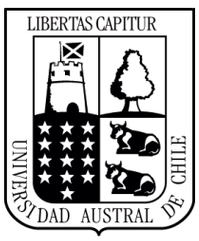

Universidad Austral de Chile

Facultad de Ciencias de la Ingeniería

Escuela de Ingeniería Civil en Informática

DISPOCITIVO IDENTIFICADOR DE PERSONAS CON RFID Y BIOMETRÍA

DIPRB

Proyecto para optar al título de
Ingeniero Civil en Informática

PROFESOR PATROCINANTE:
NOMBRE DEL PATROCINANTE
TÍTULOS Y GRADOS DEL PATROCINANTE

PROFESOR CO-PATROCINANTE:
NOMBRE DEL CO-PATROCINANTE
TÍTULOS Y GRADOS DEL CO-PATROCINANTE

PROFESOR INFORMANTE:
NOMBRE DEL INFORMANTE
TÍTULOS Y GRADOS DEL INFORMANTE

ENZO EDGARDO VERA PAGNARD

VALDIVIA - CHILE
2014

AGRADECIMIENTOS

ÍNDICE

ÍNDICE DE TABLAS

ÍNDICE DE FIGURAS

FIGURA PÁGINA

RESUMEN

ABSTRACT

1. INTRODUCCIÓN

En la búsqueda de soluciones más eficientes y a bajo costo, conocer de componentes electrónicos como sensores (luminosidad, humedad, temperatura, etc.), microcontroladores, servo motores, pantallas LCD, entre otros, son herramientas poderosas debido a las diferentes problemáticas que pueden dar solución, integrar estas tecnologías dan un gran valor agregado a cualquier tipo proyecto, permitiendo solucionar en el ambiente del usuario diferentes problemáticas de manera útil y efectiva.

Para lograr que este dispositivo interactúe con el ambiente donde está inmerso y se comunique con una base de datos de manera local o de forma remota a través de Internet se hace necesario el desarrollo de piezas de software, capaz de procesar la información recolectada, ya sea en tiempo real o cuando sea necesario, dando de esta manera las funcionalidades necesaria para cubrir las necesidades demandadas.

Para realizar este proyecto se utilizara plataformas de Open Hardware, lo que nos brinda la libertada de construir un dispositivo capaz integrar cualquier tipo de sensor estándar, lo cual nos permite generar el conocimiento para manipular cualquier tipo de sensor.

1.1. Objetivos

1.1.1. Objetivo general

Construir un dispositivo capas de cuantificar y controlar el flujo de personas de algún espacio físico y con esto gestionar su mantención de mejor manera. El dispositivo debe ser capaz de integrar distintos sensores de reconocimientos (RFID y lector biométrico), comunicarse con un servidor para poder guardar la información en una base de datos y generar algunos reportes.

1.1.2. Objetivos específicos

1. Estudiar las diferentes tecnologías de Open Hardware relevantes para este proyecto, incluyendo sensores (RFID y lector biométrico) y microcontrolador.

2. Definir arquitectura del sistema que permita la escalabilidad e integración con otros sistemas, definiendo estándares de comunicación entre otros.

3. Seleccionar la plataforma de Open Hardware y sensores atingentes al proyecto, diseñar piezas de software que permita comunicar el dispositivo con la base de datos.

4. Modelar e implementar la base de datos que permita manipular la información eficientemente.

5. Entender nuevas tecnologías de programación web para implementar un prototipo de software de administrador de espacios.

6. Realizar pruebas evaluación del funcionamiento del sistema.

1.2. Motivación

El desarrollar conocimiento de plataformas de Open Hardware, tanto desde el punto de vista de la electrónica, como de metodologías de desarrollo de software, si bien las metodologías de desarrollo de software tradicionales no son las más adecuadas para este tipo de plataformas, es importante explorar como adaptar está metodologías a este tipo de proyectos.

Una de las áreas donde existe una brecha considerable en la formación como estudiantes, es en la solución de problemas en industrias manufactureras, no desde el punto de vista de la gestión o administración, sino en cubrir funcionalidades prácticas que presenten problemas dentro de los procesos productivos, como por ejemplo detener un motor si la temperatura de él es mayor a 100 grados Celsius o detener una prensa hidráulica si ocurre algún improvisto en la línea de producción, esta área sea transformado en un mercado creciente dentro de este tipo de industria[Ind09] y representa un potencial nicho de mercada para futuros emprendimientos en el área de tecnologías de información y comunicación.

Además poder realizar algunas estadísticas sobre estas máquinas, ayudando a la gestión de estás misma, contribuyendo a los objetivos estratégicos del cliente, con este proyecto en algún grado se acortará esta brecha obteniendo datos del ambiente para luego procesarlos y automatizar procesos.

1.3. Impacto

Como este proyecto estará desarrollado en plataformas de Open Hardware y Open Software generará una base de conocimiento con respecto a la integración de dispositivos electrónicos a motores de bases de datos y plataformas web para manejar esta información, ahorrando tiempo y dinero, si en algún momento se requiere de este conocimiento para

realizar algún producto de TIC que necesite manejar variables del ambiente en donde se encuentran inmersos y controlar otros dispositivos.

2. MARCO TEÓRICO

A lo largo del presente capítulo se pretende describir los conceptos en torno a los cuales se efectuará el siguiente trabajo. Además se llevará a cabo una revisión de las tecnologias relacionadas con este proyecto como son las plataformas open hardware, sensores y microcontroladores .

2.1. Open Hardware

2.1.1. ¿Qué es Open Hardware?

