identificación reciben la denominación de *fase operacional*. A continuación se entregan detalles de esta última.

- **Fase Operacional de un Sistema de Identificación Personal**

Un sistema biométrico en su fase operacional puede operar en dos modos:

- *Modo de verificación*
- *Modo de identificación*

Un sistema biométrico operando en el modo de verificación comprueba la identidad de algún individuo comparando la característica sólo con las plantillas del individuo. Por ejemplo, si una persona ingresa su nombre de usuario entonces no será necesario revisar toda la base de datos buscando la plantilla que más se asemeje al de él, sino que bastará con comparar la información de entrada sólo con la plantilla que está asociado al usuario. Esto conduce a una comparación uno-a-uno para determinar si la identidad reclamada por el individuo es verdadera o no. De manera más sencilla, el modo de verificación responde a la pregunta: ¿eres tú quién dices ser?

Entre las aplicaciones más utilizadas en el modo verificación encontramos los siguientes:

- Control de acceso a un recinto.
- Control de acceso a un sistema informático.
- Control de identidad por las autoridades.
- Identificación en votaciones.
- Utilización de servicios (cajeros automáticos, transporte público, etc.).
- Cobro de servicios (comercio electrónico, pago a distancia, etc.)

Un sistema biométrico operando en el modo de identificación descubre a un individuo mediante una búsqueda *exhaustiva* en la base de base de datos con las plantillas. Esto conduce a una comparación del tipo *uno-a-muchos* para establecer la identidad del individuo. En términos sencillos el sistema responde la pregunta: ¿quién eres tú?

Entre las aplicaciones más utilizadas en el modo identificación encontramos los siguientes:

- Identificación forense de huellas dactilares latentes.
- Detección de sujetos en “listas negras”(terrorismo, delincuencia, etc.)
- Control de fronteras.
- Cobro automático sin interacción del usuario (pequeñas cantidades).

Generalmente es más difícil diseñar un sistema de identificación que uno de verificación. En ambos casos es importante la exactitud de la respuesta. Sin embargo, para un sistema de identificación la rapidez también es un factor crítico. Un sistema de identificación necesita explorar toda la base de datos donde se almacenan las plantillas, a diferencia de un sistema verificador. De la discusión anterior resulta obvio notar que la exigencia sobre el extractor y el comparador de características es mucho mayor en el primer caso.

- **Exactitud en la identificación.** La información dada por las plantillas permite fraccionar una base de datos de acuerdo a la presencia o ausencia de ciertos patrones particulares para cada indicador biométrico. Las "clases" así generadas permiten reducir el rango de búsqueda de alguna plantilla en la base de datos. Sin embargo, las plantillas pertenecientes a una misma clase también presentarán diferencias conocidas como *variaciones interclases*. Las variaciones interclases implican que la identidad de una persona puede ser establecida sólo con un cierto nivel de confianza. Una decisión tomada por un sistema biométrico distingue "personal autorizado" o "impostor". Para cada tipo de decisión, existen dos posibles salidas, verdadero o falso. Por lo tanto existe un total de cuatro posibles respuestas del sistema:

1. Una persona autorizada es aceptada
2. Una persona autorizada es rechazada
3. Un impostor es rechazado
4. Un impostor es aceptado

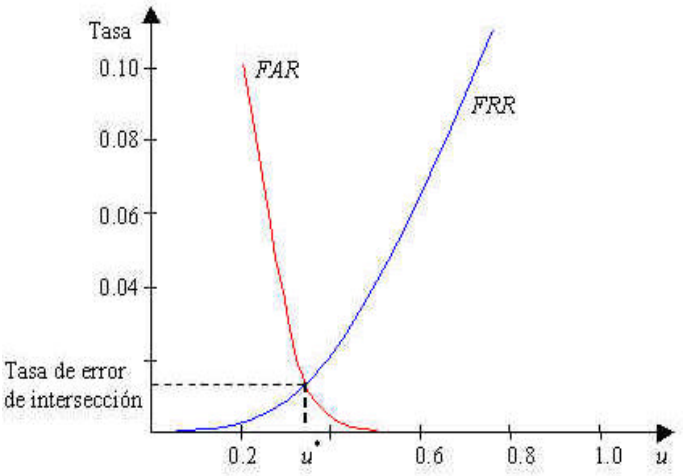
Las salidas números 1 y 3 son correctas, mientras que las números 2 y 4 no lo son. El grado de exactitud asociado a las diferentes decisiones puede ser caracterizado por la distribución estadística del número de personas autorizadas e impostores. En efecto, las estadísticas anteriores se utilizan para establecer dos tasas de errores:

Tasa de falsa aceptación (*FAR*: False Acceptance Rate), que se define como la frecuencia relativa con que un impostor es aceptado como un individuo autorizado.

Tasa de falso rechazo (*FRR*: False Rejection Rate), definida como la frecuencia relativa con que un individuo autorizado es rechazado como un impostor.

La *FAR* y la *FRR* son funciones del grado de seguridad deseado. En efecto, usualmente el resultado del proceso de identificación o verificación será un número real normalizado en el intervalo [0, 1], que indicará el "grado de parentesco" o correlación entre la característica biométrica proporcionada por el usuario y la(s) almacenada(s) en la base de datos. Si, por ejemplo, para el ingreso a un recinto se exige un valor alto para el grado de parentesco (un valor cercano a 1), entonces pocos impostores serán aceptados como personal autorizado y muchas personas autorizadas serán rechazadas. Por otro lado, si el grado de parentesco requerido para permitir el acceso al recinto es pequeño, una fracción pequeña del personal autorizado será rechazada, mientras que un número mayor de impostores será aceptado. El ejemplo anterior muestra que la FAR y la FRR están íntimamente relacionadas, de hecho son duales una de la otra: una FRR pequeña usualmente entrega una FAR alta, y viceversa. El grado de seguridad deseado se define mediante el umbral de aceptación u, un número real perteneciente al intervalo [0,1] que indica el mínimo grado de parentesco permitido para autorizar el acceso del individuo.

Figura 2. Gráfica típica de la tasa de falso rechazo (FRR) y la de falsa aceptación (FAR) como funciones del umbral de aceptación *u* para un sistema biométrico.



La FRR es una función estrictamente creciente y la FAR una estrictamente decreciente en u. La FAR y la FRR al ser modeladas como función del umbral de aceptación tienen por dominio al intervalo real [0,1], que es además su recorrido, puesto que representan frecuencias relativas. La figura 2 muestra una gráfica típica de la FRR y la FAR como funciones de u. En esta figura puede apreciarse un umbral de aceptación particular, denotado por *u**, donde la FRR y la FAR toman el mismo valor. Este valor recibe el nombre de tasa de *error de intersección (cross-over error rate)* y puede ser utilizado como medida única para caracterizar el *grado de seguridad* de un sistema biométrico.

En la práctica, sin embargo, es usual expresar los requerimientos de desempeño del sistema, tanto para verificación como para identificación,

mediante la FAR. Usualmente se elige un umbral de aceptación por encima de u* con el objeto de reducir la FAR, aumentando así la FRR.

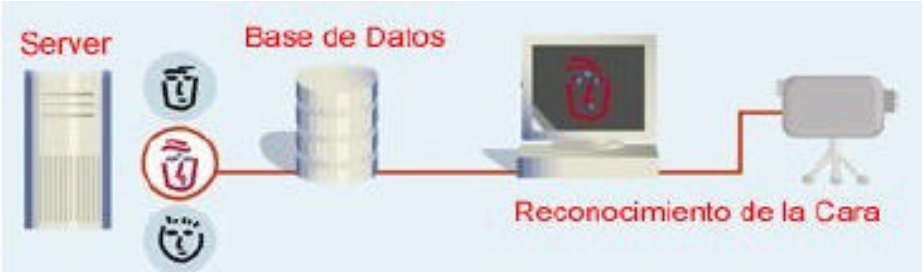
2.1.3 Descripción de los sistemas biométricos más usados. A continuación se hace una breve descripción de los sistemas biométricos mas usados en el control de acceso, para ello mencionaremos el reconocimiento de rostro, geometría de la mano, iris, voz, y de escritura (firma). En la siguiente sección explicamos detalladamente el funcionamiento de los sistemas de reconocimiento de huellas dactilares.

- **Reconocimiento del Rostro**

El sistema de reconocimiento de rostro consta de dos partes importantes que son la detección y el reconocimiento del rostro.

En la etapa de detección se aíslan los elementos faciales de una imagen y se elimina la información que no es útil. Existen software para el reconocimiento de rostros que permiten examinar la imagen en sus estructuras faciales típicas (tales como ojos y nariz), para luego calcular el resto de la cara y cortar los detalles del fondo, dando como resultado una cara dentro de un marco rectangular llamado una máscara binaria.

Figura 3. Sistema de Reconocimiento facial



En la etapa de reconocimiento se desarrollan las herramientas matemáticas que permiten analizar Las características faciales únicas. Generalmente en esta etapa se usa un sistema eigenfacebased o un sistema Eigenfeature.

El sistema eigenfacebased considera cada imagen facial como conjunto en dos dimensiones de las áreas claras y oscuras (eigenfaces) de un modelo determinado. El algoritmo del reconocimiento salva cada imagen como una combinación de eigenfaces y después compara las características del eigenface de la cara actual con las que se encuentran en la base de datos.

El sistema eigenfeature-based se centra en características específicas tales como la nariz, ojos, boca, cejas, y curvaturas del hueso, y las distancias relativas entre ellas. El sistema analiza la cara que se este explorando y extrae eigenfeatures determinados, que luego compara los que se encuentran en la base de datos.

La desventaja para los sistemas de reconocimiento de rostro es que la cara de la persona cambia a través del tiempo. El sistema debe tener en cuenta esos

cambios para hacer una correcta identificación y así poder ir actualizando su base de datos.

- **Reconocimiento de Iris**

El iris es uno de los órganos más propicios para usarlos en aplicaciones biométricas, puesto que es inmune a influencias medioambientales, las contracciones pupilares con los cambios de iluminación, son corregidas matemáticamente por los algoritmos que localizan los límites internos y exteriores del iris. Solamente en el iris hay más de 400 características distintivas, o grados de libertad (DOF), que pueden ser cuantificadas y usadas para identificar a un individuo.

En la práctica, se usan aproximadamente 260 de estas características. Algunas de estas son: surcos de contracción, estrías, huecos, fibras de colágeno, filamentos, anillos y manchas negras.

Figura 4. Sistema de Reconocimiento de Iris

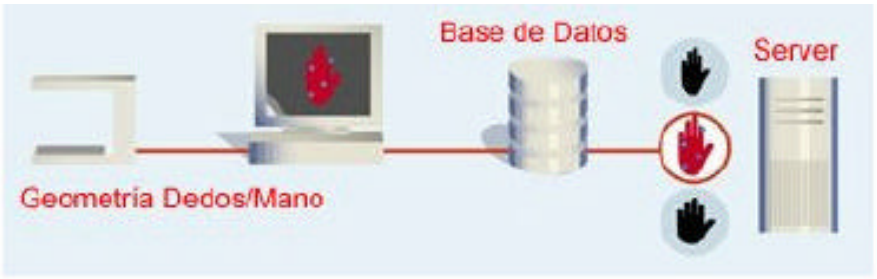
Los sistemas de reconocimiento basados en el Iris, se consideran muy seguros, debido a la distinción de los modelos y a la calidad de los dispositivos de la captura. Estos sistemas de reconocimiento de iris utilizan una cámara de video para capturar la muestra de un modelo determinado de iris y un software para comparar el modelo adquirido con los guardados en la base de datos.

El reconocimiento retinal ha sido predominantemente utilizado en agencias de alta seguridad. Tanto militares como instituciones financieras hacen uso de estos sistemas, entre ellas podemos destacar la CIA, FBI y NASA.

- **Reconocimiento de geometría de la mano**

En los sistemas de reconocimiento de geometría de la mano se crea una imagen tridimensional de la mano y analizan la dimensión de una variable sean, las longitudes, las áreas, y las posiciones relativas de los dedos, nudillos.

Figura 5. Sistema de Reconocimiento de Geometría de la Mano



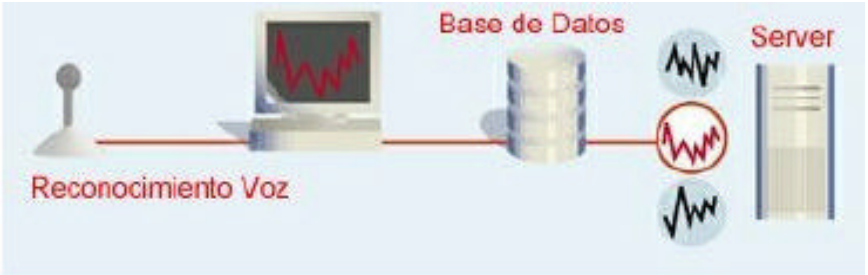
Con un sistema de este tipo, el usuario debe alinear una mano según unas marcas de guía que se encuentran en los scanner para geometría de mano,

luego un programa de lectura captura una imagen tridimensional de los dedos y los nudillos y salva los datos en un modelo. La geometría de la mano ha estado en uso por varios años, y fue utilizada para un sistema de seguridad en 1996 para los juegos olímpicos.

- **Reconocimiento de voz**

En los sistemas de reconocimiento de voz, se captura el sonido de la voz del hablante así como los comportamientos lingüísticos. Su uso primario está en aplicaciones telefónicas, pero su exactitud se puede afectar por cosas tales como ruidos extraños y los efectos de alguna enfermedad (gripa, laringitis) o de la fatiga en la voz. Un problema obvio con el reconocimiento de voz es la posibilidad de fraude: El sistema puede ser engañado por una cinta grabada. Por esta razón, los sistemas avanzados de reconocimiento pueden ampliar el proceso de la verificación dando al usuario algunas frases largas y difíciles para leer en voz alta, o solicitando cada vez que se lea una frase distinta. Esto aumenta el tiempo requerido para la verificación, pero aumenta mucho la utilidad total del sistema.

Figura 6. Sistema de Reconocimiento de la Voz



- **Reconocimiento de la Firma**

Generalmente en este tipo de sistemas no solo se analizan las variables geométricas firma sino también la velocidad, la presión a la que se escribe. Estos parámetros se obtienen cuando la persona escribe con una pluma o en una tablilla especialmente diseñadas para esta función, luego se compara con las firmas y los patrones analizados y previamente recopilados en una base de datos.

Figura 7. Arquitectura de un sistema de reconocimiento de firma

La desventaja de los sistemas de reconocimiento de firma esta en la necesidad de tomar múltiples muestras de un mismo modelo de firma, con el fin de asegurar la verificación a pesar de que existan variaciones en esta.

3. RECONOCIMIENTO BIOMETRICO POR MEDIO DE LA IDENTIFICACIÓN DE HUELLAS DACTILARES

Ahora que las técnicas biométricas mas empleadas para el control de acceso han sido brevemente explicadas, iniciaremos el estudio detallado que corresponde a la presente monografía, el análisis del reconocimiento biométrico de huellas dactilares para su uso en sistemas de control de acceso.

3.1 ANTECENDENTES DE LA HUELLA DACTILAR

Las huellas dactilares han tenido diferentes usos a lo largo de la historia de la humanidad. Debido a que las huellas dactilares son un rasgo distintivo entre los seres humanos, estas han sido utilizadas como medio de identificación. Según B.C. Bridgest, especialista en la materia, las huellas dactilares comenzaron a usarse en las antiguas civilizaciones: “Algunos de lo primeros usos prácticos de la identificación mediante impresiones dactilares son acreditados a los chinos; quienes la aplicaban diariamente en sus negocios y empresas legales mientras tanto el mundo occidental se encontraba en el periodo conocido como la edad oscura”. Asimismo, dice Bridgest, en el libro de leyes chino de Yung Hwui: “Se establecía que para divorciarse de la esposa, el esposo debía dar un documento que expusiera siete razones para hacerlo. Todas las letras deberían estar escritas con su propia mano y signar el documento con sus huellas dactilares”.

