Implementación arquitectura general para la construcción de identificadores de huellas dactilares distribuidas

Guadalupe Morales, Nelson Rangel y Miguel Morales

G. Morales, N. Rangel y M. Morales
Universidad Politécnica de Victoria, Av. Nuevas Tecnologías 5902, Parque Científico y Tecnológico de Tamaulipas, Carretera Victoria - Soto la Marina Km. 5.5, Ciudad Victoria, Tam. México, C. P. 87138
CINVESTAV, Unidad Tamaulipas Laboratorio de Tecnologías De Información, Parque Científico y Tecnológico TECNOTAM -- Km. 5.5 carretera Cd. Victoria- Soto La Marina, C.P. 87130 Cd. Victoria, Tam.
nrangelv@upvictoria.edu.mx

M. Ramos.,V.Aguilera.,(eds.). Ciencias de la Ingeniería y Tecnología, Handbook -©ECORFAN- Valle de Santiago, Guanajuato, 2013.

Abstract

Currently various government agencies have fingerprints databases. Even with that information existing mechanisms do not have the ability to integrate it in order to identify persons using a fingerprint, either latent or from some other means, which usually are located in different geographic locations. In this paper we propose the design of an architecture that allows implementing a distributed system for the recognition of individuals through fingerprints databases. The suggested architecture provides a set of advantages over existing media, such as reducing the cost of hardware used, run on a conventional network connection reducing connection costs, make decentralized recognition on all connected databases, further more facing the scalability problem in communication and heterogeneity in hardware, operating systems and database managers.

13 Introducción

En instancias de gobierno existen procedimientos para la captura de huellas dactilares, por ejemplo, cuando una persona es consignada por algún delito, cuando se solicita una identificación oficial, sus huellas son tomadas, incluso al momento de registrar un neonato en el registro civil. Todos estos trámites, cuya documentación es obligatoria, han llegado a constituir una gran base de datos de huellas dactilares que abarca gran parte de la población del país. Sin embargo, el máximo potencial que se puede aprovechar derivado de las Bases de Datos de Huellas Dactilares (BDHD) aún se encuentra condicionado por factores físicos y tecnológicos como:

a) la distribución geográfica de las bases de datos.

b) la diversidad de manejadores para el control de huellas dactilares

c) la diversidad de los sistemas operativos a través de los cuales se accede a la información

d) los costos que implica en ocasiones usar equipo especializado.

Con el propósito de avanzar en la integración de BDHD, la investigación presentada en este artículo busca el desarrollo de una arquitectura que permita implementar un Sistema de Información Distribuida (SID) que integre diversas instancias donde se cuente con una BDHD a una búsqueda distribuida y descentralizada. La arquitectura contemplará dentro de las características esperadas del SID lo siguiente: 1) integración de BDHD dispersas; 1) heterogeneidad en el uso de BDHD; 2) heterogeneidad en el Sistema Operativo donde se implantará; 3) escalabilidad en la comunicación; 4) bajos costos en el hardware requerido para su implementación. El resto del documento se organiza de la siguiente manera. La Sección 13.1 presenta un estado del arte, donde se analizan los sistemas de reconocimiento de huellas dactilares. La Sección 13.2 describe formalmente el problema abordado en esta investigación. La Sección 13.3 expone la metodología usada, la cual contempla el análisis de diferentes estrategias para el reconocimiento de huellas dactilares, y el procesamiento y comunicación distribuido. La Sección 13.4 muestra la arquitectura resultado de la investigación. Finalmente, la Sección 13.5 contiene la discusión y conclusiones derivadas a partir de la información presentada en este documento.

13.1 Estado del arte

Actualmente existen grandes sistemas dedicados a la identificación de personas, tanto en el ámbito gubernamental como en el comercial. En Estados Unidos existe un sistema llamado IAFIS usado por el FBI. IAFIS cuenta con una base de datos de 74 millones de registros [10] lo que la convierte en la base de datos biométrica más grande del mundo [11]. La arquitectura del IAFIS está definida por 3 niveles; federal, estatal y local. La interoperabilidad de los niveles es completa desde federal hasta local, pero limitada para los demás niveles, es decir, un nodo de nivel local no puede iniciar una búsqueda en otro nivel local de otro estado un estado no puede iniciar una búsqueda a nivel de otro estado[12].