Se les llama Open Hardware a todos los dispositivos de hardware cuyas especificaciones y diagramas esquemáticos son de acceso público, ya sea bajo algún tipo de pago o de forma gratuita. Algo que tienen en común el Open Hardware y el Open Software es que ambos corresponden a las partes tangibles de un sistema informático.
El Open Software ofrece al usuario cuatro libertades de uso, de estudio y modificación, de distribución y de redistribución de las versiones modificadas. Existen licencias que garantizan y dan cobertura legal, como por ejemplo la licencia GNU GPL. El Open Hardware toma es mismas ideas del Open Software para aplicarlas en su campo.[Osh14]
Esta idea es tan antigua como la del Open Software, sin embargo su empleo no es tan directo compartir diseños de hardware es un poco más complicado no se cuenta con una definición exacta. Incluso Richard Stallman Presidente de la Free Software Foundation afirma que las ideas del Open Software se pueden aplicar a los archivos o fichero necesarios para el diseño y especificación, pero no al circuito físico en sí.
Al no existir una definición clara de Open Software cada persona lo interpreta a su manera. Dependiendo del enfoque pueden ser establecidas dos clasificaciones la primera tiene en cuenta cómo es su naturaleza estático o reconfigurable y la otra en función de su filosofía.

2.1.1.1. Según su Naturaleza

Dada su diferente naturaleza, al hablar de Open hardware hay que especificar de qué tipo de hardware se está hablando. A continuación se describen cada uno de los diferentes hardwares según su naturaleza:

- **Hardware reconfigurables**

  Es aquél descrito mediante un lenguaje de descripción de hardware. Su naturaleza es completamente diferente a la del hardware estático. Se desarrolla de una manera

muy similar a como se hace con el software, mediante archivos de texto, que contienen el código fuente. Se les puede aplicar directamente una licencia libre, como la GPL. Los problemas no surgen por la definición de qué es libre o qué debe cumplir para serlo, sino que aparecen con las herramientas de desarrollo necesarias. Para hacer que el hardware reconfigurable sea libre, sólo hay que aplicar la licencia GPL a su código.

- **Hardware estático**

  Es el conjunto de elementos materiales o tangibles de los sistemas electrónicos.

2.1.1.2. Según su filosofía

Al no existir una definición clara de Open Hardware, también existe libertad en su interpretación. Muchos de los argumentos acerca del diseño de Open Hardware provienen de quienes hablan en las comunidades de software y hardware. Una causa de esto es el simple hecho de que la palabra "software" refiere tanto al código fuente como a los archivos o ficheros ejecutables, mientras que las palabras "hardware" y "diseño de hardware" se refieren claramente a dos cosas distintas. Usar la palabra "hardware" como taquigrafía para el diseño y el objeto físico es una receta para la confusión. Los términos siguientes se han utilizado en discusiones de este asunto.

- **Free hardware design**

  Se refiere a un diseño que pueda ser copiado, distribuido, modificado, y fabricado libremente. No implica que el diseño no pueda también ser vendido, o que cualquier puesta en práctica de hardware del diseño estará libre de coste. Todas las mismas discusiones sobre el significado de la "libertad" entre los partidarios de la *Free Software Foundation*, y los partidarios de la Licencia BSD que afecta al software, desafortunadamente las trasladan a los diseños del hardware.

- **Open source hardware**

  Se refiere al hardware para el cual toda la información del diseño se pone a disposición del público en general. Open source hardware se puede basar en un free hardware design, o el diseño en el cual se basa puede ser restringido de alguna

manera.

- **Open Hardware**

  Es una marca registrada del Open Hardware Specification Program. Es una forma limitada de open source hardware, para la cual el requisito es que: La suficiente documentación del dispositivo debe estar disponible para que un programador competente pueda escribir un controlador del dispositivo. La documentación debe cubrir todas las características de la interfaz del dispositivo - controlador que se espera que cualquier usuario emplee. Esto incluye funciones de entrada-salida, de control y funciones auxiliares como medidas de funcionamiento o diagnósticos de auto prueba. Los detalles de soporte de firmware on-board y de la puesta en práctica de hardware no necesitan ser divulgados excepto cuando son necesarios para permitir programar un controlador para el dispositivo.[Del07]

  Es decir, solamente una cantidad de información limitada sobre el diseño necesita estar disponible; posiblemente no mucha, por ejemplo, para hacer una reparación.

2.2. Biometría

Históricamente, la identificación personal se ha basado en posesiones especiales (llaves, tarjetas) o en conocimientos secretos (palabras claves, números de identificación personal), todos estos aspectos son casi únicos, y se emplean para verificar la identidad de su portador. Ahora bien, el ser humano posee características propias que lo hacen único: huellas dactilares, la voz, el rostro, la forma de escritura, e incluso el iris del ojo.Entonces, podemos decir que nosotros llevamos nuestras propias palabras claves, tarjetas o números PIN. Entonces, ¿Porque no aprovechar estas características?

Los científicos se formularon está misma pregunta hace algunos años, dando origen a la Biometría. Ésta consiste en la identificación o verificación de la identidad de un individuo, empleando sus características biológicas, psicológicas y de conducta. En la actualidad, existen distintos tipos de dispositivos que soportan la biometría, tales como lectores de huella digital o lectores de retina.[Car08]

Por definición, un sistema biométrico, es un sistema automático capaz de:

1. Obtener la muestra biométrica del usuario final.
2. Extraer los datos de la muestra.
3. Comparar los datos obtenidos con los existentes en la base de datos.
4. Decidir la correspondencia de datos.
5. Indicar el resultado de la verificación.

Algunos de los dominios para esta tecnologia son:

- **Bioinformática**: Aplicación de la informática en el área de la medicina y la biología.
- **Biometría forense**: La ciencia y tecnología de usar e interpretar la evidencia física para propósitos legales.
- **Interacción Humano-Computador *(Human-to-Computer Interaction-HCI)***: Su objetivo es mejorar el rendimiento y la precisión de esas interfaces, mediante el reconocimiento de los usuarios y adaptarse a las características específicas de cada usuario para labores de reconocimiento.
- **Seguridad biométrica**: Autenticación de usuarios. Enlazar la información digital a una determinada identidad para lograr control de acceso, autenticación de información entre otras.

En este trabajo de titulación,este último dominio es el que nos interesa y en el cual se centraremos especial atención y esfuerzos.
Cabe destacar que todos los métodos biométricos conocidos son “no determinísticos” y necesitan estar basadas en aproximaciones heurísticas.
Existen 2 modos de operación en los sistemas de autenticación biométrica: El enrolamiento (*Enrollment*) y la autentificación (*Authentication*).

2.2.1. Enrrolamiento y Autenticación

Existen 2 modos de operación en los sistemas de autenticación biométrica: El enrolamiento (*Enrollment*) y la autentificación (*Authentication*).