Las huellas dactilares también son mencionadas en la Biblia: “y puso un sello sobre su mano para memoria ante sus ojos” (Éxodo 13:9) y se refiere a ellas precisamente como una característica distintiva entre los seres humanos.

En investigaciones criminalísticas han sido utilizadas desde el siglo XIX y en la actualidad, haciendo uso de métodos electrónicos se constituyen en un recurso mucho más efectivo en este campo.

En México (artículo 1834 del Código Federal Civil) como en otros países del mundo, las huellas digitales son reconocidas legalmente como sustituto de la firma escrita, indispensable para imponer obligación en un contrato o documento, en los casos en que la persona involucrada no pueda o no sepa firmar.

3.2 VENTAJAS DE LA HUELLA DACTILAR FRENTE A OTROS SISTEMAS BIOMETRICOS

De los muchos sistemas biométricos disponibles, la tecnología de reconocimiento de la huella dactilar se convierte en la mejor opción para la aceptación, conveniencia, fiabilidad, precisión para el usuario y fácil integración con las aplicaciones.

El reconocimiento de las huellas dactilares es la tecnología más antigua y más comúnmente usada teniendo probados sus méritos por más de un siglo.

Solamente esta tecnología puede presumir de su aceptación científica e histórica.

Actualmente, los dispositivos de reconocimiento de huellas tienen la porción más grande del mercado de los dispositivos biométricos estimado en $250.000.000 de dólares anuales. Los campos de aplicación donde el reconocimiento de huellas se destaca no tienen límites, sistemas de control de acceso, sistemas de administración, sistemas de ignición de vehículos, sistemas de autorización de credenciales, comercio electrónico, seguridad informática, autorización de acceso a webs y redes, etc.

Con esta tecnología de reconocimiento, es posible acceder a un mundo más conveniente y seguro con sólo la punta de los dedos.

3.3 DESVENTAJAS DEL RECONOCIMIENTO DE HUELLAS DACTILARES

La tecnología biométrica basada en la huella dactilar necesita que la huella de todos los individuos que serán registrados en el sistema se encuentre en buen estado; esto la hace sensible a posibles defectos en la huella, ya sean permanentes o temporales, asociados a una determinada herida o enfermedad (dermatitis, quemaduras, etc.), desgaste causado por manipular o tocar líquidos o superficies abrasivas, (detergentes, ácidos, etc) o simplemente dedos con la superficie extremadamente arrugada o con durezas (lo cual es muy común en

personas de edad avanzada). Esto puede causar que un bajo porcentaje del personal no pueda ser identificado por los equipos.

En el caso de reconocimiento de geometría de mano, variaciones en el volumen o forma de la mano pueden originar falsos rechazos y llevar a la necesidad de volver a registrar al individuo nuevamente, con el fin de que pueda ser identificado. En los casos en que los cambios o deterioro de los patrones físicos (huella o mano) sean permanentes o imposibiliten la identificación, la mayoría de los equipos permiten optar por identificar a la persona sólo ingresando una clave adicional o al pasar una tarjeta del tipo magnético, código de barras o de proximidad por un lector externo.

Tabla 2. Comparación entre los métodos biométricos

	Ojo - Iris	Ojo - Retina	Huellas dactilares	Geometría de la mano	Escritura - Firma	Voz
Fiabilidad	Muy alta	Muy alta	Alta	Alta	Alta	Alta
Facilidad de uso	Media	Baja	Alta	Alta	Alta	Alta
Prevención de ataques	Muy Alta	Muy alta	Alta	Alta	Media	Media
Aceptación	Media	Media	Media	Alta	Muy alta	Alta
Estabilidad	Alta	Alta	Alta	Media	Media	Media
Identificación y autenticación	Ambas	Ambas	Ambas	Autenticación	Ambas	Autenticación
Interferencias	Gafas	Irritaciones	Suciedad, heridas,	Artritis, reumatismo	Firmas	Ruido, resfriado

Utilización	Instalaciones nucleares, servicio médico	Instalación nuclear, servicio médicos,	Policía, industrial	General	Industrial	Accesos remotos en bancos o bases de datos

En la tabla anterior se muestra una comparación entre los diferentes métodos biométricos. Se observa que la huella dactilar tiene grandes ventajas frente a los demás métodos biométricos.

3.4 CARACTERÍSTICAS BIOMÉTRICAS DE LAS HUELLAS DACTILARES

Las huellas dactilares son uno de los sistemas biométricos mas utilizados en el mercado, debido a que cumple con todas las características biométricas necesarias para que el sistema sea óptimo.

Las huellas dactilares son una característica exclusiva de los primates. En los seres humanos se forman en la sexta semana intrauterina y en situaciones de vida normal sus características son invariantes con el tiempo y únicas para cada individuo, aún cuando se trate de gemelos.

La huella dactilar de un individuo se va formando debido a pequeñas variables en las concentraciones del factor del crecimiento y a las hormonas localizadas dentro del tejido. Las rigurosidades de la huella dactilar están constituidas por salientes y depresiones. Las salientes se denominan crestas papilares y las

depresiones surcos interpupilares. En las crestas se encuentran las glándulas sudoríparas. El sudor que éstas producen contiene aceite, que se retiene en los surcos de la huella, de tal manera que cuando el dedo hace contacto con una superficie, queda un residuo de éste, lo cual produce un facsímil o negativo de la huella.

Las huellas dactilares se toman de los dedos índices de ambas manos, tanto por la comodidad al capturarlas, como porque estos dedos están menos propensos a sufrir accidentes que dejen cicatriz.

Tabla 3. Características biométricas de las huellas dactilares

CARACTERÍSTICAS BIOMÉTRICAS	RENDIMIENTO	COMENTARIOS
Facilidad de medida	Media	Lectores sencillos, pero sujetos a suciedad, cicatrices, etc.
Universalidad	Alta	
Permanencia	Alta	
Unicidad	Alta	Abundante evidencia
Prestaciones	Buena	Algoritmos eficientes
Aceptabilidad	Alta	Larga tradición
Resistencia al engaño	Media	Algunos sensores son relativamente fáciles de confundir.

3.4.1 Clasificación de las huellas dactilares. Una huella dactilar es la representación de la morfología superficial de la epidermis de un dedo. Posee un conjunto de líneas que, en forma global, aparecen dispuestas en forma paralela (colinas o *ridge lines* y *furrows*). Sin embargo estas líneas se

interceptan y a veces terminan en forma abrupta. Los puntos donde las colinas terminan o se bifurcan se conocen técnicamente como minucias. Otros puntos singulares de una huella dactilar son aquellos donde la curvatura de las colinas es máxima. Esos puntos reciben el nombre de deltas. La característica más interesante que presentan tanto las minucias como los puntos singulares deltas es que son únicos para cada individuo y permanecen inalterados a través de su vida. A pesar de esta variedad de minucias (18 tipos distintos de minucias han sido enumerados) las más importantes son las *terminaciones y bifurcaciones* de colinas. Esto último se debe a que las terminaciones de colinas representan aproximadamente el 60.6% de todas las minucias en una huella y las bifurcaciones el 17.9%. Además varias de las minucias menos típicas pueden expresarse en función de las dos señaladas.

Figura 8. Puntos característicos de una huella dactilar

En la figura 8 se muestran 5 puntos característicos que hay en un dedo, éstos se repiten indistintamente para formar entre 60 y 120 en total.

Para concluir si dos huellas dactilares corresponden o no a la misma persona se lleva a cabo un procedimiento que comienza con la clasificación de la huella dactilar y termina con el *matching* o comparación de las minucias de ambas

huellas. La clasificación de huellas corresponde a un análisis a escala "gruesa" de los patrones globales de la huella que permite asignarla a un conjunto predeterminado o *clase*, lo que se traduce en una partición de la base de datos a ser revisada. Por otro lado, la comparación de huellas lleva a cabo una comparación a escala "fina" de las huellas dactilares a partir de los vectores de características resultantes de representar la geometría de cada una de las *minucias*. En otras palabras, la comparación de huellas dactilares consiste en encontrar el grado de *similaridad* entre dos vectores de características cuyas componentes representan a las minucias de cada huella.

3.5 TIPOS DE SISTEMAS DE RECONOCIMIENTO POR MEDIO DE HUELLAS DACTILARES

Básicamente los sistemas biométricos basados en huellas dactilares son de dos tipos:

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 similitud entre ésta y la huella dada. Ambos sistemas utilizan los detalles formados por las huellas dactilares.

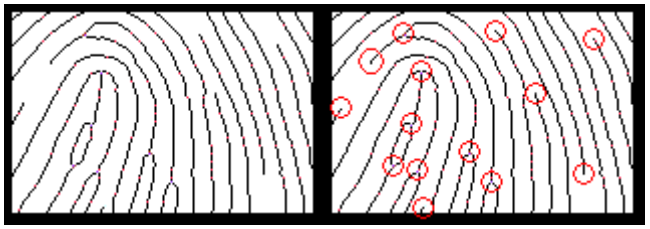
3.6 TÉCNICAS PARA LA VERIFICACIÓN DE LAS HUELLAS

Existen dos técnicas para realizar la verificación de las huellas:

Basada en Detalles: Esta técnica elabora un mapa con la ubicación relativa de "detalles" sobre la huella, los cuales permiten ubicar con certeza a un individuo. Sin embargo, existen algunas dificultades cuando se utiliza está aproximación. Es muy difícil ubicar los detalles con precisión cuando la huella suministrada es de baja calidad. También este método no toma en cuenta el patrón global de las crestas y los surcos. Entre algunos detalles que podemos encontrar en una huella, tenemos:

Cada individuo posee uno y solo uno, arreglo de detalles.

Figura 9. Detalles de las minucias



El mismo puede ser descrito por un modelo de probabilidad:

$P(C)=P(N).P(M).P(A)$

Donde: $P(C)$ = f(Ley de Poisson)

$P(M)$= f(frecuencia de aparición del detalle)

$P(A)$ = f(número de permutaciones posibles de detalles)

Basadas en correlación: Este método viene a mejorar algunas dificultades presentadas por la aproximación creada por los el patrón de detalles, pero inclusive él mismo presenta sus propias fallas, está técnica requiere de la localización precisa de un punto de registro el cual se ve afectado por la rotación y traslación de la imagen.

Una vez obtenida la huella digital es necesario clasificarla. Este proceso consiste en ubicar dicha huella dentro de los varios tipos existentes, los cuales proveen un mecanismo de indexado; esto con la finalidad de reducir el tiempo de búsqueda. Los algoritmos existentes permiten clasificar la huella en cinco clases:

- Anillo de Crestas.
- Lazo Derecho.
- Lazo Izquierdo.
- Arco.
- Arco de Carpa

Estos algoritmos separan el número de crestas presentes en cuatro direcciones (0°, 45°, 90° y 135°) mediante un proceso de filtrado de la parte central de la huella

3.7 TIPOS DE SENSORES BIOMÉTRICOS PARA LA ADQUISICION DE HUELLA DACTILAR

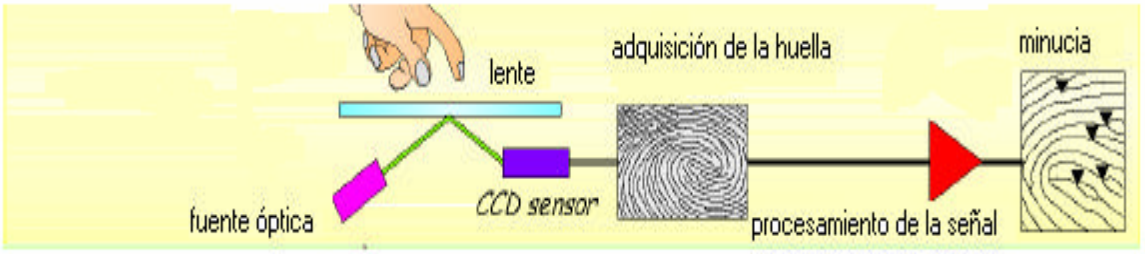
Existen cuatro tipos de sensores biométricos para adquirir una huella dactilar que son; Sensores ópticos, capacitivos y térmicos y de campo eléctrico a continuación se define el principio de funcionamiento de cada uno de ellos.

3.7.1 Sensores de Tipo Óptico. El método óptico es uno de los más comunes. El núcleo del escáner óptico es una cámara CCD (Dispositivo de Carga Acoplada)

La cámara CCD consiste simplemente en una serie de diodos sensibles a la luz llamados fotolitos. Normalmente el dedo se coloca en una placa de cristal y la cámara hace una foto.

El sistema CCD tiene una capa de LEDs (diodos emisores de luz) para iluminar las crestas y surcos del dedo. La ventaja de los sistemas ópticos es su bajo precio; la desventaja es que son bastante fáciles de falsificar. Otro problema es que en ocasiones pueden permanecer en la superficie del sensor algunos rasgos del dactilograma anterior.

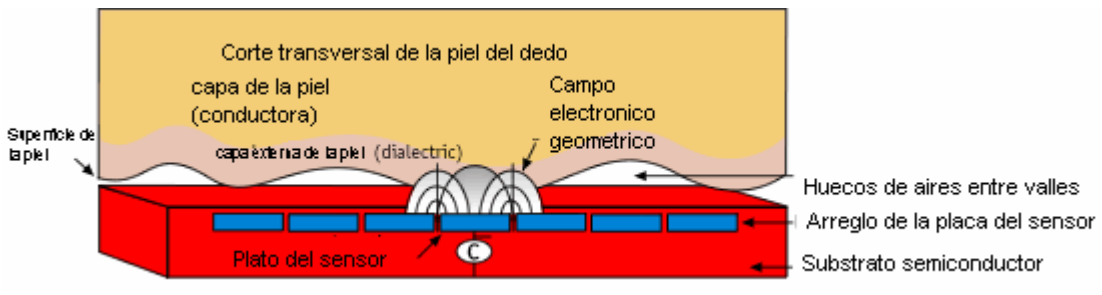
Figura 10. Funcionamiento de Sensor Óptico



3.7.2 Sensores De Tipo Capacitivo. El método capacitivo es uno de los más populares. Al igual que otros escáner, genera una imagen de las cresta y valles. En la superficie de un circuito integrado de silicona se dispone un arreglo de platos sensores capacitivos conductores cubiertos por una capa aislante.

La capacitancia en cada plato sensor es medida individualmente depositando una carga fija sobre ese plato (Ver figura 11). La mayor ventaja es que se requiere una huella real pero se pueden presentar problemas si la yema del dedo está húmeda o muy seca. En este caso se obtendrán imágenes negras o pálidas.

Figura 11. Funcionamiento de Sensor Capacitivo



3.7.3 Sensores de Tipo Termoeléctrico. El método termoeléctrico es menos común. Este tipo de sensores utiliza un sistema único para reproducir el dedo completo “arrastrándolo” a través del sensor. Durante este movimiento se realizan tomas sucesivas (slices) y se pone en marcha un software especial que reconstruye la imagen del dedo. Este método permite obtener una gran calidad de la imagen impresa de la huella dactilar.