El gobierno mexicano cuenta también con un sistema llamado Sistema Automatizado de Identificación del Registro Nacional de Huellas Dactilares abreviado AFIS, por sus siglas en inglés, utilizado para la localización de personas desaparecidas y criminales. El AFIS está integrado a una plataforma disponible en los 32 estados de la republica llamada Plataforma México [13]. Al año 2009 se contaba con un registro de más de 4.8 millones de personas recopiladas por las procuradurías generales de justicia de los estados, lo consejos de seguridad estatal y los centros de readaptación social [14]. De los registros de huellas correspondientes más de 300 miles son registros palmares. La principal desventaja que se tiene con este sistema es que el registro se limita a personas con antecedentes penales, personal de corporaciones policiacas o del ejército limitando así el límite los resultados.

Existe una solución comercial llamada ExpressID AFIS creada por una compañía Eslovaca con aplicaciones más generales como bancarias, civiles, control de fronteras, entre otros [15]. Ofrece la posibilidad de trabajar en un solo servidor o con una arquitectura multiservidor, además de una aplicación cliente para contactar el servidor. Es una aplicación multiplataforma y ofrece soporte para múltiples SMBD (Sistemas Manejadores de Bases de Datos).

La Tabla 13 presenta un resumen comparativo de lo esperado por la arquitectura propuesta en este documento, al implementar un SID, contra SID existentes. En esta tabla se analizan los sistemas de acuerdo a los criterios: a) Distribuido, se identifican usando varios núcleos de procesamiento; b) Descentralizado, cada núcleo de procesamiento es independiente en la búsqueda; c) Capacidad, se refiere al número de registros de huellas dactilares que contiene; d) Heterogeneidad, se refiere a la habilidad para soportar diferentes BDs o SOs; e) Interoperabilidad, o bien la capacidad para interactuar con otros sistemas de identificación de huellas dactilares; f) Escalable, es decir que puede crecer el repositorio de BDs o la cantidad de nodos que se agreguen al sistema; y g) Equipo Especializado, que tiene requerimiento en hardware de equipo que no es de uso común o convencional.

Tabla 13 Comparación entre diversos sistemas identificadores automáticos de huellas dactilares. La capacidad está dada en millones de registros (N.A. significa "No Aplica")

	IAFIS(FBI)	AFIS(Mex)	ExpressID AFIS	Arquitectura Propuesta
Distribuido	✓	✓	✓	✓
Descentralizado	✓	✗	✗	✓
Capacidad	74 m.	4.5 m.	3+ m.	N.A.
Heterogeneidad en BDs	✓	✗	✓	✓
Heterogeneidad en SOs	✗	✗	✓	✓
Interoperabilidad	✓	✓	✗	✓
Escalable	✓	✓	✓	✓
Equipo Especializado	✓	✗	✓	✗

Dada la información presentada en la Tabla 1 se puede observar que la arquitectura mejoraría los sistemas ya existentes al incluir de forma conjunta la Heterogeneidad en BDs y SOs, y la Interoperabilidad. En la siguiente sección se describe de manera formal la problemática a resolver para poder dar origen a la arquitectura distribuida propuesta en este documento.

13.2 Descripción de la Problemática

A partir de la comparación de las características de diversos sistemas existentes dentro del reconocimiento de huellas dactilares y detectar sus fortalezas y debilidades, se plantea una propuesta que busque aportar soluciones en las debilidades de los ejemplos discutidos, como lo son buscar una opción a la centralización de la información y el procesamiento, integración de repositorios de datos de manera fácil, lograr tener repositorios de datos que incluyan en mayor medida los registros de huellas dactilares ya existentes en las diversas instancias de gobierno del país y así ampliar la cobertura de los sistemas de reconocimiento actuales.

Por lo tanto, la problemática a resolver quedaría describa formalmente como: es posible diseñar una arquitectura que especifique las componentes necesarias, y las interacciones entre ellas, para implementar un Sistema de Información Distribuido que permita reconocer individuos a través de sus huellas dactilares tomando en cuenta las siguientes restricciones:

1) Sea capaz de integrar BDs heterogéneas

2) Sea capaz de incorporar fácilmente una nueva base de datos

3) Pueda funcionar en diferentes SOs

4) El procesamiento de huellas dactilares se lleve a cabo de manera distribuida

5) Sea escalable, y cuente con un sistema de comunicación ligero que permita transmitir información a todas las bases de datos.