Enrolamiento

El proceso de enrolamiento ocurre cuando nos registramos en el sistema, donde las características de cada usuario se almacenan para futuras referencias y asociaciones de identidad de los sujetos. Una representación gráfica de este modo se aprecia en la Figura 1

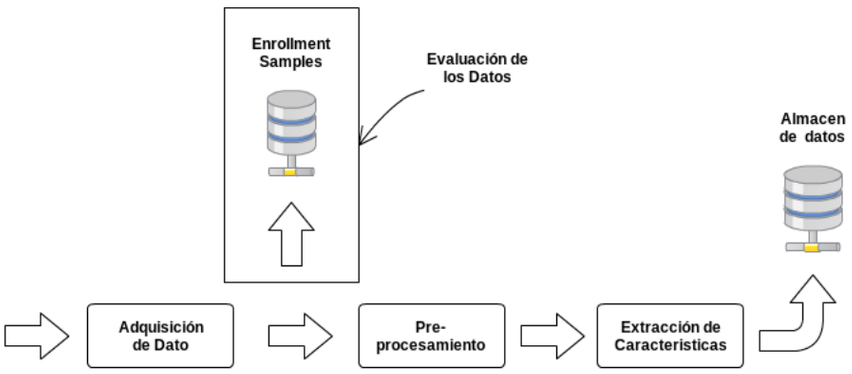

Figura 1. Esquema gráfico del proceso de Enrrolamiento

Aquí se observa que el proceso comienza con la toma de datos (por ejemplo, medir y realizar conversiones análogo-digital). La representación digital posterior a este proceso es denominada Enrollment Samples(Ejemplos de Enrolamiento) o simplemente enrollments. Desde el enrollment original se extraen las características biométricas, son preprocesadas, y en algunos casos almacenadas en algún soporte de datos (como una base de datos) para poder reproducirlas en otro momento.

2.2.1.1. Autenticación

La Autenticación (*authetication*) consiste en el proceso de verificar o identificar la identidad de algún sujeto, según corresponda, en la Figura 2 se muestra en forma gráfica este proceso.

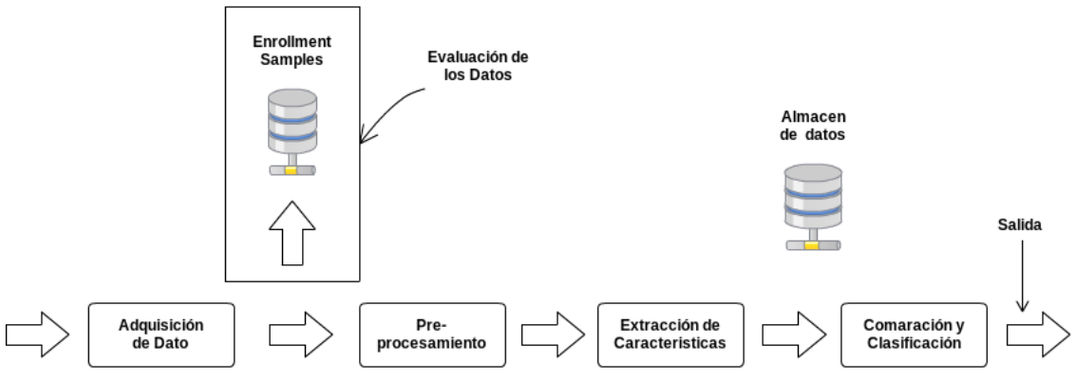

Figura 2. Esquema gráfico del proceso de Autenticación

2.2.2. Verificación versus Identificación

La autenticación la podemos dividir en dos acciones verificación y identificación, en función de cómo se desee obtener la identidad del sujeto.

2.2.2.1. Verificación

El modo de Verificación es el sistema de autentificación que determina si un set determinado de características son similares al template de dicha persona para determinar si es o no es la persona. El resultado de esta acción es siempre una decisión binaria(si o no, 0 o 1) entregando en algunos casos el puntaje de acierto (Matching Score), lo que muestra el grado de similitud entre su template y ésta persona.

2.2.2.2. Identificación

El modo de Identificación describe el proceso de determinar la identidad de un sujeto (dadas sus características biométricas) comparándolas con un rango de sujetos. Así, la clasificación asignada será una entre todas las personas registradas en el sistema.
Para ejemplificar estos conceptos, veamos los siguientes ejemplos.

- Si tenemos un control de acceso para un portal principal, nuestro problema es "Determinar quién es", para en función de eso, determinar si ingresa o no. Esto sería una identificación.
- Si tenemos una oficina del usuario "Pedro Paredes", donde sólo él tiene asignado acceso, nuestro problema es "Determinar si soy Pedro Paredes", por lo tanto, verificar si soy el usuario determinado. Esto es una verificación.

Es fundamental entender ambos mecanismos y encontrar el más adecuado para nuestros requerimientos.

2.2.3. Criterios de selección de características biométricas

Se han sugerido distintos criterios para autenticar de manera adecuada. A continuación veremos los 4 más importante:

1. **La Variabilidad** La Variabilidad tiene que ver con la variación de los valores desde un evento a otro, sobre una misma persona. Este efecto es llamado variabilidad Intra-Personal o Intra-Class. La variabilidad es inherente a todos los sistemas biométricos

debido a la naturaleza no determinística de las mediciones biométricas, en la Figura 3 vemos un ejemplo de variabilidad [Way00].