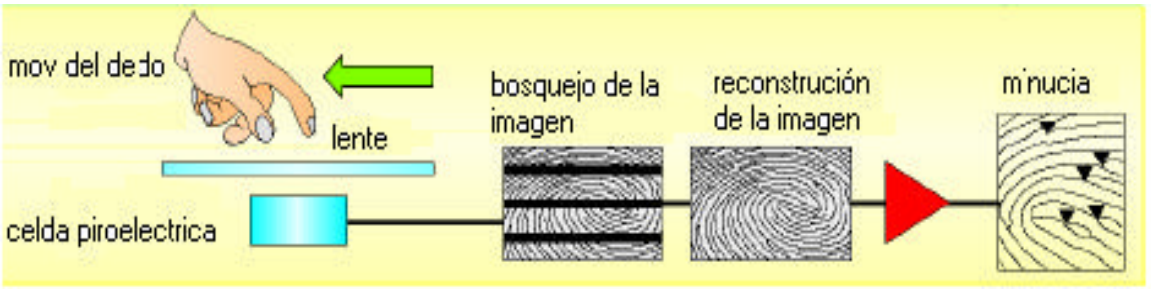
El sensor mide la temperatura diferencial entre las crestas papilares y el aire retenido en los surcos. Este método proporciona una imagen de gran cualidad incluso cuando las huellas dactilares presentan alguna anomalía como sequedad o desgaste con pequeñas cavidades entre las cimas y los surcos de la huella. La tecnología termal permite también su uso bajo condiciones medioambientales extremas, como temperaturas muy altas, humedad, suciedad o contaminación de aceite y agua.

Además, también cuenta con la ventaja de autolimpiado del sensor, con lo que se evitan las huellas latentes. Se denomina así a las huellas que permanecen en el sensor una vez utilizado, lo cual puede ocasionar problemas no sólo en las lecturas posteriores sino que permite que se copie la huella para falsificarla y acceder así al sistema. De hecho, este método de arrastre que utiliza la tecnología basada en el calor hace que el sensor esté por encima de otras tecnologías. El sensor funciona con bajas temperaturas, alto porcentaje de humedad, etc.

Otra ventaja es la reproducción de una imagen grande de alta cualidad y siempre un sensor limpio. La desventaja es que la cualidad de la imagen depende un poco de la habilidad del usuario que utiliza el escáner. La segunda desventaja es el calentamiento del sensor que aumenta el consumo de energía considerablemente. Este calentamiento es necesario para evitar la posibilidad de un equilibrio térmico entre el sensor y la superficie de la yema dactilar.

El elevado volumen de diseño del escáner permite que su precio sea bajo ya que en el proceso de manufacturación se necesita menos silicona. En la figura 12 se observa el funcionamiento de este tipo de sensor.

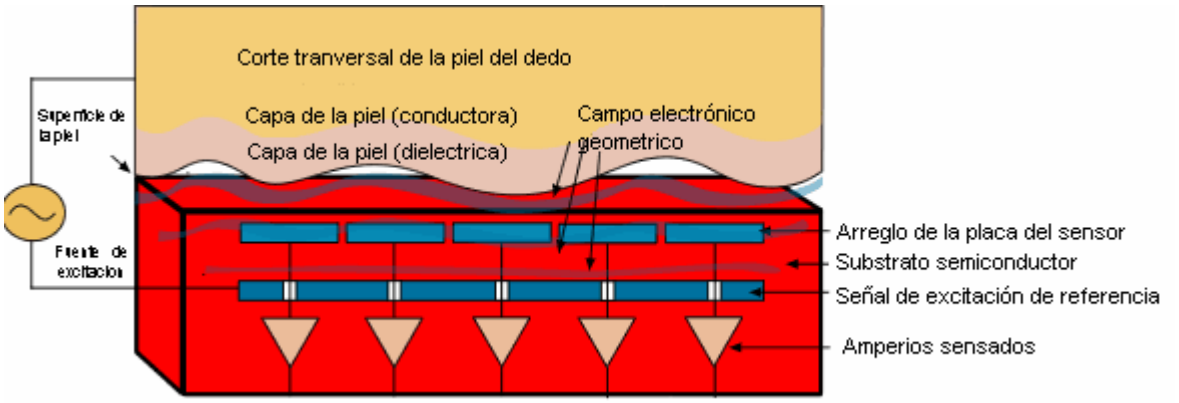
Figura 12. Funcionamiento de Sensor Termoeléctrico



3.7.4 Sensor de Matriz De Antena (Campo Eléctrico). Un pequeño campo RF es aplicado entre dos capas conductoras, una oculta dentro de un chip de silicon (llamado plano de referencia de la señal de excitación) y la otra localizada por debajo de la piel del dedo. (Ver figura 13.) El campo formado entre estas capas reproduce la forma de la capa conductora de la piel en la amplitud del campo AC. Diminutos sensores insertados por debajo de la

superficie del semiconductor y sobre la capa conductora, miden el contorno del campo. Amplificadores conectados directamente a cada plato sensor convierten estos potenciales a voltajes, representando el patrón de la huella. Estas señales son acondicionadas en una etapa siguiente para luego ser multiplexadas fuera del sensor.

Figura 13. Funcionamiento de matriz de antena



4. REDES NEURONALES ARTIFICIALES

Inspiradas en el sistema nervioso biológico, la tecnología de las redes neuronales artificiales está siendo utilizada para solucionar una gran variedad de problemas científicos, económico/comerciales y de ingeniería. Las redes neuronales son ideales para esa clase de problemas porque como sus compañeras biológicas, una red neuronal artificial puede aprender, y luego ser entrenada para encontrar soluciones, reconocer patrones, clasificar datos y hacer previsión de eventos futuros.

En contraste a las aproximaciones clásicas en campos como la estadística y la teoría de control, las redes neuronales no requieren un modelo explícito o la toma limitada de normalidad o linealidad. Las redes neuronales son una herramienta muy poderosa en aplicaciones en donde el análisis formal debería ser extremadamente difícil, o hasta imposible, como reconocimiento de patrones e identificación de sistemas no lineales, y control.

El comportamiento de una red neuronal es definido por la forma en que sus elementos computacionales individuales están conectados entre sí, y por el ancho de esas conexiones, o pesos. Los pesos son automáticamente ajustados por el entrenamiento de la red de acuerdo con una regla específica de aprendizaje, hasta que ésta llegue al nivel de error deseado.

Las RNAs han permitido avances significativos en diversas áreas de investigación tales como biología, fisiología, sicología, ingeniería electrónica, sistemas, matemáticos, etc. Las cuales tienen objetivos diferentes, tales como entender los sistemas biológicos, el comportamiento humano y animal, desarrollar sistemas para aplicaciones específicas, etc.

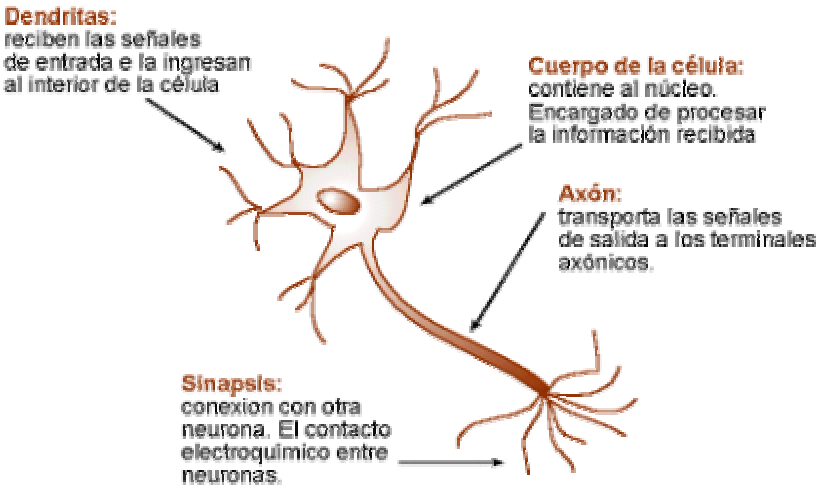
Las redes neuronales artificiales son una herramienta potencial puesto que tienen aplicaciones en tareas donde no hay reglas bien definidas las cuales parecen fáciles para los humanos y difíciles para las computadoras.

La Inteligencia Artificial ha estado generalmente dominada por las áreas de manipulación lógica y simbólica, pero las RNAs han tomando campo en las aplicaciones de la Inteligencia Artificial tradicional. Más bien parece que se combinaran para apoyarse mutuamente, como sucede en los seres humanos, pues los sistemas biológicos se apoyan en sistemas neuronales que permiten reconocer patrones como la voz, olores, imágenes, etc. Es el caso de los sistemas biométricos, donde las redes neuronales artificiales representan un apoyo para abstraer las características de los patrones de entrada (voz, firma, huella dactilar, etc.) al sistema y posteriormente hacer el reconocimiento.

4.1 COMPARACIÓN DE LAS NEURONAS BIOLÓGICAS CON LAS NEURONAS ARTIFICIALES

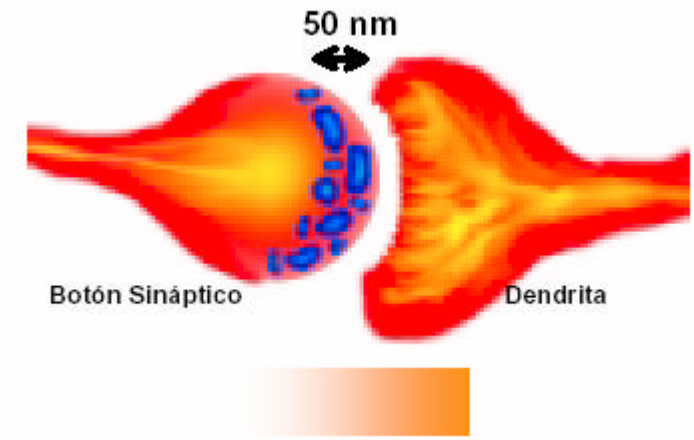
La estructura de las Redes Neuronales Artificiales se basa vagamente en la estructura del cerebro.

Figura 14. Componentes de una neurona biológica.



Una neurona biológica, como la que se muestra en la Figura 14, es el bloque fundamental de construcción del sistema nervioso. Esta es una célula similar a otras del cuerpo con ciertas especializaciones.

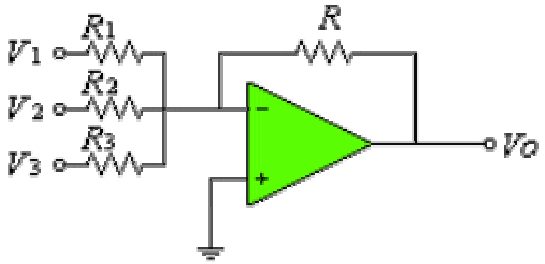
Figura 15. Salto sináptico



Una neurona está compuesta de 3 partes fundamentales que son: cuerpo, dendritas y axón. Las dendritas reciben señales de otras células en puntos de conexión llamadas sinapsis (ver Figura 15), de donde las señales pasan al cuerpo de la célula, para ser esencialmente promediadas con otras señales. Si este promedio en un determinado tiempo es suficientemente grande, la célula es excitada, mandando un pulso a través del axón a otras células. No obstante esta simplicidad en su operación, las neuronas realizan la mayoría de las actividades cerebrales. Internamente existe un complicado sistema electroquímico de comunicación y control.

El modelo de una neurona artificial es una imitación del proceso de una neurona biológica, puede también asemejarse a un sumador hecho con un amplificador operacional tal como se ve en la figura 16.

Figura 16. Diagrama de una Neurona Artificial



$$Vo = -\sum_{i=1}^{n} \frac{R}{Ri} Vi$$

Las entradas, que pueden ser llamadas vector X, corresponden a las señales que llegan a la sinápsis de una neurona biológica. Cada señal se multiplica por un peso que tiene asociado, W_1,W_2 ... Wn (Controlados por los valores de las resistencias R_1, R_2... Rn). Los pesos los podemos llamar vector W.

Cada peso corresponde a la intensidad o fuerza de la conexión de una sinápsis en una neurona biológica. Estas multiplicaciones se sum0an. Este sumador corresponde vagamente al cuerpo de una neurona biológica. Como se observa, esta es una suma algebraica de las entradas ponderadas, entonces:

NET = X1 W1 + X2 W2 + X3 W3 + ... Xn Wn.

4.2 CARACTERISTICAS DE LAS REDES NEURONALES ARTIFICIALES

Debido a su constitución y a sus fundamentos, las RNA presentan un gran número de características semejantes a las del cerebro. Por ejemplo, son capaces de aprender de la experiencia, de generalizar de casos anteriores a nuevos casos, de abstraer características esenciales a partir de entradas que representan información irrelevante, etc. Esto hace que ofrezcan numerosas ventajas y que este tipo de tecnología se esté aplicando en múltiples áreas. Estas ventajas incluyen:

4.2.1 Aprendizaje Adaptativo. Es una de las características más atractivas de las redes neuronales, es la capacidad de aprender a realizar tareas basadas en un entrenamiento o una experiencia inicial.

En el proceso de aprendizaje, los enlaces ponderados de las neuronas se ajustan de manera que se obtengan unos resultados específicos. Una RNA no necesita un algoritmo para resolver un problema, ya que ella puede generar su propia distribución de los pesos de los enlaces mediante el aprendizaje. También existen redes que continúan aprendiendo a lo largo de su vida, después de completado el periodo inicial de entrenamiento.

La función del diseñador es únicamente la obtención de la arquitectura apropiada. No es problema del diseñador el cómo la red aprenderá a discriminar; sin embargo, si es necesario que desarrolle un buen algoritmo de

aprendizaje que proporcione la capacidad de discriminar de la red mediante un entrenamiento con patrones.

4.2.2 Autoorganización. Las redes neuronales usan su capacidad de aprendizaje adaptativo para organizar la información que reciben durante el aprendizaje y/o la operación. Una RNA puede crear su propia organización o representación de la información que recibe mediante una etapa de aprendizaje. Esta autoorganización provoca la facultad de las redes neuronales de responder apropiadamente cuando se les presentan datos o situaciones a los que no habían sido expuestas anteriormente.

4.2.3 Tolerancia a Fallos. Comparados con los sistemas computacionales tradicionales, los cuales pierden su funcionalidad en cuanto sufren un pequeño error de memoria, en las redes neuronales, si se produce un fallo en un pequeño número de neuronas, el comportamiento del sistema se ve influenciado, sin embargo, no sufre una caída repentina.

Hay dos aspectos distintos respecto a la tolerancia a fallos: primero, las redes pueden aprender a reconocer patrones con ruido, distorsionados, o con información incompleta. Segundo pueden seguir realizando su función (con cierta degradación) aunque se destruya parte de la red.

La razón por la cual las redes neuronales son tolerantes a fallos es que tienen su información distribuida en las conexiones entre neuronas, existiendo cierto

grado de redundancia en ese tipo de almacenamiento, a diferencia de la mayoría de los ordenadores algorítmicos y sistemas de recuperación de datos que almacenan cada pieza de información en un estado único, localizado y direccionable.

4.2.4 Operación en Tiempo Real. Los computadores neuronales pueden ser realizados en paralelo, y se diseñan y fabrican máquinas con hardware especial para obtener esta capacidad.

4.2.5 Fácil Inserción Dentro de la Tecnología Existente. Debido a que una red puede ser rápidamente entrenada, comprobada, verificada y trasladada a una implementación hardware de bajo costo (Ej. Microcontroladores), es fácil insertar RNA para aplicaciones específicas dentro de sistemas existentes (Ej. LVDQ). De esta manera, las redes neuronales se pueden utilizar para mejorar sistemas de forma incremental, y cada paso puede ser evaluado antes de llevar a cabo un desarrollo más amplio.