Las ventajas que se lograrán al desarrollar dicha arquitectura serán que los sistemas implementados por medio de ella puedan ser ejecutados en computadoras de convencionales y redes convencionales, reduciendo así costos de hardware y conexión.

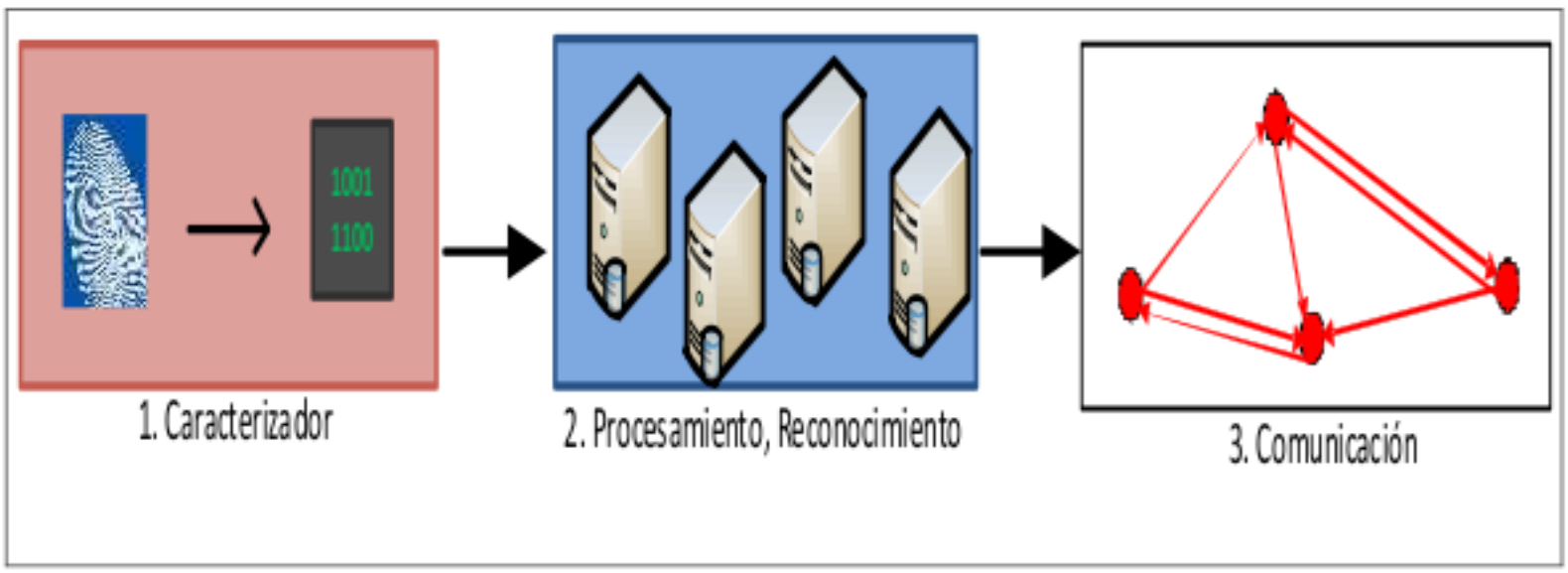
13.3 Metodología usada

Con el propósito de poder definir la arquitectura deseada, se siguió la metodología dividida en 3 etapas mostradas en la Figura 13 En la etapa 1 se plantea el desarrollo del componente de la arquitectura que se hará cargo del reconocimiento del individuo.

Una vez resuelto este problema, se procederá a encontrar el mejor modelo de procesamiento distribuido que permita implementar la estrategia de reconocimiento, la identificación de dicho modelo constituirá un segundo conjunto componentes de la arquitectura.