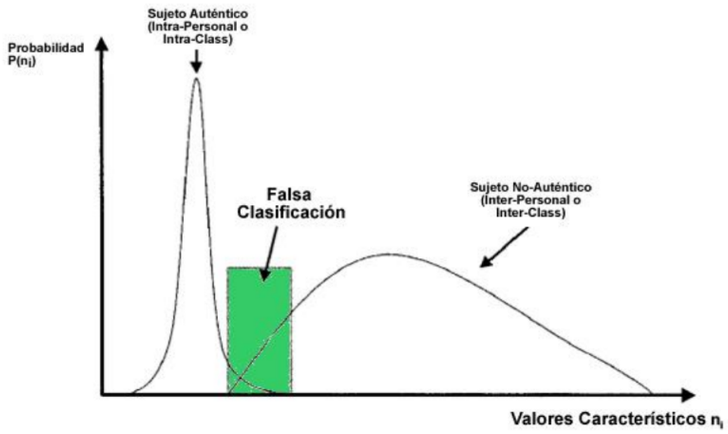

Figura 3. Ejemplo de variabilidad y capacidad de discriminar una característica biométrica

2. **La Capacidad Discriminatoria** está determinada por el grado de unicidad de las características biométricas que serán utilizadas en la comparación. Aparentemente, un buen sistema biométrico posee una baja variabilidad Intra-Personal y una alta variabilidad Inter-Personal (entre distintas personas). El grado de variabilidad Intra-Personal está reflejado por el ancho de una distribución gaussiana (ver Figura 3) para sujetos auténticos, donde la capacidad discriminatoria puede ser estimada en la intersección de las curvas de sujetos auténticos versus sujetos no-auténticos [Zha00].

3. **La Acertividad**, para diseñar un sistema biométrico funcional, las características deben poseer bastante acertabilidad en un tiempo aceptable. Hoy en día, el criterio es determinado por la tecnología del sensor, planteando la inquietud de saber si obtuvo la característica en un tiempo aceptable y con la suficiente calidad. Por ejemplo, un examen de ADN es muy exacto, sin embargo, requiere un amplio tiempo de trabajo de verificación [Zha00].

4. **El Rendimiento**, cuando nos referimos a que una característica biométrica debe ser procesada en un tiempo aceptable nos referimos al rendimiento de un sistema biométrico. de una persona para el ingreso a una oficina. Por lo general asociamos el grado de exactitud en función del tiempo de respuesta que deseemos obtener [Way00].

2.2.4. Medidas de Rendimiento y Exactitud

Los sistemas biométricos intentan determinar o verificar la identidad de cada miembro registrado en nuestro sistema utilizando medidas y/o características distintivas. Debido a la naturaleza no-determinística de este proceso, es imposible realizar un análisis exacto (con los sistemas del día de hoy). Evaluaciones técnicas sugieren que éstas deben ser realizadas mediante análisis estadísticos y mediciones empíricas.

Según el tipo de medición biométrica que deseemos utilizar, se utilizan distintos indicadores. A través de las últimas 2 décadas, se llegó al consenso en cuáles eran las mediciones más importantes, para realizar las evaluaciones técnicas pertinentes [Way99] y que son presentadas en la tabla 1.

Tabla 1. Pricipales medidas para evaluaciones de los sistemas biométricos

Medida	Descripción
Tasa de Falsos Aciertos *False Match Rate* (FMR) *False Accept Rate* (FAR)	Tasa entre coincidencias detectadas por el sistema pero que no son reales (falsos positivos) versus el número total de muestras.
Tasa de Falso Rechazo *False Non-Match Rate (FNMR)* *False Reject Rate (FRR)*	Tasa entre coincidencias que no son detectadas por el sistema pero que sí son reales (falsos negativos) versus el número total de muestras.
Tasa donde los errores son iguales *Equal-Error-Rate (EER)*	El punto en el diagrama de tasa de errores donde las tasa de falsos aciertos es igual a la tasa de falsos rechazos.
Tasa de error por particionamiento *Binning Error Rate (BNR)*	Tasa de falsos rechazos debido a errores de particionamiento.
Coeficiente de Penetración *Penetration Coefficient (PC)*	Porcentaje promedio del tamaño del repositorio de datos a ser revisado para cada proceso de autenticación.
Tiempo de Transacción *Transaction Time (TT)*	Tiempo requerido para una sola transacción de autenticación, compuesto por la suma del tiempo de recolección de datos y el tiempo de cálculo.

Las dos primeras medidas definen el umbral de decisión (*threshold*) desde donde se puede optimizar el nivel de exactitud en función del tiempo de búsqueda como se muestra en la Figura4. esto quiere decir que a un alto valor de umbral implica un sistema menos exacto, por lo cual podria aceptar a quien no posee los permisos correspondientes, pero más rápido a la hora de entregar resultados. Por el contrario, con un bajo umbral de decisión, es menos probable equivocarse, pero el tiempo de procesamiento es mucho mayor. A pesar de la importancia de estos indicadores en los distintos dispositivos biométricos, no es objetivo de este proyecto de título entrar en mayores detalles.

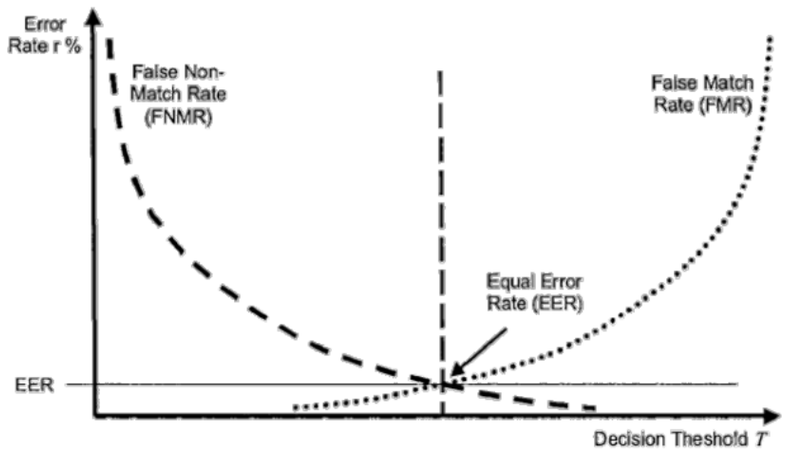

Figura 4. FNMR, FMR y EER en función del umbral de decisión

2.2.5. Dactiloscopía: Reconocimiento de huellas dactilares

La base de ésta modalidad biométrica es la estructura que posee la piel en la punta de los dedos. Se trata de una característica biológica fenotípica, es decir, una manifestación específica de determinados rasgos, que serían únicos, incluso en caso de personas que son gemelos.