4.3 ARQUITECTURAS Y APRENDIZAJES TIPICOS DE LAS RNAs

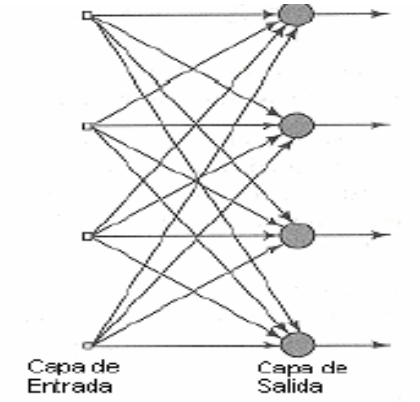
Las RNAs tienen asociada una estructura, formada por muchos procesadores simples llamados nodos o neuronas, conectados por medio de canales de comunicación o conexiones. Cada una de ellas tiene una cantidad de memoria local, operando solamente con sus datos locales y sobre las entradas que recibe a través de esas conexiones. Las RNAs llevan asociadas algún tipo de

regla de aprendizaje o entrenamiento particular por lo cual esas conexiones son ajustadas acorde a los ejemplos proporcionados. En otras palabras, las RNAs aprenden a partir de ejemplos, y muestran alguna capacidad para generalizar más allá de esos datos mostrados.

4.3.1 Arquitecturas. La implementación de las RNAs puede plantearse siguiendo dos vías: el de la simulación software para aplicaciones sencillas, donde el tiempo de decisión sea razonable, y el de la implementación hardware, para aplicaciones que precisen alta velocidad de decisión (respuesta en tiempo real). La formulación de los algoritmos de aprendizaje en forma matricial facilita ambas prácticas. Existen 4 bases estructurales para las RNAs, siendo estas el origen en la implementación de redes más complejas.

- **Redes progresivas Monocapa**

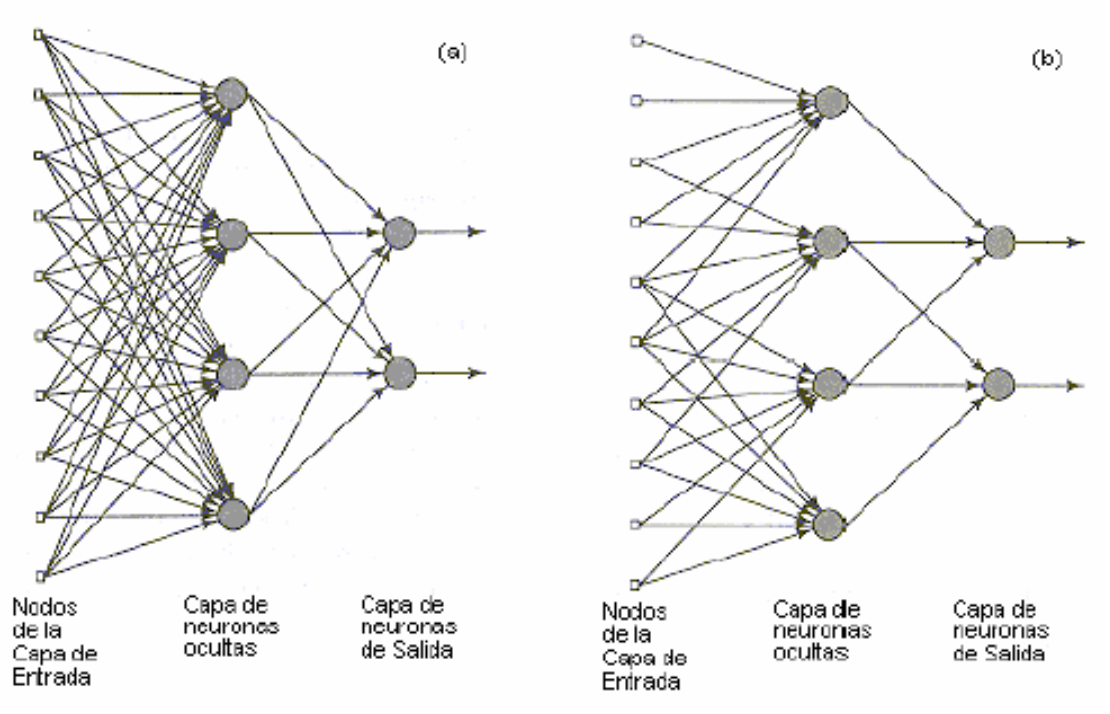
Figura 17. Redes progresivas monocapa



Una RNA formada por sucesivas capas tendrá como forma más simple una capa de nodos de entrada y otra de nodos de salida, ver figura 17.

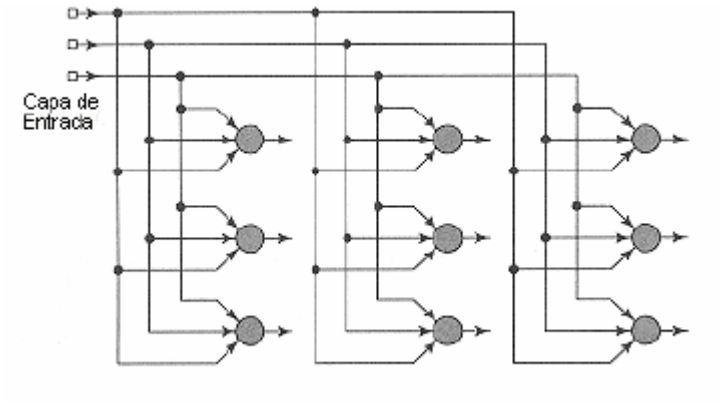
- **Redes progresivas Multicapas**

Figura 18. Redes progresivas Multicapa. a) Conexión total. b) Conexión parcial.



Una RNA multicapa consiste de la extensión de la monocapa en una estructura con tantas capas ocultas como se requiera. Encontramos en esta arquitectura dos variantes: las RNAs totalmente conectadas (figura 18a), y las parcialmente conectadas (figura 18b) donde, dentro de éstas últimas, tenemos el caso de las RNAs localmente conectadas. Este subgrupo se caracteriza porque no todas las unidades de la capa oculta están conectadas a todas las unidades de entrada.

Figura 19. Estructuras Lattice bidimensional de 3x3 neuronas.

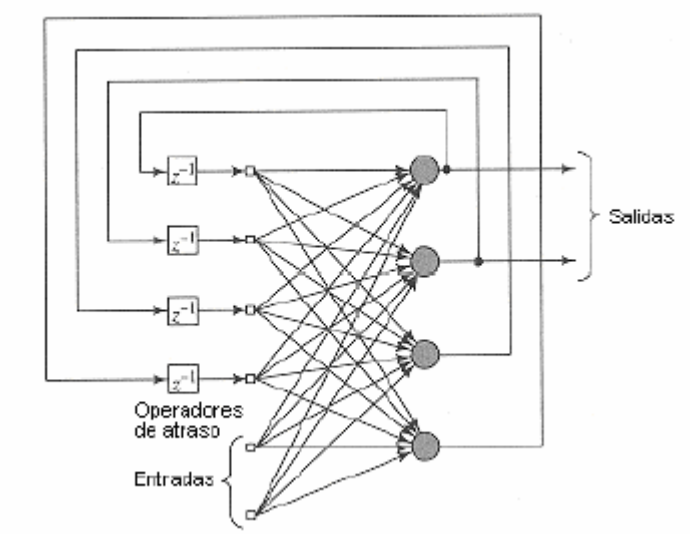


Consisten en arreglos de neuronas de varias dimensiones con su correspondiente conjunto de nodos fuente, la conexión de este tipo de neuronas se muestra en la figura 19.

- **Redes Recurrentes**

La diferencia fundamental con las arquitecturas anteriores está en que aquí existe un lazo de realimentación.

Figura 20. Red Recurrente con neuronas ocultas



En la figura 20 se muestra un tipo de arquitectura recurrente donde aparecen neuronas ocultas (opcional) y una realimentación formada por unidades de retardo denotadas por z-1.

4.3.2 Reglas de Aprendizaje. El aprendizaje en RNAs es el proceso por el cual los parámetros libres de una red neuronal son adaptados por medio de un proceso de estimulación. El modo en que estos cambios se produzcan nos indicará el tipo de aprendizaje realizado. La definición de aprendizaje implica que la RNA estará estimulada desde fuera y que se producirán cambios como consecuencia directa de esta estimulación. La RNA responderá de alguna manera, ya que esos cambios se reflejarán en su estructura interna.

Existen varias clasificaciones posibles, según las reglas o a los esquemas de aprendizaje. Las diferencias se centran en la formulación matemática de los algoritmos de aprendizaje o en sus *n* características conceptuales. La división más genérica distingue entre aprendizaje supervisado y no supervisado.

Una clasificación mas amplia de aprendizaje puede estar constituidas de cuatro reglas básicas de aprendizaje que son: aprendizaje por corrección del error, aprendizaje hebbiano, aprendizaje competitivo y aprendizaje de Boltzmann; junto con tres esquemas fundamentales que generan esas reglas de aprendizaje: aprendizaje supervisado, aprendizaje reforzado y aprendizaje auto-organizativo o no supervisado. Cada regla, por tanto, tendrá unas ventajas específicas respecto las otras, dependiendo entre otros factores, de la aplicación.

- **Aprendizaje por Corrección del Error**

En principio, la señal proporcionada por una neurona de salida es diferente de la respuesta deseada para esa neurona por lo que es posible definir una señal de error. El propósito de este tipo de aprendizaje consiste en minimizar una función de error o coste basada en ese error cometido. Un criterio muy usado es el error cuadrático medio. La corrección de los pesos con ese fin es proporcional a la señal de error y a la de entrada.

- **Aprendizaje de Hebb o Hebbiano.**

Aquí el ajuste de los pesos sinápticos será función de las actividades pre-sinápticas y post-sinápticas, es decir de la entrada y salida de la neurona. Como la definición es bastante amplia, existen muchos modelos para esta regla.

- **Aprendizaje de Boltzmann**

En una máquina de Boltzmann, las neuronas constituyen una estructura recurrente y operan de forma binaria esto es, +1/-1 son estados on/off. Además se caracteriza por una función de energía E que está definida por los estados ocupados por cada neurona en la máquina. La máquina funciona de forma que se elige una neurona aleatoriamente y se le cambia de estado a una temperatura T (se trata de una analogía de una temperatura física) con una probabilidad determinada. Si esta regla se aplica sucesivamente la máquina alcanzará un equilibrio térmico.

- **Aprendizaje Competitivo.**

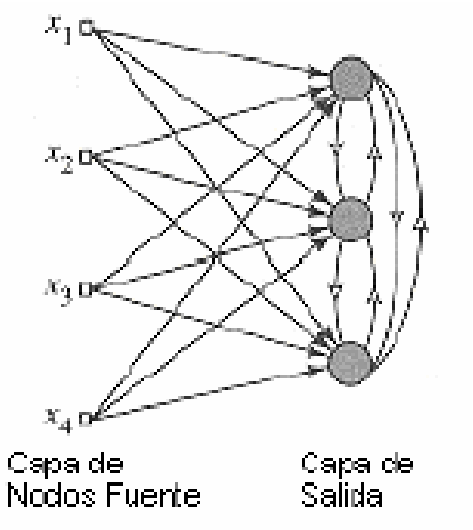
Hay tres elementos fundamentales en este tipo de aprendizaje:

1. Un conjunto de neuronas idénticas excepto por que existen algunas conexiones aleatoriamente distribuidas que responden de forma diferente a un conjunto de entradas.

2. Un límite impuesto a los pesos relacionados con cada neurona.

3. Un mecanismo que permite a las neuronas competir por el derecho a responder a unas entradas, de forma que sólo una neurona, o una por grupo activo, podrá hacerlo. Una RNA de este tipo puede tener conexiones laterales con otras neuronas actuando de inhibitorias y el resto de neuronas de la red serán excitadoras (Figura 21).

Figura 21. Red de Aprendizaje Competitivo.



4.3.3 Esquemas de aprendizaje. Las RNAs pueden ser clasificadas atendiendo a su esquema conceptual en tres bloques: las RNAs de pesos fijados, las supervisadas y las no supervisadas.

Las RNAs de pesos fijos no cuentan con una regla de aprendizaje por la cual, a través de un proceso iterativo, los pesos de la red sean ajustados por lo que un modelo podrá definirse de partida como supervisado o no supervisado. En cambio otros autores incluyen en la clasificación de los esquemas de aprendizaje las RNAs de aprendizaje reforzado, si bien estas podrían agruparse junto a las supervisadas. La distinción se apoya en que los sistemas supervisados se definen en términos de objetivos o respuestas deseadas que son empleadas directamente en el cálculo de unas determinadas funciones de error a minimizar, mientras que las de aprendizaje reforzado se basan en la asignación de un premio o un castigo según la actuación, sin tener en cuenta en realidad el valor de la señal deseada. Es pues, una sutil distinción entre aprendizaje instructivo y evaluativo, entre identificación y control o entre explotación y exploración.

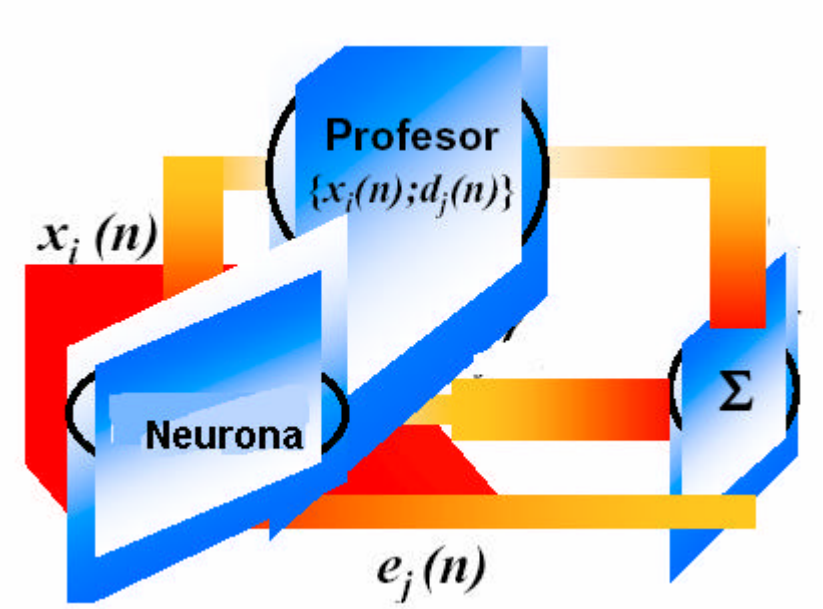
Tabla 4. Clasificación de las RNAs según Esquema Conceptual

Clasificación	Estructuras características
Pesos fijados	Red de Hamming, de optimización combinacional
No supervisadas	Neocognitrón, Aprendizaje competitivo, Hebbiano, ART
Supervisadas	Perceptrón, MLP, DBNNs, Modelo de Markov

- **Aprendizaje Supervisado**

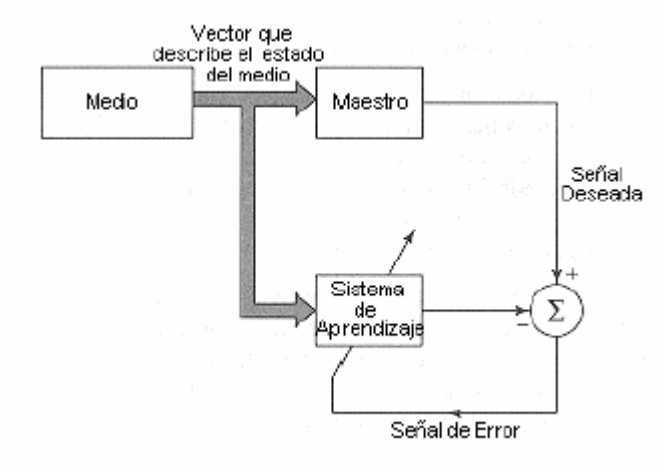
También se llama aprendizaje activo o formulación basada en la aproximación, y se caracteriza primordialmente por disponer de un maestro capaz de proveer a la RNA de una salida deseada con el fin de calcular una señal de error que sirva a la red para emular al maestro (Ver Figura 22)

Figura 22. Aprendizaje supervisado



En la figura 23 se muestra el diagrama de bloques de un sistema supervisado donde se muestran los elementos que intervienen es este tipo de aprendizaje: medio, el maestro y el sistema de aprendizaje.