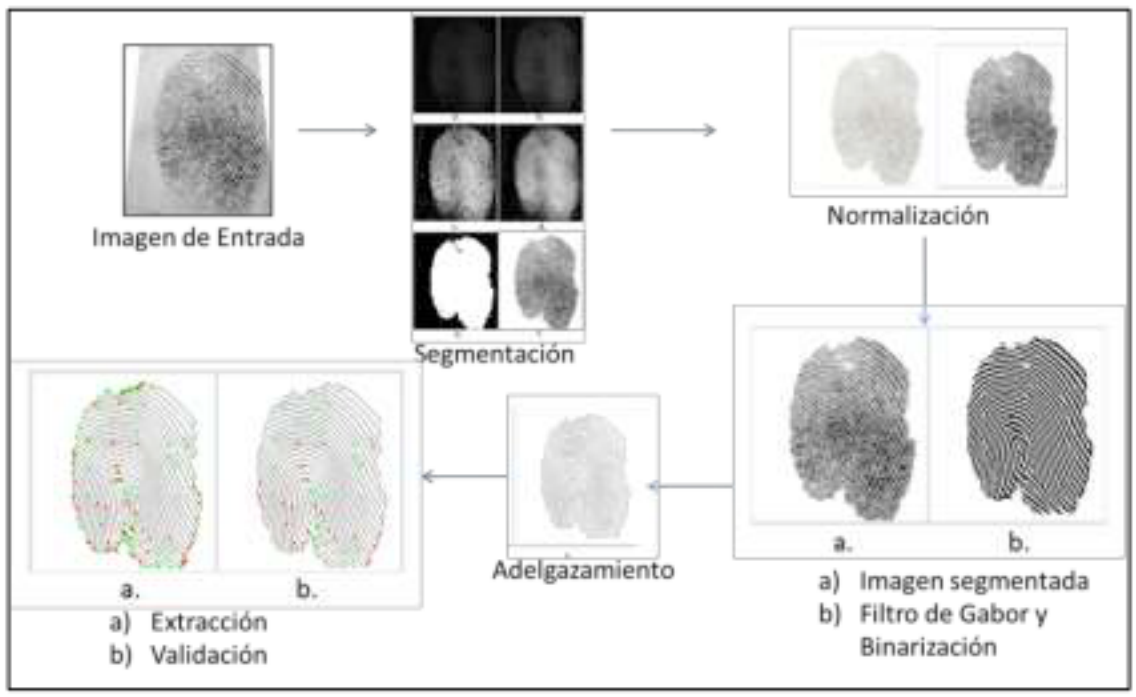
Finalmente, en la etapa 3 se concentrará la tarea de ajustar el modelo de comunicaciones al modelo de procesamiento identificado en la etapa 2. El detalle sobre el desarrollo de estas etapas se muestra en el resto de esta sección.

Figura 13 Esquema que muestra la arquitectura propuesta con los diversos componentes propuestos



Caracterización de las Huellas Dactilares:La arquitectura a desarrollar en este artículo debe definir componentes para caracterizar las huellas dactilares de un individuo, de tal manera que permitan su posterior identificación. En la Figura 13.1 se muestran los componentes que, derivados de la literatura [5 6 9], la arquitectura debe incluir para llevar a cabo el reconocimiento del individuo.

Figura 13.1 Componentes para la caracterización del individuo



La tarea de reconocimiento de un individuo por su huella dactilar empieza por la caracterización de la misma.

El primer componente que debe considerar en la arquitectura para esta tarea es la representación de la huella dactilar, cómo será almacenada en el equipo.

En la literatura es muy común almacenar la huella dactilar a través de una imagen de la misma, sin embargo esta requiere un preprocesamiento para que pueda servir en el proceso de reconocimiento.

El segundo componente, que inicia el preproceso hecho a la imagen de entrada que contiene la huella dactilar, comenzará con una *Segmentación*, donde se busca aislar la información de interés de la imagen, el método más comúnmente usado para la segmentación es realizado mediante varianza [1]. Así como algunos otros métodos compuestos que utilizan una serie de filtros como el promedio o suavizado como base para la segmentación [4].

El método seleccionado para esta arquitectura está relacionado también con el filtro promedio combinado con gradiente propuesto en [3], dado que es capaz de realizar la segmentación aún en imágenes con ruido y poca calidad.

El siguiente componente a definir después de que la imagen ha sido segmentada es para realizar un realzado de las crestas encontradas en las huellas dactilares, esto también es conocido como mejoramiento de la imagen. Sin embargo, dependiendo de la estrategia es posible requerir algún preprocesamiento extra.