La estructura biométrica está compuesta por "crestas papilares" y los "surcos interpapilares", comúnmente llamados "crestas" y "valles". Las crestas papilares son los relieves epidérmicos situados en la palma de las manos y en la planta de los pies, mientras que los surcos interpapilares se determinan por las depresiones que separan dichos relieves o crestas. Dentro de las crestas papilares existen los llamados "poros papilares", que son diminutos orificios de variadas formas y dimensiones por los cuales se expulsa el sudor. Una vez que el sudor sale al exterior, se derrama por todas las crestas y se mezcla con la grasa natural de la piel, dando lugar a que cuando se toque un objeto apto para la retención de huellas, éstas queden impresas en el mismo. Esta es la base de la impresión dactilar.
Se ha demostrado científicamente y comprobado por la experiencia, que son perennes, inmutables y diversiformes

- **Son perennes**, porque desde que se forman en el sexto mes de la vida intrauterina, permanecen invariantes en número, situación, forma y dirección hasta la muerte, en que la putrefacción destruye la piel.
- **Son inmutables**, ya que las crestas papilares no pueden

modificarse fisiológicamente. Si hay un traumatismo poco profundo, se regeneran y si es profundo, las crestas no reaparecen con forma distinta a la que tenían, sino que la parte afectada por el traumatismo resulta invadida por un dibujo cicatrizal.

- **Son diversiformes**, pues no se ha hallado todavía dos impresiones idénticas producidas por dedos diferentes.

2.2.5.1. Clasificación

En la actualidad, existen tres niveles de clasificación entre los cuáles es posible obtener imágenes de las huellas dactilares:

1. **Características globales**: patrón de características definido a nivel mundial a partir de la colección de crestas existentes en un dedo, clasificado en dos clases de "Wirbel" (Whorl y doble ciclo) y cuatro clases de "lazos" [Bal97]. La Figura 5 muestra un diagrama con la taxonomía respectiva.

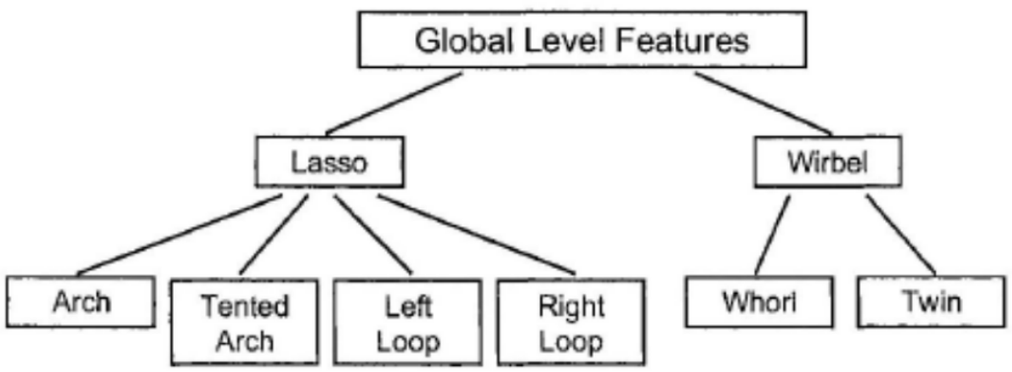

Figura 5. Clasificación de tres niveles de características globales de una huella dactilar

2. **Características basadas en minucias**: estas se basan en características e interrelaciones entre los distintos puntos, surcos y crestas dentro de un dominio espacial. La clasificación se origina a partir de elementos utilizados en medicina forense desde hace más de un siglo. Aquí se incluyen elementos tales como bifurcaciones, islas, terminaciones, empalmes, horquillas, lagos, cordilleras independientes, entre otros. En las Figuras 6 y 7 se puede observar algunos ejemlos de caracteristicas basadas en minucias.

Figura 6. Ejemplos de algunas características basadas en minucias

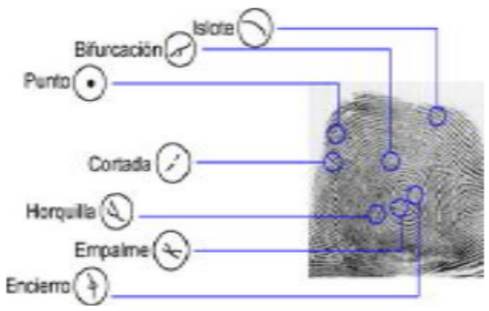

Figura 7. Ejemplo de Huella digital y algunas características basadas en minucias

3. **Características basadas en**: Los poros, aberturas de las glándulas sudoríparas, son visibles en la superficie del dedo y constituyen un patrón formado por los puntos en la cima de las crestas[Rod97]. La adquisición de estas características, requieren de sensores de alta resolución espacial. En la figura 8 se muestra una ilustración de la distribución de éstas características.

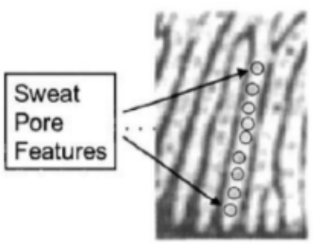

Figura 8. Ejemplo de Huella digital y algunas características basadas en minucias

2.2.5.2. Adquisición de los datos

Para adquirir los datos de una huella dactilar se requieren dispositivos sensores específicos que puedan obtener una imagen de ella. Estos se puede dividir en sensores ópticos y sensores no ópticos. Los primeros requieren exponer la punta de los dedos a una superficie transparente que es sometida a la luz, observando su respuesta óptica; Los sensores no ópticos capturan la información sobre el perfil de altitud de la superficie de los dedos por medios distintos a la luz. Aquí se establece un voltaje eléctrico entre la piel y la superficie del sensor, que posee un conjunto de diminutos electrodos que generan voltaje cuando se

expone a presión, obteniendo el perfil de alturas de las crestas y los valles. Existen otros sensores no ópticos que obtienen un perfil térmico de la piel de una distancia específica y que extraen la información de elevación desde un termograma bidimensional. En todos los casos, el resultado de la adquisición de los datos es un arreglo bidimensional de mediciones escalares que es habitualmente interpretado como imágenes en escalas de gris de distintas resoluciones y tamaños.