Figura 23. Diagrama de bloques del Aprendizaje Supervisado.



- **Aprendizaje Reforzado**

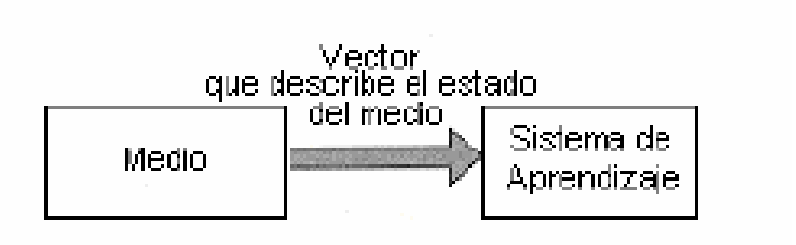
También se denominan de formulación basada en la competición, refiriéndose al hecho de que el aprendizaje se realizará asignando nodos ganadores y perdedores dependiendo de los resultados obtenidos. Se basa en un mapeo de las señales de entrada-salida por medio de un proceso de prueba y error diseñado para maximizar un índice de actuación o éxito llamado señal de refuerzo.

- **Aprendizaje Auto-Organizado o No Supervisado**

En este tipo de aprendizaje la red puede considerarse autónoma, determinando características generales de los datos presentados y aprendiendo a reflejar esas propiedades en las salidas correspondientes. Lo que en realidad son estas propiedades, y que la red puede aprender a reconocer, dependerá del

modelo neuronal concreto así como del método de aprendizaje utilizado (Figura 24).

Figura 24. Diagrama de bloques del Aprendizaje No Supervisado.

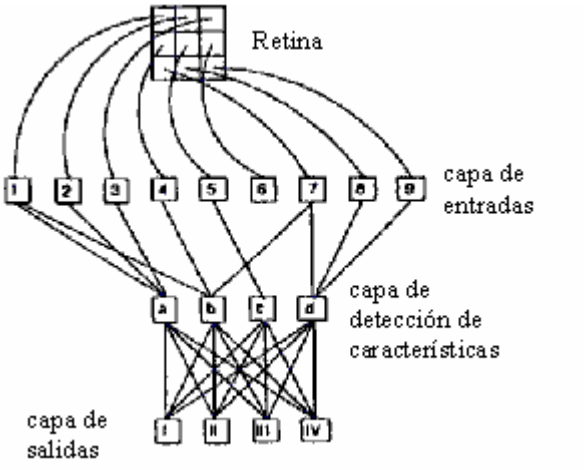


4.4 MODELOS DE REDES NEURONALES.

- **Modelo del Perceptrón**

Este modelo de red simple, seria un modelo *reducido* del modelo del Perceptrón, desarrollado por *Rosenblatt* entre 1958 y 1962, a partir de los modelos de red de *McCullough-Pitts*. En el *modelo* del Perceptrón (figura 25) los *detectores* están conectados con neuronas de la *capa de entrada*; estas neuronas se activan (*1*) cuando se activa el detector correspondiente. Cada neurona de la capa de entrada está conectada con diferentes neuronas de la *capa de detección de características*. Y cada neurona de esta capa estaría conectada a su vez con diferentes neuronas de la *capa de salidas* del Perceptrón (Ver figura 25).

Figura 25. Esquema de un modelo Pérceptron



La regla de aprendizaje usada para entrenar la red es una versión simplificada de la regla de aprendizaje del Perceptrón.

El modelo simple de red neuronal (al igual que el modelo del Perceptrón en el que se basa), presenta bastantes limitaciones en las tareas que pueden llegar a aprender. Así, por ejemplo, el modelo seria incapaz de aprender a realizar la operación *XOR* (*O* exclusivo): no puede ser entrenado con éxito para que la neurona 3 se active si las neuronas 1 *o* 2 están activas, pero *no* las dos a la vez.

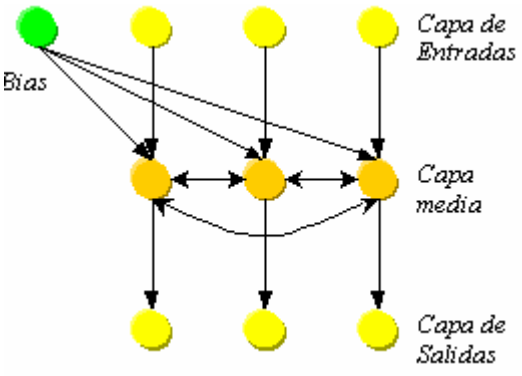
Para realizar este tipo de tareas "complejas" es preciso una red neuronal que contenga más de una capa de pesos sinápticos ajustables. Para ello, se añaden *capas ocultas* de neuronas entre la capa de entradas y la capa de salidas.

- **Redes de Hopfield**

Estas redes son bastante parecidas al modelo del Perceptrón, pero presentan una característica adicional: las neuronas en la capa media, presentan conexiones de salida hacia otras neuronas de la capa media.

Además, cada neurona de la capa de entradas esta conectada con una neurona de la capa media, y cada neurona de la capa media emite una sola conexión hacia la capa de salidas. Y estas conexiones (capa de entradas - capa media, y capa media - capa de salidas) *no* implican *calculo* de pesos sinápticos ni de valores umbral.

Figura 26. Red autoasociativa de Hopfield



En la figura anterior se observa una Red de Hopfield formada por: 3 neuronas de entrada (1, 2 y 3), 3 neuronas en la capa media (4, 5 y 6), 3 neuronas en la capa de salida (7, 8 y 9) y una neurona Bias (0).

El hecho de que todas las neuronas de la capa media se encuentren interconectadas, hace que en esta capa se dé un feedback o retroalimentación entre sus neuronas, de forma que al activarse una neurona de esta capa hace que las otras neuronas cambien su estado de activación, que a la vez harán cambiar el suyo propio. Esta nueva característica de las redes de Hopfield hace que funcionen de manera diferente al Perceptrón. Así, en el Perceptrón todas las neuronas de una misma capa transmiten el *patrón de activación inmediatamente* hacia las neuronas de la siguiente capa. (El *patrón de activación* seria un *vector* formado por los *valores* de las neuronas de una capa; ejemplo: (0, 1, 0, 1, 1)). Mientras que en una red de Hopfield las neuronas de la *capa de entradas* si transmiten *inmediatamente* su *patrón de activación* hacia las neuronas de la capa media (y además lo hacen sin variación debida a pesos sinápticos,...), pero las neuronas de la *capa media no* transmitirán ningún patrón de activación hasta que hayan llegado a un *estado de equilibrio*, en el cual el *patrón de activación* de la capa media se mantiene *estable.*

En una red de Hopfield sencilla (como la de la figura 26), cuando se introduce un dato en la *capa de entradas*, este es transmitido *sin variación* hacia la capa media. Una vez en la *capa media*, las neuronas que la forman modificaran su estado en función del estado de activación de las otras neuronas de la capa. Pero para esto, es preciso que las neuronas de la capa media *no* dejen de estar *activas* después de transmitir su estado a las otras neuronas (como sí sucedía en el modelo del Perceptrón). Además, las neuronas de esta capa

media *actualizan* su estado de manera *aleatoria*: la neurona a la que le toca actualizarse es elegida al *azar*. De esta manera primero se actualizara una neurona elegida al azar, luego otra, también elegida al azar hasta que se alcance un equilibrio. Cuando se llega al *equilibrio*, los *estados* de las neuronas de la capa media ya *no* se modifican; se mantienen *estables*. Y es entonces cuando la capa media transmite su patrón de activación a la *capa de salidas*, que lo recibe sin modificación alguna.

- **Back-propagation**

El método de *back-propagation* (o *entrenamiento hacia atrás*) es un sistema automático de *entrenamiento* de redes neuronales con *capas ocultas*, perfeccionado en la década de los 80. En este tipo de redes, el *problema* a la hora de *entrenarlas* estriba en que sólo conocemos la *salida* de la red y la *entrada*, de forma que no se pueden ajustar los pesos sinápticos asociados a las neuronas de las capas ocultas, ya que no podemos inferir a partir del estado de la capa de salida como tiene que ser el estado de las capas ocultas.

El sistema de entrenamiento mediante back-propagation consiste en:

- Empezar con unos pesos sinápticos cualquiera (generalmente elegidos al azar).
- Introducir unos datos de entrada (en la capa de entradas) elegidos al azar entre los datos de entrada que se van a usar para el entrenamiento.

- Dejar que la red genere un vector de datos de salida (propagación hacia delante).
- Comparar la salida generada por al red con la salida deseada.
- La diferencia obtenida entre la salida generada y la deseada (denominada *error*) se usa para ajustar los pesos sinápticos de las neuronas de la capa de salidas.
- El error se *propaga hacia atrás* (back-propagation), hacia la capa de neuronas anterior, y se usa para ajustar los pesos sinápticos en esta capa.
- Se continua propagando el error hacia atrás y ajustando los pesos hasta que se alcance la capa de entradas.

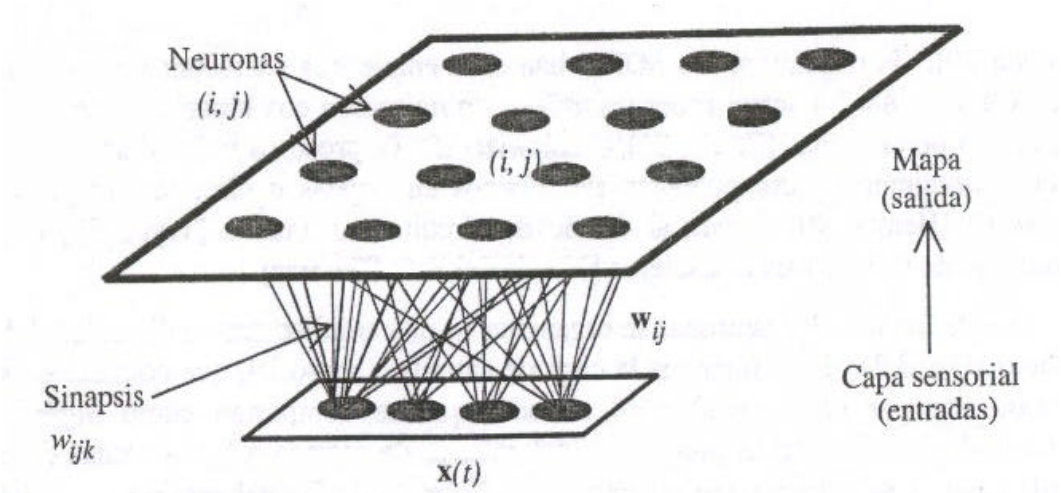
Este proceso se repetirá con los diferentes datos de entrenamiento.

- **SOM**

En este tipo de redes el entrenamiento o aprendizaje es diferente al de las redes con entrenamiento supervisado. A la red no se le suministra junto a los patrones de entrenamiento, una salida deseada. Lo que hará la red es encontrar regularidades o clases en los datos de entrada, y modificar sus pesos para ser capaz de reconocer estas regularidades o clases.

Uno de los tipos de redes que pertenece a esta familia y que se ha usado bastante son los mapas autoorganizados, SOM (Self-Organizing Maps). La arquitectura típica de este tipo de mapas es la siguiente:

Figura 27. Arquitectura típica de un mapa SOM



Como se puede apreciar en la figura anterior, es una red de tipo unidireccional. La red se organiza en dos capas, siendo la primera capa la formada por las neuronas de entrada. La segunda capa consiste en un array de neuronas de dos dimensiones. Como se necesitan dos índices para etiquetar cada neurona, los pesos sinápticos asociados a cada neurona tendrán tres índices (i,j,k) donde (i,j) indican la posición de la neurona en la capa y k, la componente o conexión con cierta neurona de entrada.

En cuanto al entrenamiento, este es un ejemplo de red que utiliza un aprendizaje de tipo no supervisado. Además, cada neurona utiliza como regla de propagación una distancia de su vector de pesos sinápticos al patrón de entrada.

A continuación se presentan los modelos de Redes Neuronales más importantes, con una breve información sobre cada modelo:

Tabla 5. Resumen de los diferentes tipos de redes neuronales

Nombre de la red	Año	Aplicaciones más importantes	Comentarios	Limitaciones
Avalancha	1967	Reconocimiento de habla contínua. Control brazos robot.	Ninguna red sencilla puede hacer todo esto.	No es fácil alterar la velocidad o interpolar el movimiento.
ADALINE/ MADALINE	1960	Filtrado de señales. Ecualizador adaptativo. Modems.	Rápida, fácil de implementar con circuitos analógicos o VLSI.	Sólo es posible clasificar espacios linealmente separados.
Back Propagation	1974-85	Síntesis de voz desde texto. Control de robots. Predicción. Reconocimiento de patrones.	Red más popular. Numerosas aplicaciones con éxito. Facilidad de aprendizaje. Potente.	Necesita mucho tiempo para el aprendizaje y muchos ejemplos.
Memoria Asociativa Bidireccional	1985	Memoria heteroasociativa de acceso por contenido.	Aprendizaje y arquitectura simples.	Baja capacidad de almacenamiento. Los datos deben ser codificados.
Máquinas de Boltzmann y Cauchy	1985-86	Reconocimiento de patrones (imágenes, sonar y radar). Optimización.	Redes simples. Capacidad de representación óptima de patrones.	La máquina de Boltzmann necesita un tiempo muy largo de aprendizaje.
Counter-propagation	1986	Comprensión de imágenes.	Combinación de Perceptron y TPM	Numerosas neuronas y conexiones.
Hopfield	1982	Reconstrucción de patrones y optimización.	Puede implementarse en VLSI. Fácil de conceptualizar.	Capacidad y estabilidad.
Perceptrón	1957	Reconocimiento de caracteres impresos.	La red más antigua. Construida en HW.	No puede reconocer caracteres complejos.
SOM	1980-84	Reconocimiento de patrones, codificación de datos, optimización.	Realiza mapas de características comunes de los datos aprendidos.	Requiere mucho entrenamiento.

4.5 RECONOCIMIENTO DE PATRONES UTILIZANDO RNAs

El proceso de reconocimiento de patrones tiene que ver con la actividad de identificar un patrón en alguna clase determinada (clasificación supervisada) o asignar un patrón a una clase no definida (clasificación no supervisada, agrupamiento o clustering), teniendo en cuenta las particularidades del patrón que son comunes a los miembros de una misma clase. Un patrón puede definirse como una entidad a la que se le puede dar un nombre y que está representada por un conjunto de propiedades medidas y las relaciones entre ellas (vector de características). Por ejemplo, un patrón puede ser una señal sonora y su vector de características el conjunto de coeficientes espectrales extraídos de ella (espectrograma). Otro ejemplo podría ser una imagen de la huella dactilar de un dedo de la cual se extrae el vector de características formado por un conjunto de valores numéricos calculados a partir de la misma. El reconocimiento automático, descripción, clasificación y agrupamiento de patrones son actividades importantes en una gran variedad de disciplinas científicas, como biología, sicología, medicina, inteligencia artificial, etc. Es decir, que el reconocimiento de patrones consiste en la categorización de datos de entrada en clases identificadas, por medio de la extracción de características significativas o atributos de los datos extraídos de un medio ambiente que contiene detalles irrelevantes. Matemáticamente hablando, la clasificación consiste en la partición del espacio n-dimensional definido por las características de un objeto, en varias regiones, donde cada región

corresponde a una clase. Se denomina clase a la categoría determinada por algunos atributos comunes a sus miembros, los cuales representan los patrones. Las características de un patrón se representan en un vector de características que puede estar formado por números binarios o valores reales.

4.5.1 Fases del diseño de un sistema reconocedor de patrones. El diseño de un sistema de reconocimiento de patrones se desarrolla normalmente en 3 fases fundamentales que son:

- La representación de los datos de entrada, realizada por un transductor
- La extracción de características, donde extraen los datos entregados por el transductor a una matriz que pueda procesar la red neuronal.
- La determinación del proceso de decisión óptimo y estimación de parámetros, realizado por el reconocedor.

El dominio del problema, gobierna la elección de las diferentes alternativas en cada paso: tipos de sensores, técnicas de preprocesamiento, modelo de toma de decisiones etc.

- **Transductor**

En esta etapa se toma información del patrón y la transforma a señales analógicas, que a su vez son convertidas a su forma digital. En la mayoría de

los sistemas los esquemas de representación de patrones son desarrollados por los diseñadores.

La RNA lleva a cabo, en esencia, el proceso de clasificación. Sin embargo, las redes neuronales tienen la propiedad de construir una representación interna de los patrones (extracción de características), aunque difícilmente visible. Por esta razón, algunos investigadores alimentan a la red con los datos en bruto (o con un preproceso mínimo, como normalización) y esperan que la propia red extraiga (aprenda) una representación a partir de ellos. En cualquier caso, una representación adecuada de los datos facilita el proceso de toma de decisión y mejora las tasas de generalización. Sin embargo, el diseño de una buena representación exige un conocimiento profundo de la naturaleza del problema, lo cual no siempre es posible.

Una buena representación de patrones debe cumplir, al menos, los siguientes requisitos:

- Tasa de compresión de datos alta.
- Buena capacidad discriminatoria.
- Invariancia frente a transformaciones de los datos.
- Robustez frente al ruido.

- **Extractor de características**

Mide propiedades importantes que representan al objeto. Su propósito es reducir la cantidad de datos obtenidos del transductor sin perder información esencial. El resultado de tales medidas se llama vector de características. Por un lado, se le extrae algunas medidas numéricas de los datos en bruto de los patrones (representación inicial). Por otro lado, forma un conjunto de características (de dimensión n) partiendo de los datos de entrada (de dimensión m>n).

Esta es, en la mayoría de los casos, la etapa más compleja e importante en el diseño de un reconocedor de patrones, ya que de la extracción de las características relevantes del elemento que se desea reconocer depende la efectividad del reconocimiento de la red neuronal.

Un ejemplo claro se da en un sistema de reconocimiento de figuras, donde el transductor es una cámara digital, se requiere de un robusto preprocesamiento que incluye, filtrado de ruido, ajuste de histograma de intensidades, selección de contorno, detección de bordes, etc y finalmente un algoritmo que permita convertir la matriz de la imagen resultante en un vector con características únicas y representativas de la imagen extraída.

- **Reconocedor**

Esta es la etapa final del diseño de un sistema de reconocimiento de patrones, ya que la salida de la red neuronal determina la clasificación del elemento que le fue introducido (imagen de un rostro, huella digital, patrones de voz) y a pesar de que existen ciertas técnicas para la escogencia de la arquitectura de la red a trabajar y el algoritmo de entrenamiento, estos dependen en gran medida de la aplicación a trabajar.

Las principales características que determinan la efectividad de reconocimiento de la red neuronal se mencionan a continuación:

Set de entrenamiento: Debe ser un set significativo, con características representativas de todos los elementos. Nos se debe exceder en el numero de muestras porque se puede incurrir en el error de memorizar la red neuronal impidiendo su capacidad de generalizar y extrapolar algunos datos, ni trabajar con un set muy reducido porque la red incurriría en una alta generalización y le impediría diferenciar elementos.

Arquitectura de la red neuronal: El numero de neuronas de la capa de entrada esta directamente relacionada con el tamaño de la matriz de salida en la etapa de preprocesamiento, las capas ocultas y el numero de neuronas en ellas depende netamente de los criterios del diseñador, y por ultimo la capa de salida

corresponde al numero de elementos entre los cuales la red neuronal debe diferenciar.

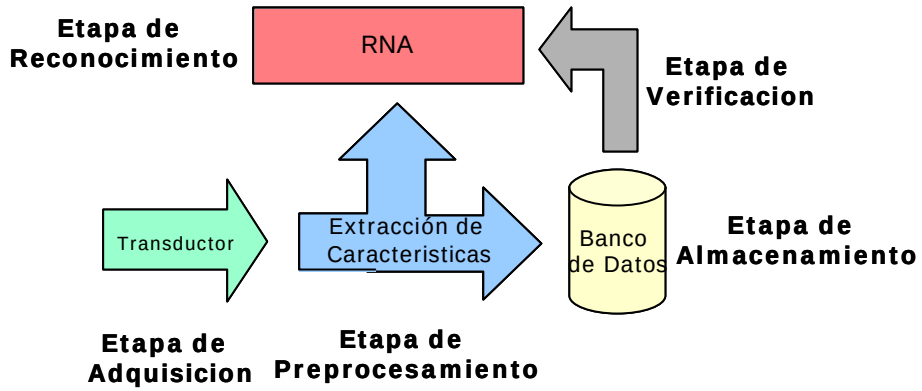
Algoritmo de entrenamiento: Existen decenas de algoritmos de entrenamiento que se han desarrollado a lo largo de los últimos años, y la escogencia del mismo depende exclusivamente de la aplicación que se va a trabajar. Esta determina la velocidad de convergencia que se requiere y el comportamiento que se requiere de la misma.

5. SISTEMA DE CONTROL DE ACCESO A RECINTOS USANDO EL RECONOCIMIENTO NEURONAL DE LA HUELLA DACTILAR

Se propone un sistema de control de acceso a recintos haciendo uso de un sistema de autentificación biométrica de huella dactilar (AFAS), que permita habilitar o negar la entrada a un determinado lugar dependiendo de la persona que haga la solicitud.

Se escoge un AFAS (Automatic Fingerprint Authentification System), puesto que este tipo de sistemas permite complementar el control de acceso con un sistema de contraseña adjunto. En un sistema AFAS las entidades (generalmente dos) que participan en la autenticación acuerdan una clave, la cual debe mantenerse en secreto. Cuando una persona desee ser reconocido por el sistema, debe teclear su clave y luego suministrar al sistema la imagen de su huella dactilar, a través del scanner biométrico para que este autentifique que puede acceder o no a lugar restringido.

Figura 28. Diagrama de bloques del sistema de control de acceso



En la Figura 28 se muestra el diagrama de bloques del sistema de control de acceso que se propone. Es un sistema de control que utiliza el reconocimiento de la huella dactilar en conjunto con un sistema mediante clave (AFAS). La persona debe digitar un número personal y luego el equipo pedirá automáticamente colocar el dedo en el sensor de huella dactilar. Luego estas señales se someten a un procesamiento digital para ser comparadas con las de la base de datos. Si la persona es reconocida, ósea la huella coincide con alguna registrada, el equipo dispara un relay, que puede estar conectado a una puerta, barrera, portón, etc. En ese mismo momento registra la fecha, la hora y el número de identificación de la persona que ingreso. El sistema también guardara los datos de los rechazos, por no conocer la huella dactilar.

La base de datos debe ser almacenada en un computador con suficiente capacidad de memoria que permita almacenar una gran cantidad de usuarios y

que además responda con rapidez a la búsqueda que se hace inicialmente con la clave del usuario.

- **ETAPA DE ADQUISICION**

Se realizó la selección de un scanner de huellas digitales tomando en cuenta las siguientes características:

- ❖ Desempeño
- ❖ Aceptabilidad
- ❖ Fiabilidad
- ❖ Soporte de software (compatibilidad)
- ❖ Interfase de datos
- ❖ Requerimientos de hardware
- ❖ Precio

Con base en las características anteriormente mencionadas se selecciono el scanner óptico *U are U 4000 Module* debido a que es un dispositivo diseñado especialmente para desarrollo de aplicaciones.

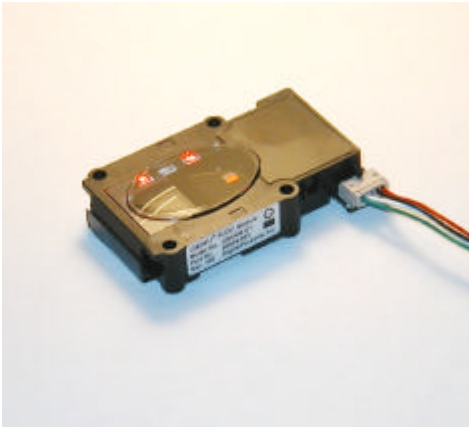
Las especificaciones del dispositivo son las siguientes:

Tabla 6. Especificaciones del sensor seleccionado

Característica	Especificaciones
Tipo de Sensor:	Óptico
Resolución:	512 dpi
Área de Captura de Imagen:	14.1mm x 18.1mm
Interfase de datos	Estándares USB 1, 1.1, 2.0
Niveles de intensidad	256 niveles de gris (8 bits)
Precio:	$95 USD

Adicionalmente el dispositivo es compatible con herramientas de desarrollo como VeriFinger SDK (Software Development Kit), FX3 SDK y MATLAB. Todas las anteriores herramientas altamente difundidas en el mercado para el desarrollo de aplicaciones de identificación y reconocimiento de huellas dactilares.

Figura 29. Módulo U are U 4000



El modulo se encuentra aislado del polvo y posee características de montaje que permite su fácil integración en cualquier sistema físico de control de acceso.

Como se planteo en el diseño del sistema de control de acceso, este será un sistema de verificación, en lugar de uno de identificación, por ende el sistema debe recibir información preliminar sobre a quien pertenece la huella dactilar, para hacer la respectiva comprobación. Esta información será introducida en forma de un número de identificación personal (PIN) a través de un teclado numérico.

La selección del teclado numérico se hizo tomando en cuenta su robustez, durabilidad y protección contra el medio ambiente.

El teclado seleccionado es el KP-10 de la empresa Northern Computers INC y posee las siguientes características:

Tabla 7. Características del teclado seleccionado

Característica	**Especificaciones**
Protección contra el medio	Construcción en acero inoxidable Superficie impermeable Protección contra impactos
Tamaño	13.018 cm x 8.57 cm
Interfase de datos	Matriz de salida de 2 x 7
Precio:	$50 USD

5.2 ETAPA DE EXTRACCIÓN DE CARACTERÍSTICAS

Cuando las huellas dactilares son adquiridas por el scanner, son convertidas a un formato de imagen compatible con el software que estamos empleando para

su procesamiento, sin embargo en muchos de los casos las condiciones de la imagen no son las optimas para la extracción de sus características (minucias), es necesario un proceso previo de restauración y ajuste de la imagen.

Los procedimientos de preprocesamiento en el ajuste de la imagen se muestran a continuación:

5.2.1 Ecualización del Histograma. Las transformaciones de las escalas de grises pueden incrementar significativamente la visibilidad de una imagen, el problema es que requiere de un gran trabajo de ensayo y error. La ecualización del histograma es una manera de automatizar el procedimiento La ecualización del histograma usa el propio histograma como la curva de ajuste de contraste, eliminando así la supervisión humana, de esta forma, la transformación de la salida se obtiene mediante la integración y la normalización del histograma, en lugar de una curva generada manualmente. Como resultado, obtenemos un alto contraste en aquellos valores que tienen mayor número de píxeles.

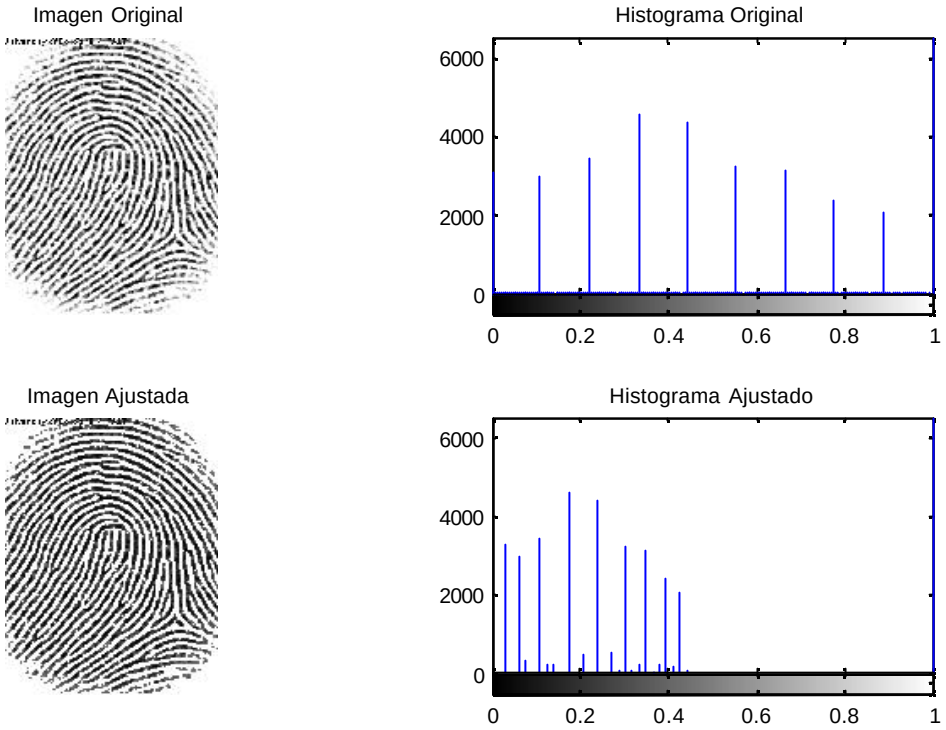
En las imágenes que se muestran a continuación se aprecia la mejora en la imagen al realizar una ecualización automática del histograma de intensidades.

En MATLAB este procedimiento es llevado a cabo con el comando *histeq* del toolbox de procesamiento de imágenes. Los comandos utilizados fueron los siguientes:

```
%Adquisicion de la Imagen
[X,MAP]=bmpread('dedo');
X2=ind2gray(X,MAP);
subplot(2,2,1)
imshow(X2)
title('Imagen Original')
subplot(2,2,2)
imhist(X2)
title('Histograma Original')

% Ajuste del Histograma
X3=histeq(X2)
subplot(2,2,3)
imshow(X3)
title('Imagen Ajustada')
subplot(2,2,4)
imhist(X3)
title('Histograma Ajustado'
```

Figura 30. Ajuste del Histograma de la imagen



5.2.2. Transformada de Fourier. Se divide la imagen en bloques de 32x32 y se aplica la transformada rápida de fourier, posteriormente se aplica la transformada inversa a la convolución de la transformada con su magnitud elevada a un factor n. En MATLAB este proceso es llevado a cabo empleando los comandos fft2, conv y ifft2 del Toolbox de procesamiento de señales.