En las impresiones dactilares, los tamaños de imágenes generalmente se encuentran en el rango de 0,4 a 1 pulgada de altura y de 0,4 a 0,6 pulgadas de ancho, mientras que las resoluciones de escaneo de estos sensores se encuentran con valores entre 200 a 1000 dpi [Mal03].

2.2.5.3. Extracción de Características

Como se mencionó anteriormente, las características pueden ser clasificadas en 3 niveles: características globales, basadas en minucias y por el sudor de los poros. Aunque la primera y tercera categoría han mostrado una buena precisión en reconocimiento biométrico [Bal97], la mayoría de los enfoques se basan en la detección de minucias, no siendo ésta la excepción, por lo que se expondrá brevemente sobre las más comunes técnicas de procesamiento de imágenes para encontrar y clasificar los puntos característicos. Este procesamiento entrega un mapa de la ubicación espacial, la orientación y el tipo de características con respecto a la imagen original [Rod97].

La detección de minucias requiere numerosos pasos de preprocesamiento, que comienza con la utilización de filtros de mejoramiento de imagen tales como la ecualización de histogramas, para poner énfasis en las frecuencias relevantes en la imagen. Otro filtro que ha mostrado alta eficiencia es el filtrado basado en la dirección de la frecuencia, por ejemplo los filtros *Gabor*, ya que pone énfasis en los cerros en una dirección local. Además, son aplicadas algunas rutinas estándares en el procesamiento de imágenes como lo son el suavizado, y el perfilado, seguido de un proceso de binarización para obtener imágenes reales en blanco y negro.

Basados en la imagen binaria, se aplican algoritmos de adelgazamiento y de erosión, que dan lugar a una imagen de representación en virtud de la representación de las crestas, que tendrán un ancho de 1 pixel llamado “esqueleto”. Un ejemplo de cómo va quedando la imagen con cada uno de estos procesos puede ser observado en la figura 9.

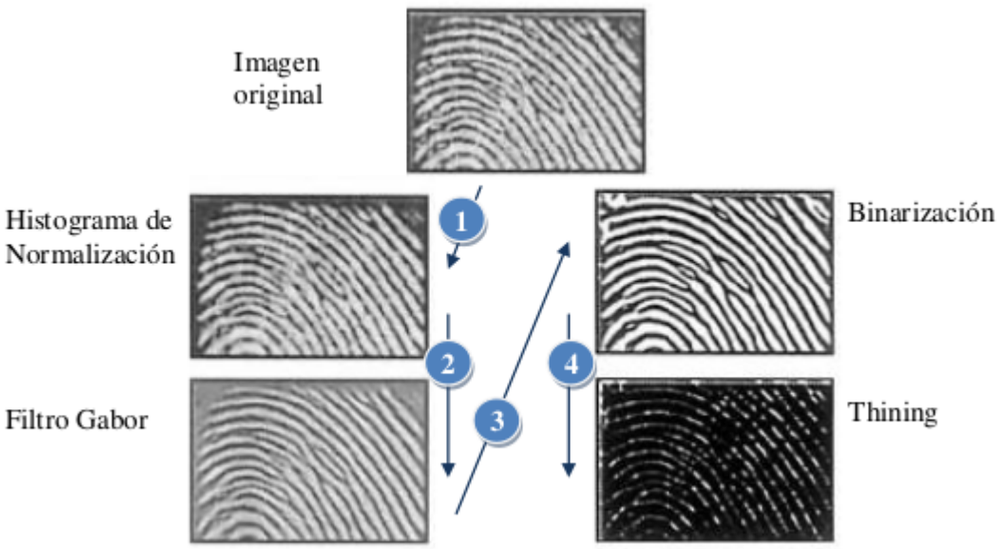

Figura 9. Tratamineto de imagen de una huella dactilar para encontrar puntos caracteristicos

Una vez obtenida las imágenes del esqueleto, la detección de las minucias es una tarea sencilla. Esto puede lograrse mediante de 8 reglas de vecindad: cada pixel de la imagen es analizado en el contexto de sus 8 pixeles vecinos. Un ejemplo es el caso que 1 pixel tenga sólo 1 vecino: este será clasificado como minucia terminal.

Note que detrás las técnicas basadas en minucias, existen otros tipos de características como crestas y características basadas en correlación, que requieren diferentes tipos de preprocesamiento. Particularmente, los métodos basados en correlación son sensibles a las transformaciones, por lo que requieren normalizaciones de tamaño y de orientación.

2.2.5.4. Comparación y Clasificación

La gran ventaja del reconocimiento de huellas dactilares basadas en minucias es la invariabilidad en escala y rotación de los puntos detectados. Esto quiere decir, que si rotamos o ampliamos la huella dactilar, los valores seguirán siendo los mismos, sin necesidad de hacer cálculos adicionales, razón por la que en vez de medir sus posiciones en términos de coordenadas absolutas o posición relativa, estas pueden compararse durante el proceso de correspondencia. Un ejemplo simplificado de esto es posible verlo en la figura 10. Aquí (x_1, y_1) y (x_2, y_2) muestran la posición absoluta de los puntos 1 y 2 respectivamente, mientras que $\Theta 1$ y Θ_2 sus orientaciones angulares. Un posible enfoque para la comparación de minucias es calcular un mapa de las posiciones de cada punto con respecto a las otras minucias en la imagen. Este modelo se puede lograr por ejemplo

mediante coordenadas polares, donde las distancias y los ángulos de todos los puntos son enumerados por cada minucia. Las distancias se pueden calcular mediante la ecuación no 1, mientras que la orientación angular se puede obtener a la partir de la ecuación no 2

$$\delta_{1,2} = \sqrt{(y_2 - y_1)^2 + (x_2 - x_1)^2} \tag{1}$$

$$\alpha_{1,2} = \Pi - \arctan\left(\frac{y_1 - y_2}{x_2 - x_1}\right) \tag{2}$$

Por lo tanto tenemos tres medidas escalares de distancia entre los puntos característicos, independiente de la orientación del sistema de coordenadas.

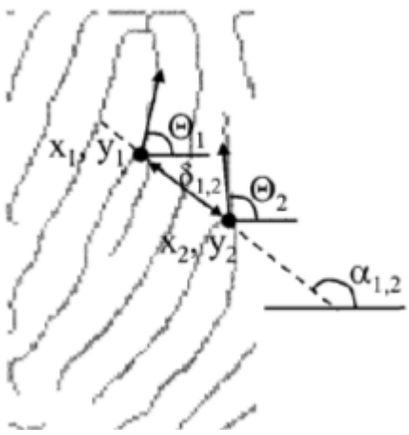

Figura 10. Puntos característicos tipo bifurcación. Sus coordenadas y orientaciones angulares están dadas por (x_1, y_1, Θ_1) y (x_2, y_2, Θ_2) .

Hay un gran número de nuevos métodos para la extracción de distancias locales.Independiente de su tipo, la colección de mediciones de distancias locales pueden ser acumuladas durante el proceso de correspondencia, y en consecuencia, dar lugar a una medida de similitud, ya mencionada anteriormente, denominada umbral de decisión, que determina con qué nivel de exactitud queremos verificar o identificar a un sujeto, lo que puede determinar la búsqueda en base a “que tan similar es un sujeto con el patrón almacenado”.

Este método es sólo un ejemplo ilustrativo de cómo tratar un enfoque para características basadas minucias, pero es necesario saber que existe un gran número de enfoques muy distintos al aquí comentado, razón por la que es necesario estudiar literatura adicional para ser más experto en el tema.

2.3. Identificación por Radio Frecuencia RFID

Si bien en la actualidad la tecnología más extendida para la identificación de objetos es la de los códigos de barras, éstos presentan algunas desventajas, como son la escasa cantidad de datos que pueden almacenar y la imposibilidad de ser modificados o reprogramados. La mejora que se ideó, y que constituye el origen de la tecnología RFID, consistía en usar chips de silicio que pudieran transferir los datos que almacenaban al lector sin contacto físico.

Entnces podemos definir RFID como uns sistema de almacenamieto y recuperación de datos de manera remota, utilizando dispositivos denominados tags o etiquetas RFID. El propósito fundamental de la tecnología RFID es transmitir la identidad de un objeto, similar a un número de serie único, mediante ondas de radio.

Un tags RFID es un dispositivo pequeño, similar a una pegotina, que puede ser adherida en un producto, animal o persona. Contienen antenas para permitir recibir y responder a peticiones por radiofrecuencia desde un emisor-receptor RFID.

Una de las ventajas del uso de radiofrecuencia, en lugar de otras tecnologias como de infrarrojos, es que no se requiere visión directa entre emisor y receptor.

2.3.1. Arquitectura y tipos de tarjetas

El funcionamiento de los sistemas RFID es simple. La etiqueta RFID, genera una señal de radiofrecuencia con la información. Ésta es captada por un lector que lee la información y se la entrega, digitalmente, a la aplicación específica que utiliza RFID.

Por tanto, un sistema RFID consta de tres componentes Etiquetas o Tags RFID, Lector o Transceptor RFID y Aplicación como se ve en la figura 11

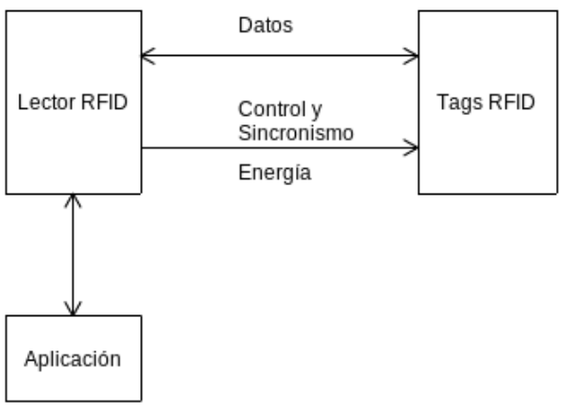

Figura 11. Arquitectura de un sistema RFID

2.3.1.1. Etiqueta RFID

Esta compuesta por una antena, un radiotransmisor y un material encapsulado o chip. El propósito de la antena es permitir al chip, que contiene la información, transmitir la información de identificación de la etiqueta. El chip posee una memoria interna con una determinada capacidad, depende del modelo y varía desde una decena hasta millares de bytes.
Existen varios tipos de memoria:

- **Solo lectura**: El código de identificación que contiene es único y es personalizado durante la fabricación de la etiqueta.
- **De lectura y escritura**: La información de identificación puede ser modificada por el lector.
- **Anticolisión**: Se trata de etiquetas especiales que permiten que un lector identifique varias al mismo tiempo y no se solapen, normalmente las etiquetas deben ingresar una a una en la zona de cobertura del lector.

2.3.1.2. Lector de RFID

Compuesto por una antena, un transceptor y un decodificador. El lector envía periódicamente señales para ver si hay alguna etiqueta en sus inmediaciones. Cuando capta la señal de una etiqueta, que contiene la información de identificación de ésta, extrae la información y se la pasa al subsistema de procesamiento de datos.

2.3.1.3. Subsistema de Procesamiento de datos

: Proporciona los medios de procesamiento y almacenamiento de los datos.
Para comunicarse, los tags responden a peticiones o preguntas generando señales que a su vez no deben interferir con las transmisiones del lector, ya que las señales que llegan de los tags pueden ser muy débiles y han de poder distinguirse.

2.3.2. Tipos de Etiquetas

Las etiquetas RFID pueden ser activas, semipasivas o semiactivas y pasivas. Los tags pasivos no requieren ninguna fuente de alimentación interna, sólo se activan cuando un lector se encuentra cerca para suministrarles la energía necesaria. Los otros dos tipos

necesitan alimentación, típicamente una batería pequeña. Como las etiquetas pasivas son mucho más baratas de fabricar y no necesitan batería, la gran mayoría de las etiquetas RFID existentes en el mercado son del tipo pasivo.
A pesar de las ventajas en cuanto al costo de las etiquetas pasivas con respecto a las etiquetas activas son significativas, otros factores como la exactitud, funcionamiento en ciertos ambientes como cerca del agua o metal, que disminuye la exactitud, y la confiabilidad hacen que el uso de etiquetas activas empiece a aumentar considerablemente. Además, una de las principales desventajas de los dispositivos activos es el tamaño.