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:

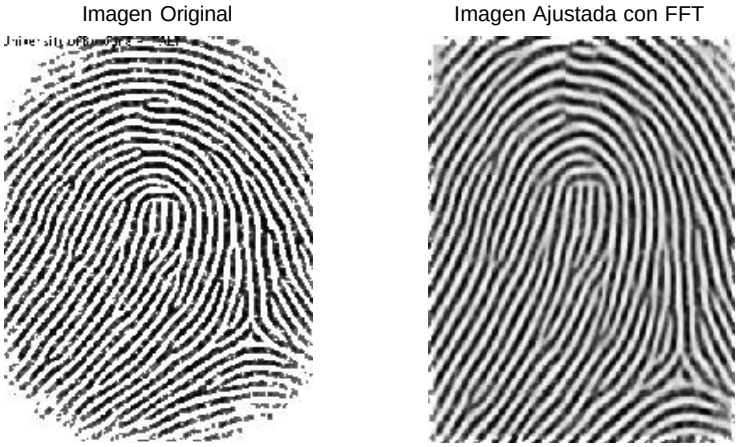
$$g(x,y) = F^{-1}\left\{F(u,v)x\left|F(u,v)\right|^{k}\right\} \quad (2)$$

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

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

Los resultados se visualizan en las imágenes que se muestran a continuación.

Figura 31. Mejora de imágenes usando la transformada FFT



5.2.3 Umbralización y Segmentación. Posterior a las mejoras realizadas procedemos a extraer solo la información que nos interesa, para ello realizamos la umbralización de la imagen (conversión a color blanco y negro) eliminando así las sombreas y otros factores que pueden dificultar el proceso de extracción de características.

En MATLAB este procedimiento se lleva a cabo empleando los comandos graythresh e im2bw.

Los resultados obtenidos se muestran a continuación:

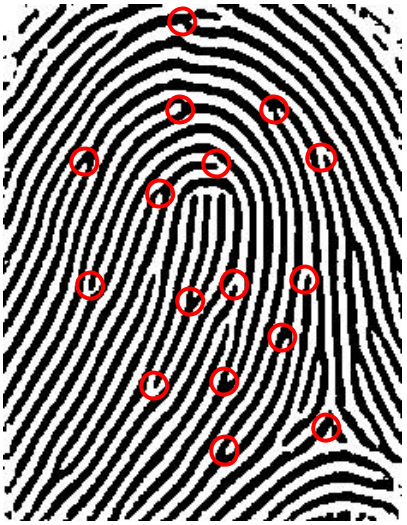
Figura 32. Imagen Umbralizada

Figura 33. Imagen Segmentada

5.2.4 Extracción de Patrones. Los patrones (minucias) son extraídas de una huella dactilar usando un algoritmo de extracción de minucias. Cada patrón es caracterizado por su ubicación y la orientación en el surco en el cual reside. El

algoritmo que se ha escogido para el presente diseño recibe el nombre de transformada de Hough.

Figura 34. Extracción de características a partir de la plantilla de minucias



La transformada de Hough es una técnica utilizada para aislar características de forma particular dentro de una imagen. La idea básica es encontrar curvas que puedan ser parametrizadas como líneas rectas, polinomios y círculos. Se puede analíticamente describir un segmento de línea en varias formas. Sin embargo una ecuación conveniente para describir un conjunto de líneas es la notación paramétrica o normal:

$$\rho = x\cos\theta + y\sin\theta$$

Donde ρ es la longitud de una normal desde el origen hasta la línea y θ es el ángulo de ρ con respecto al eje x.

Para realizar la comparación entre plantillas de minucias, el algoritmo realiza 2 principales procedimientos:

Computa los parámetros de transformación *dx, dy, dh* y *s*, donde *dx* y *dy* son traslaciones a lo largo de los ejes *x* y *y*, respectivamente, h es el ángulo de rotación, y *s* es el factor de escala.

Alinea los 2 sets de puntos de minucias con los parámetros estimados y cuenta los pares que concuerdan.

5.3 ETAPA DE RECONOCIMIENTO

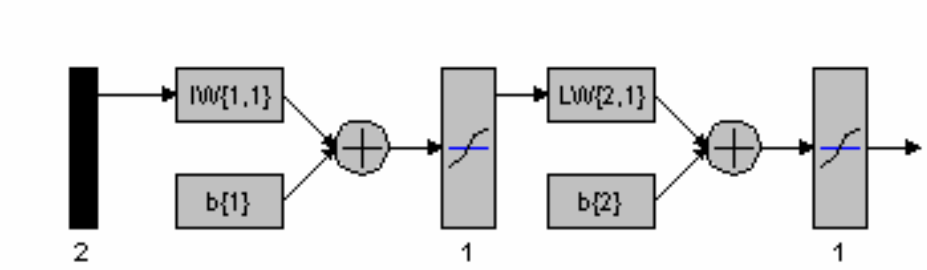
Con base en las experiencias obtenidas en anteriores proyectos realizados en la CUTB en reconocimiento de patrones, el tipo de red neuronal seleccionada es de tipo FeedForward Backpropagation, debido a su robustez, flexibilidad, y facilidad de aprendizaje.

5.3.1 Número de Capas. En la capa de entrada se tienen el número de neuronas equivalentes al tamaño de la matriz de salida del algoritmo de extracción de minucias.

En la capa oculta se tiene 1 capa con un total de 75% de las neuronas empleadas en la capa de entrada

En la capa de salida solo se tiene una neurona que se activara en caso de que la huella presentada y la almacenada concuerden.

Figura 35. Arquitectura de la red neuronal

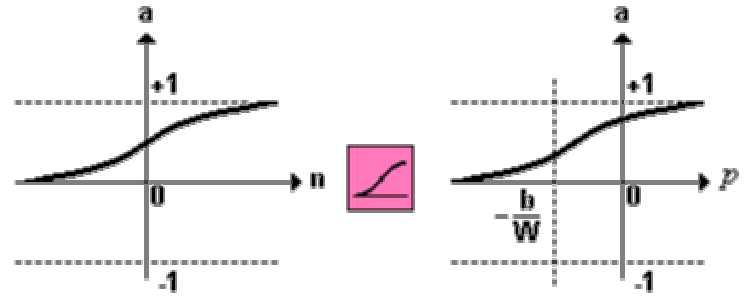


5.3.2 Función de Activación. Para todas las capas, la función de activación será de tipo *Logsig,* esta función toma los valores de entrada, los cuales pueden oscilar entre +/- infinito, y restringe la salida a valores entre cero y uno, de acuerdo a la expresión

$$a = \frac{1}{1+e^{-n}}$$

Esta función es comúnmente empleada en redes multicapas, como la Backpropagation, en parte porque la función logsig es diferenciable.

Figura 36. Función de transferencia sigmoidal



a= *logsig* (n)

Función de Transferencia Logaritmica Sigmoidal

a=*logsig*(Wp+b)

Entrada a una Neurona Logaritmica Sigmoidal

5.3.3 Función de Entrenamiento. Se emplea el algoritmo de entrenamiento Levenberg Marquardt, éste algoritmo es una modificación del método de Newton, el que fue diseñado para minimizar funciones que sean la suma de los cuadrados de otras funciones no lineales; es por ello que el algoritmo de Levenberg - Marquardt, tiene un excelente desempeño en el entrenamiento de redes neuronales donde el rendimiento de la red esté determinado por el error medio cuadrático.

Es el algoritmo más rápido para redes Backpropagation; tiene la desventaja de requerir de un set de entrenamiento lo más estándar posible, pues de otra forma solo aproximará correctamente valores que se encuentren dentro de los patrones de aprendizaje.

Esta función se implementa en MATLAB mediante el comando trainlm del Toolbox de Redes Neuronales Artificiales.

5.3.4 Función de Aprendizaje. La función de aprendizaje de pesos y bias que se va a emplear es la de gradiente descendiente con momento, ésta calcula los cambios en los pesos para una neurona dada con base en su entrada P y el

error E, el peso (o bias) W, la tasa de aprendizaje LR y la constante de momento MC, conforme la ecuación de gradiente descendiente con momento:

$$dW = MC * dW_{prev} + (1 - MC) * LR * gw$$

El cambio de peso anterior dW_{prev} es almacenado y leído desde el estado de aprendizaje LS.

Esta función se implementa en MATLAB mediante el comando Learngdm del Toolbox de Redes Neuronales Artificiales.

5.3.5 Función de desempeño. La función de desempeño que será empleada es la función MSE, esta mide el desempeño de la red acorde con la media de los errores cuadrados. La función toma de uno a tres argumentos, E – matriz o arreglo de vectores de error. X – Vector de los valores de todos los pesos y los bias. PP – Parámetros de rendimiento. Y entrega el error cuadrado medio.

5.4 ETAPA DE ALMACENAMIENTO DE DATOS

El punto de partida para realizar un sistema de control de acceso utilizando el reconocimiento de personas a través de la huella dactilar es crear una base de datos de parámetros biométricos, en este caso la huella dactilar que servirá como base para el resto del proyecto.

Por ser nuestro diseño en su fase inicial con propósitos académicos, la base de datos se maneja directamente en el programa de reconocimiento, en este caso

MATLAB y tanto los patrones biométricos como las características de las redes neuronales son almacenados en forma de variables en el mismo.

Para cada individuo se requiere de 25 muestras de huellas dactilares (5 por cada dedo) y 5 configuraciones de red neuronal (1 para cada dedo), de esta forma el cuando la persona introduce su PIN, MATLAB carga la configuración del individuo y realiza la respectiva comparación de la huella que esta siendo presentada con los parámetros que tiene almacenados.

5.5 ETAPA DE CONTROL

Para el control del acceso se seleccionó un contactor que se activará cuando la salida de la red neuronal sea positiva, es decir reconozca la huella dactilar que ha sido ingresada al sistema. Las especificaciones del contactor son las siguientes:

Tabla 8. Características del contactor seleccionado

Marca	Características	Precio
Multilin General Electric	2 entradas digitales, 2 salidas digitales, 1 salida análoga. Puerto COM 1 y Com 2	$80 USD

5.6 LISTA DE EQUIPOS

La lista final del los equipos seleccionados es la siguiente:

Tabla 9. Lista de equipos

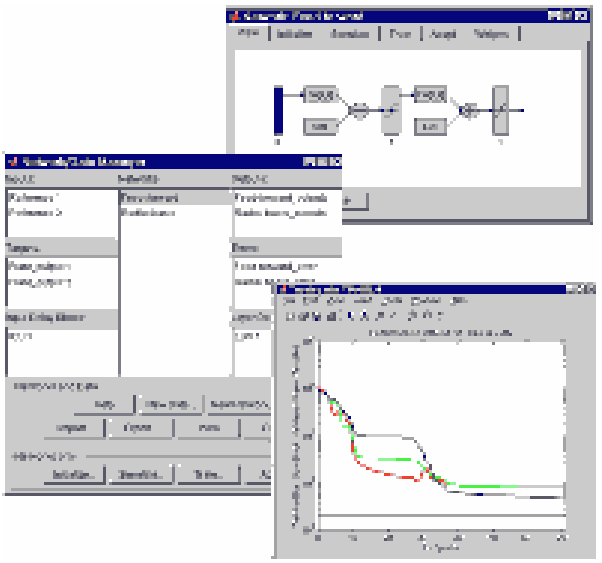
EQUIPO	NOMBRE	PRECIO
SENSOR BIOMÉTRICO	*U are U 4000 Module*	*$95 USD*
TECLADO	*KP –10*	*$45 USD*
COMPUTADOR	*Pentium 4*	*$1300 USD*
CONTACTOR	*Telemecanique*	*$80 USD*

ANEXOS

Anexo A. GUI de Neural Network Toolbox

Esta herramienta le permite importar conjuntos de datos potencialmente grandes y complejos. La GUI también le permite crear, inicializar, entrenar, simular y gestionar sus redes. Las representaciones gráficas sencillas le permiten visualizar y entender la arquitectura de la red.

Figura a. *Esta ventana muestra porciones de la GUI de una red neuronal. Los diálogos y los paneles le permiten visualizar su red (arriba), evaluar los resultados del entrenamiento (abajo) y gestionar sus redes (centro).*



Arquitecturas de red soportadas

Redes supervisadas

Las redes neuronales supervisadas se entrenan para producir los resultados deseados como respuesta a la entrada de ejemplos, lo que las hace especialmente adecuadas para modelizar y controlar sistemas dinámicos, clasificar datos ruidosos y predecir acontecimientos futuros. Neural Network Toolbox es compatible con las siguientes redes supervisadas:

Las redes feed-forward tienen conexiones unidireccionales desde las capas de entrada a las de salida. Suelen utilizarse sobre todo en la predicción, el reconocimiento de patrones y el ajuste de funciones no lineales. Las redes feed-forward aceptadas incluyen redes de retropropagación feed-forward, redes

de retropropagación cascade-forward, redes de retropropagación feed-forward de entrada retardada, redes lineales y perceptrón.

Las redes de base radial ofrecen un método alternativo rápido para diseñar redes feed-forward no lineales. Entre las variaciones aplicables encontramos las redes neuronales de regresión generalizada y las redes neuronales probabilísticas

Las redes recurrentes utilizan la realimentación para reconocer patrones tanto espaciales como temporales. Entre las redes recurrentes soportadas están las redes Elman y Hopfield

La cuantificación del vector de aprendizaje (LVQ) es un potente método para clasificar patrones que no son linealmente separables. LVQ permite especificar límites de clase y la granularidad de la clasificación

Redes no supervisadas

Las redes neuronales no supervisadas se entrenan permitiendo que la red se auto-ajuste continuamente en función de las nuevas entradas. Encuentran relaciones dentro de los datos a medida que se presentan y pueden definir automáticamente esquemas de clasificación. Neural Network Toolbox acepta dos tipos de redes auto-organizadas no supervisadas.

Las capas competitivas reconocen y agrupan los vectores de entrada similares. Al utilizar estos grupos, la red clasifica automáticamente las entradas en categorías.

Los mapas de auto-organización aprenden a clasificar los vectores de entrada de acuerdo con su similitud. A diferencia de las capas competitivas, también conservan la topología de los vectores de entrada, asignando entradas cercanas a categorías cercanas.

FUNCIONES DE APRENDIZAJE Y ENTRENAMIENTO SOPORTADAS

Las funciones de aprendizaje y entrenamiento son procedimientos matemáticos utilizados para ajustar automáticamente las ponderaciones y las desviaciones de la red. La función de entrenamiento dicta un algoritmo global que afecta a todas las ponderaciones y desviaciones de una determinada red. La función de aprendizaje puede aplicarse a ponderaciones y desviaciones individuales dentro de una red.

Funciones de entrenamiento soportadas

trainb - Entrenamiento en modo batch con reglas de aprendizaje de ponderación y desviación

trainbfg - Retropropagación BFGS cuasi-Newton

trainbr - Regularización bayesiana

trainc - Actualización incremental en orden cíclico

traincgb - Retropropagación de gradiente conjugado Powell-Beale

traincgf - Retropropagación de gradiente conjugado Fletcher-Powell

traincgp - Retropropagación de gradiente conjugado Polak-Ribiere

traingd - Retropropagación de descenso de gradiente

traingda - Descenso de gradiente con retropropagación de tasa de aprendizaje adaptativa

traingdm - Descenso de gradiente con retropropagación de momento

traingdx - Descenso de gradiente con retropropagación de momento y lineal adaptativa

trainlm - Retropropagación Levenberg-Marquardt

trainoss - Retropropagaciones secantes en un paso

trainr - Actualización incremental en orden aleatorio

trainrp - Retropropagación resistente (Rprop)

trains - Actualización incremental en orden secuencial

trainscg - Retropropagación de gradiente conjugado escalado

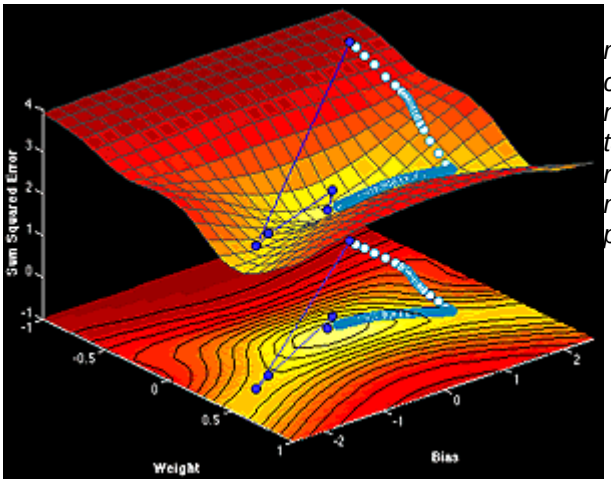


Figura b. Los gráficos MATLAB mejoran la comprensión del comportamiento de las redes neuronales. Este gráfico compara las tasas de entrenamiento de retropropagación (108 pasos) y el método Levenberg-Marquardt (5 pasos).