2.3.2.1. Tags pasivos

Los tags pasivos no poseen ningún tipo de alimentación eléctrica externa. La señal que les llega de los lectores induce una corriente eléctrica mínima que basta para operar el circuito integrado del tag, que permita generar y transmitir una respuesta. Las tarjetas contactless son de este tipo, ya que simplemente se les induce la corriente eléctrica, y con ello, se activa su antena interna.
La mayoría de tags pasivos utiliza *backscattering* o reflexión de las ondas, sobre la onda portadora recibida. Esto es, la antena ha de estar diseñada para obtener la energía necesaria para funcionar al mismo tiempo que para transmitir la respuesta por backscatter. Esta respuesta puede ser cualquier tipo de información, no sólo un código identificador.
Un tag puede incluir memoria no volátil, posiblemente con capacidad de escritura, por ejemplo, una memoria EEPROM - *electrically erasable programmable read-only memory*: ROM programable y borrable eléctricamente.
Los tags pasivos suelen tener distancias de uso práctico comprendidas entre los 10cm (norma ISO 14443) y llegando hasta unos pocos metros (normas EPC e ISO 18000 − 6) según la frecuencia de funcionamiento, el diseño y tamaño de la antena. Por su sencillez conceptual, se pueden fabricar por medio de un proceso de impresión común. Al carecer de autonomía energética, este dispositivo puede resultar muy pequeño, pueden incluirse en un sticker o insertarse bajo la piel.
En la práctica, las etiquetas pasivas tienen distancias de lectura que varían entre los 10 milímetros hasta cerca de 6 metros dependiendo del tamaño de la antena de la etiqueta, y de la potencia y frecuencia en la que opera el lector.

2.3.2.2. Tags Activos

Estos *tags* poseen su propia fuente de energía, que utilizan para dar corriente a sus circuitos integrados y propagar su señal al lector. Estos *tags* son mucho más fiables, sobre todos en distancias amplias, que los pasivos debido a su capacidad de establecer sesiones con el lector.

Gracias a su fuente de energía son capaces de transmitir señales más potentes que las de los *tags* pasivos, lo que les lleva a ser más eficientes en entornos dificultosos para la radiofrecuencia como el agua, incluyendo humanos y ganado, formados en su mayoría por agua; metal, contenedores y vehículos. También son efectivos a distancias mayores pudiendo generar respuestas claras a partir de recepciones débiles, lo contrario que los *tags* pasivos. Su principal desventaja es que suelen ser más grandes y más caros, y su vida útil es en general mucho más corta.

Muchos *tags* activos tienen rangos efectivos de cientos de metros y una vida útil de sus baterías de hasta 10 años. Algunos de ellos integran sensores de registro de temperatura y otras variables que pueden usarse para monitorizar entornos de alimentación o productos farmacéuticos. Otros sensores incluyen monitorización de humedad, vibración, luz, radiación, temperatura y componentes atmosféricos. Los *tags*, además de su mucho mayor alcance, tienen capacidades de almacenamiento mayores y la habilidad de guardar información adicional enviada por el transceptor.

Actualmente, los *tags* activos más pequeñas tienen un tamaño aproximado de una moneda. Muchos *tags* activos tienen rangos prácticos de diez metros, y una duración de batería de hasta varios años.

3. SOLUCIÓN PROPUESTA

4. ANÁLISIS Y DISEÑO

5. IMPLEMENTACIÓN

6. RESULTADOS

7. CONCLUSIONES

BIBLIOGRAFÍA

[Ind09] Electro Industria. (2009). Robótica en Chile. Cada vez más cerca de la automatización total. Disponible en http://www.emb.cl/electroindustria/articulo.mvc?xid=1269&tip=9 Consultado el 24 de Marzo de 2014.

[Osh14] OSHW-open source hardware. (2014). From Definition of Free Cultural Works. Disponible en http://freedomdefined.org/OSHW Consultado el 27 de Marzo de 2014.

[Del07] Antonio Delgado. (2007). ¿Qué es el hardware libre? Eroski Consumer Disponible en http://www.consumer.es/web/es/tecnologia/hardware/2007/11/20/171514.php. Consultado el 27 de Marzo de 2014.

[Car08] Carrasco Livio. (2008). Cancerbero: Prototipo de Control de Acceso utilizando Gestión de espacios mediante Dispositivos Contactless, Smartcard y Biometría. Escuela de Ingenieria Civil en Informática Universidad Austral de Chile.

[Vie06] Vielhauer C. (2006). Biometric User Authentication for IT Security: From Fundamentals to Handwriting. Springer.

[Way00] Wayman J.L. (2000). National Biometric Test Center - Collected Works Version 1.2 Disponible en http://www.engr.sjsu.edu/biometrics/nbtccw.pdf Consultado el 16 de Abril de 2014.

[Zha00] Zhang D. (2000). Automated Biometrics, Kluwer Springer.

[Way99] Wayman J.L. (1999). Technical Testing and Evaluation of Biometric Identification Devices. Kluwer Academic Publishers. Boston, MA, U.S.A, pp. 345 -368

[Bal97] Ballan M, Sakarya F.A. & Evans B.L. (1997). A Fingerprint Classification Technique Using Directional Images Systems and Computers. Signals, Systems & Computers. Vol. 1, pp. 101 – 104 Pacific Grove, CA USA

[Olg99] Patricio Olguín S. (1999). Sensores Biometricos. Revista electrónica de la escuela de ingeniería eléctrica - Facultad de Ingeniería - Universidad Central Venzuela. Disponible http://neutron.ing.ucv.ve/revista-e/No6/Olguin%20Patricio/SEN_BIOMETRICOS.html Consultado el 3 de Julio de 2014

[Rod97] Roddy A. & Stosz J., (1997). Fingerprint features-statistical analysis and system performance estimates Proceedings of the IEEE Disponible en http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=628710&isnumber=13673 Consultado el 3 de Julio de 2014

[Mal03] Maltoni D., Maio D., Jain A.K. & Prabhakar S. (2003). Handbook of Fingerprint Recognition Springer, New York, U.S.A