FUNCIONES DE APRENDIZAJE SOPORTADAS

learncon - Función de aprendizaje de desviación de conciencia

learngd - Función de aprendizaje de ponderación/desviación de descenso de gradiente

learngdm - Función de aprendizaje de ponderación/desviación de descenso de gradiente con momento

learnh - Función de aprendizaje de ponderación Hebb

learnhd - Regla de aprendizaje de ponderación Hebb con descomposición

learnis - Función de aprendizaje de ponderación Instar

learnk - Función de aprendizaje de ponderación Kohonen

learnlv1 - Función de aprendizaje de ponderación LVQ1

learnlv2 - Función de aprendizaje de ponderación LVQ2

learnos - Función de aprendizaje de ponderación Outstar

learnp - Función de aprendizaje de ponderación y desviación perceptrón

learnpn - Función de aprendizaje de ponderación y desviación perceptrón normalizada

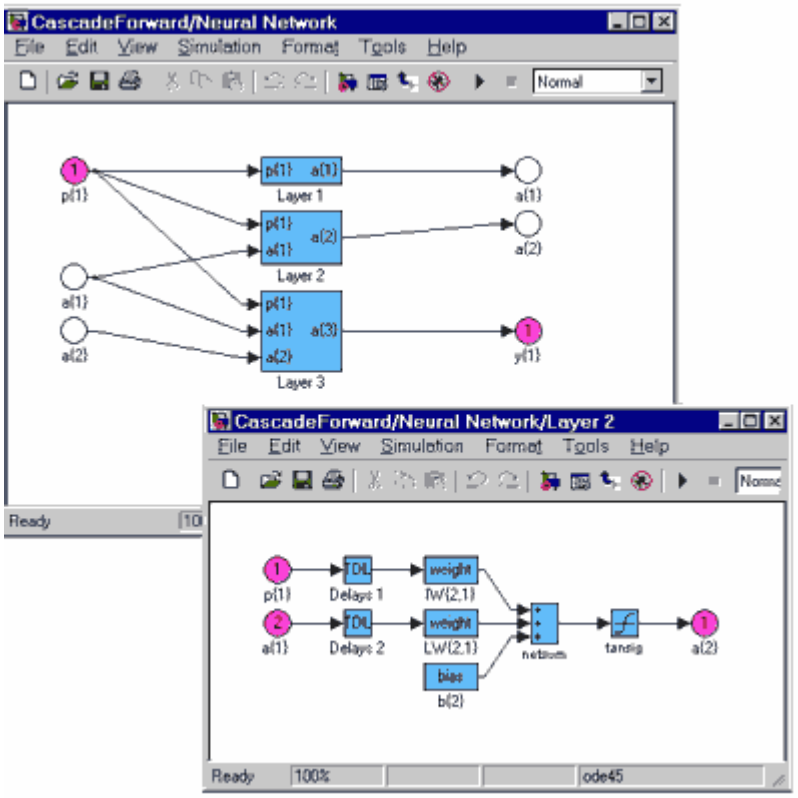
learnsom - Función de aprendizaje de ponderación de mapa auto-organizado

learnwh - Regla de aprendizaje de desviación y ponderación Widrow-Hoff

SOPORTE DE SIMULINK

Una vez que se ha creado y entrenado una red, puede incorporarse fácilmente a modelos Simulink. Un sencillo comando (gensim) genera automáticamente bloques de simulación de red para utilizar con Simulink. Gracias a esta función también puede visualizar sus redes gráficamente.

Figura c. *Los bloques de simulación de redes neuronales para usar en Simulink pueden generarse automáticamente con el comando gensim. Aquí, se ha convertido una red neuronal de tres capas en bloques Simulink. Haga clic en la imagen para obtener una vista ampliada.*



FUNCIONES DE PROCESADO PREVIO Y POSTERIOR

El procesado previo de las entradas y objetivos de la red mejora la eficiencia del entrenamiento de las redes neuronales. El procesado posterior permite analizar pormenorizadamente el rendimiento de la red.

Neural Network Toolbox ofrece las siguientes funciones de procesado previo y posterior:

El análisis de componentes principales reduce las dimensiones de los vectores de entrada

El análisis posterior al entrenamiento realiza un análisis de regresión entre la respuesta de la red y los objetivos correspondientes

Escalado de las entradas de escalas mínimas y máximas para que estén dentro del rango [-1,1]

Escalado de media y desviación estándar para normalizar la media y la desviación estándar del conjunto de entrenamiento

Mejora de la generalización

La mejora de la capacidad de generalización de la red ayuda a prevenir el sobreajuste (overfitting), un problema muy común en el diseño de redes neuronales. El sobreajuste se produce cuando una red ha memorizado el conjunto de entrenamiento pero no ha aprendido a generalizarlo a las nuevas entradas. El sobreajuste produce un error relativamente pequeño en el conjunto de entrenamiento pero producirá un error mucho mayor cuando se presenten nuevos datos a la red.

Neural Network Toolbox ofrece dos soluciones para mejorar la generalización:

La regularización modifica la función de rendimiento de la red, la medición del error que minimiza el proceso de entrenamiento. Al modificarlo para incluir el tamaño de las ponderaciones y desviaciones, el entrenamiento produce una red que no sólo funciona correctamente con los datos de entrenamiento, sino que tiene un mejor comportamiento cuando se le presentan nuevos datos.

La detección en las primeras fases es una técnica que utiliza dos conjuntos de datos diferentes. El conjunto de entrenamiento, que se utiliza para actualizar las ponderaciones y las desviaciones, y el conjunto de validación, que se utiliza para detener el entrenamiento cuando la red empieza a sobreajustar los datos.

Anexo B. Especificaciones del Sensor U are U 4000 Module

U.are.U 4000
Fingerprint Module

digitalPersona

Product Description

The **U.are.U 4000 Module** is a small fingerprint scanner designed for integration into OEM equipment where fingerprint authentication is needed.

This self-contained module optically captures and records the fingerprint image when the user touches the imaging window. Optical technology is universally acknowledged to deliver the highest quality fingerprint images, as well as being cost effective and highly reliable.

The **U.are.U 4000 Module** is designed to simplify OEM integration. The module is sealed from dust and it includes convenient mounting features. The on-board electronics automatically control calibration, image encryption, and data transfer over USB.

DigitalPersona's award-winning fingerprint matching algorithm, U.are.U applications, and developer tools make it easy to incorporate this fingerprint recognition module into your solution.

Applications

PC Peripherals, keyboards
Kiosks, point-of-sale terminals
Physical entry devices
Time and attendance devices
Government and law enforcement applications
Home and office use

Features

Small form factor
Superior image quality
Encrypted image data
Latent print rejection
Counterfeit finger rejection
Rotation invariant
Rugged
Works well with dry, moist, or rough fingerprints
Compatible with all U.are.U applications and developer kits
Drivers support Windows 98, Me, NT 4.0, 2000, XP

Key Specifications

Pixel resolution:
  512 dpi (average x,y over the field)
Image capture area:
  14.6 mm (nominal width at center)
  18.1 mm (nominal length)
8-bit grayscale (256 levels of gray)
Module size: approx. 54.5 mm x 34.2 mm x 11.0 mm
Compatible with USB specifications 1.0, 1.1, 2.0

Part Numbering

Part number	Data interface
50005-001	Full-speed USB

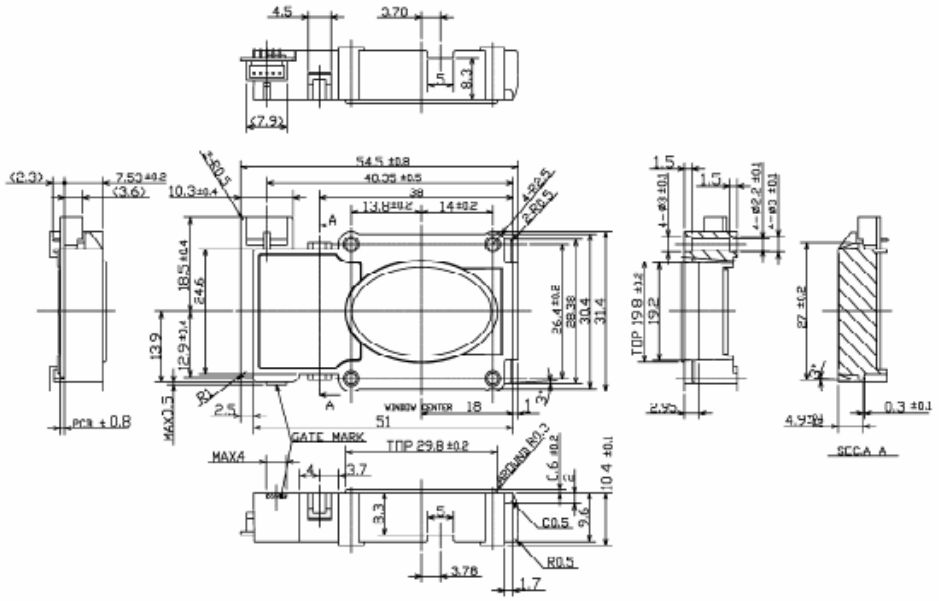
Ratings

Supply Voltage	5.0V +/- .25V
Supply Current – scanning	170 mA (typ.)
Supply Current – idle mode	120 mA (typ.)
Supply Current – suspend mode	2 mA (max.)
ESD Susceptibility	>15 KV, mounted in case
Temperature, Operating	5 - 35 C
Humidity, Operating	20% - 80% non-condensing
Temperature, Storage	-10 - 60 C
Humidity, Storage	20% - 90% non-condensing
Image data	8-bit grayscale
Standards Compliance	FCC Class B, CE, VCCI

Connector Pinout

Connector type	Hirose DF13-5P-1.25H
Pin 1:	+5 V
Pin 2:	Gnd
Pin 3:	Gnd (shield)
Pin 4:	D-
Pin 5:	D+

Mechanical Specification:



Technical data subject to change without notice
DigitalPersona Incorporated, 805 Veterans Blvd. Suite 301, Redwood City, CA USA 94063
Tel: (650) 261-6070 Fax: (650) 261-6079
www.digitalpersona.com email: sales@digitalpersona.com

MC-033-051503

CONCLUSIONES Y RECOMENDACIONES

El sistema de control de acceso que se propuso, se hizo con fines académicos, por ello recomendamos una herramienta como Matlab para la etapa de almacenamiento, procesamiento de imagen y de reconocimiento. Matlab ofrece las herramientas necesarias para desarrollar paso a paso estas etapas del sistema de control de acceso a recintos. Sin embargo, existen numerosos programas para aplicaciones de Redes Neuronales como el Stuttgart Neural Network Simulator (SNNS), que es un muy buen simulador de RNAs.

Para futuras implementaciones de un sistema de reconocimiento de huella dactilar como el propuesto, conviene aprovechar las ventajas de los chips de procesamiento digital de señal (DSP) que hay en el mercado. Estos pueden ser usados en modo microprocesador por lo que el programa de reconocimiento puede cargarse por medio de una interfaz., de esta manera podría tenerse un sistema completo, con un software de reconocimiento y con un hardware especifico para la aplicación.

En cuanto a la etapa de adquisición de datos, el mercado de sensores de huella dactilar es bastante amplio. Es necesario analizar el producto a fondo antes de integrarlo a un portafolio de soluciones de seguridad. Se debe tener en cuenta los requisitos del cliente, es decir donde se va a utilizar (si es una fabrica, una oficina, edificio, etc.) cuantas personas lo van a usar (la verificación de la identidad debe ser rápida), que tipo de personas lo van a usar (algunos

sensores tienen mas aceptación en la gente joven), etc. El sensor fue seleccionado teniendo en cuanta la resolución de la imagen entregada, el formato en que entrega la imagen (la cual debía ser compatible con Matlab) y la disponibilidad y el precio del mercado debido a que son puntos que se deben tener en cuenta en este tipo de aplicaciones.

Lo cierto es que no existe una única solución para todas las necesidades. No es posible utilizar el mismo sistema de seguridad para controlar el acceso a las salas restringidas de un banco que a un laboratorio o a un recinto ubicado en un área industrial. Para el control de acceso de las salas del banco, puede que no sea suficiente con un solo sensor biométrico, la solución puede estar en una combinación de sensores biométricos, por ejemplo, sensor de iris y huella dactilar. Otra solución sería una combinación de sensor de huella dactilar con un sensor que detecte "vida", asegurando que la persona que se está registrando tenga vida, y evitando así intentos de fraude al sistema. Esto se aplica cuando el lugar que se está protegiendo demanda sistemas suficientemente robustos, que ofrezcan un alto nivel de seguridad. No obstante lo anterior, la autentificación biométrica por sí sola no puede resolver todas las necesidades de autentificación y seguridad, sino que hemos de considerarla una herramienta más dentro de nuestro repertorio.

GLOSARIO

AFAS: Sistema automático de autentificación de huella dactilar

AFIS: Sistema automático de identificación de huella dactilar

CCD: Dispositivo de carga acoplada

FAR: Tasa de falsa aceptación

FRR: Tasa de falso rechazo

PDP: Procesamiento distribuido en paralelo

PIN: Número de identificación personal

SOM: Estructura de red neuronal autoorganizadas diseñadas explícitamente para extraer características

RIDGES: Líneas paralelas en una huella dactilar

RNAs: Redes neuronales artificiales

BIBLIOGRAFÍA

Internacional Biometric group. [En línea].http://www. biometricgroup.com7reports7public7finger_scan_optsiluit.html.[Consulta:5 Octubre 2003].

Introducción a la autentificación biométrica.[En línea].http://www. imarketing.es.[Consulta:23 Octubre 2003].

Controlde acceso por biometría. [En línea].http://www. securynet.com/rubros/productos/notas/prod104100.htm.[Consulta:13 Octubre 2003].

International Biometric industry association IBIA.[En línea]. http://www.ibia.org. [Consulta:20 Noviembre 2003].

Biometric consortion. [En línea]. http://www.biometric.org. [Consulta:9 Noviembre 2003].

A Biometric estandar for information management and security. [En línea]. http://www.compseconline.com. [Consulta:20 Noviembre 2003].

Hilera, José R. y Martínez, Víctor J. (1995). Redes neuronales artificiales. Fundamentos, modelo y aplicaciones. Madrid: Editorial RA-MA.

Tutorial redes neuronales.[En línea]. http://ohm.utp.edu.co/neuronales/maindown.htm.[Consulta:24 Septiembre 2003].

Matlab 6.5 help neural network pdf. .[En línea]. http://www.mathworks.com/acces/helpdesk/help/pdf_doc/nnet.pdf.[Consulta:52 Septiembre 2003].

Desarrollo de algoritmos de filtrado de imágenes de huellas dactilares.[En línea].http://www.iit.upco.es/palacios/pfc/itiei/pfc2000-2001/arias.pdf.[Consulta:6 Septiembre 2003].