Para propósito del diseño de la arquitectura se contemplaron dos métodos en el análisis: a) un método basado en la transformada de Fourier [5], que es conocido por ser efectivo con imágenes de baja calidad; b) el método propuesto por Hong et al. [6], el cual realiza un realzado de imágenes normalizadas de huellas dactilares mediante el filtro de Gabor de acuerdo a parámetros extraídos del bloque que está mejorando, estos dos parámetros son la estimación local de orientación y de frecuencia.

El método elegido para esta arquitectura es el algoritmo de Hong, el cual, por establecer como parámetros las estimaciones de frecuencia y de orientación, se adapta a las condiciones locales de las imágenes, logrando una mejor reconstrucción incluso de secciones entrecortadas de las crestas.

Debido a que el componente para el mejoramiento fue el algoritmo de Hong se necesita agregar un filtro extra antes de aplicar este algoritmo llamado normalización [6], la normalización es usada para reducir el efecto de las variaciones de colores de escala de grises a través de los valles y crestas.

Posterior al mejoramiento de la imagen, es necesario que la imagen contenga valores blanco o negro, por lo cual se somete a un proceso llamado binarizado donde, a partir de un umbral se decide si un pixel en la escala de grises se toma como blanco o como negro.

Después de la binarización se realizará un proceso de adelgazamiento con el cual las líneas obtenidas de la imagen binarizada se reducirán para que midan un pixel de ancho.

Una vez con la imagen adelgazada, también conocida como esqueleto, se someterá a un proceso llamado Crossing Number [2], técnica usada para la identificación de minucias, en donde cada pixel de color negro es examinado para ver si sus 8 pixeles vecinos más cercanos son de color también negro, el numero obtenido determinara este pixel es una minucia de tipo fin de cresta, si el número es 1, si el pixel es de tipo bifurcación, si el número es 3. Cualquier otro número obtenido no es de interés.

Después de la identificación de las minucias, es necesaria una validación donde se verificara si una minucia detectada es falsa o no.

La tarea de reconocimiento realizada en este módulo se realizará a partir de un vector de características, que a su vez contará con vectores que representaran minucias. Cada vector de minucias contendrá primero el tipo de minucia, los valores *i,j* de las coordenadas donde se encontró la minucia, el ángulo de la minucia, así como los valores *i,j* de los 10 pixeles vecinos de la minucia. A partir de este vector se realizara el reconocimiento basado en [9], donde se buscara una minucia llamada minucia referencia.

Esta minucia referencia será usada para hacer una serie de rotaciones y traslados del patrón de minucias base contra el de minucias de prueba. De esta manera se espera encontrar un número de minucias coincidentes dentro de un margen de error, que permitan establecer si hay coincidencia o no entre los patrones comparados.

Arquitectura de procesamiento:Esta etapa de la metodología se enfoca en el cómo se implementará la estrategia de reconocimiento de individuos, enfatizando en el aspecto de qué modelo de procesamiento es el más adecuado para desarrollarse.

Para poder llevar a cabo de forma adecuada esta tarea es necesario considerar las problemáticas a abordar en la investigación referentes a: ser capaz de integrar BDs heterogéneas, y poder funcionar en diferentes SOs.

En el ámbito de procesamiento distribuido muchos autores han analizado arquitecturas que nos permiten procesar información en múltiples formas. En una clasificación presentada en [16] se establecen tres categorías de paradigmas, 1) granjas de procesadores, basada en la replicación de trabajos independientes, 2) descomposición geométrica, la cual se apoya en paralelismo y estructuras de datos y 3) paralelismo algorítmico, el cual se traduce en un flujo de datos.

De esta clasificación el paradigma número 1 no se acopla a los requerimientos perseguidos en la arquitectura que se desea diseñar por el simple hecho de que no es aceptable trabajar con granjas de procesadores, los paradigmas 2 y 3 necesita de descomposición de los datos usados, pero es un requerimiento trabajar con estructuras de datos las cuales no se deben dividir por motivos de privacidad, por lo tanto quedan descartados.

Una segunda clasificación la encontramos en [17] donde los estudios de autor arrojan las siguientes clasificaciones; 1) Pipelining y aplicaciones basadas en anillos, 2) divide y vencerás, 3) maestro esclavo y 4) aplicaciones de autómatas celulares, en el caso particular del primer paradigma se centra en la ejecución de taras una tras otra.

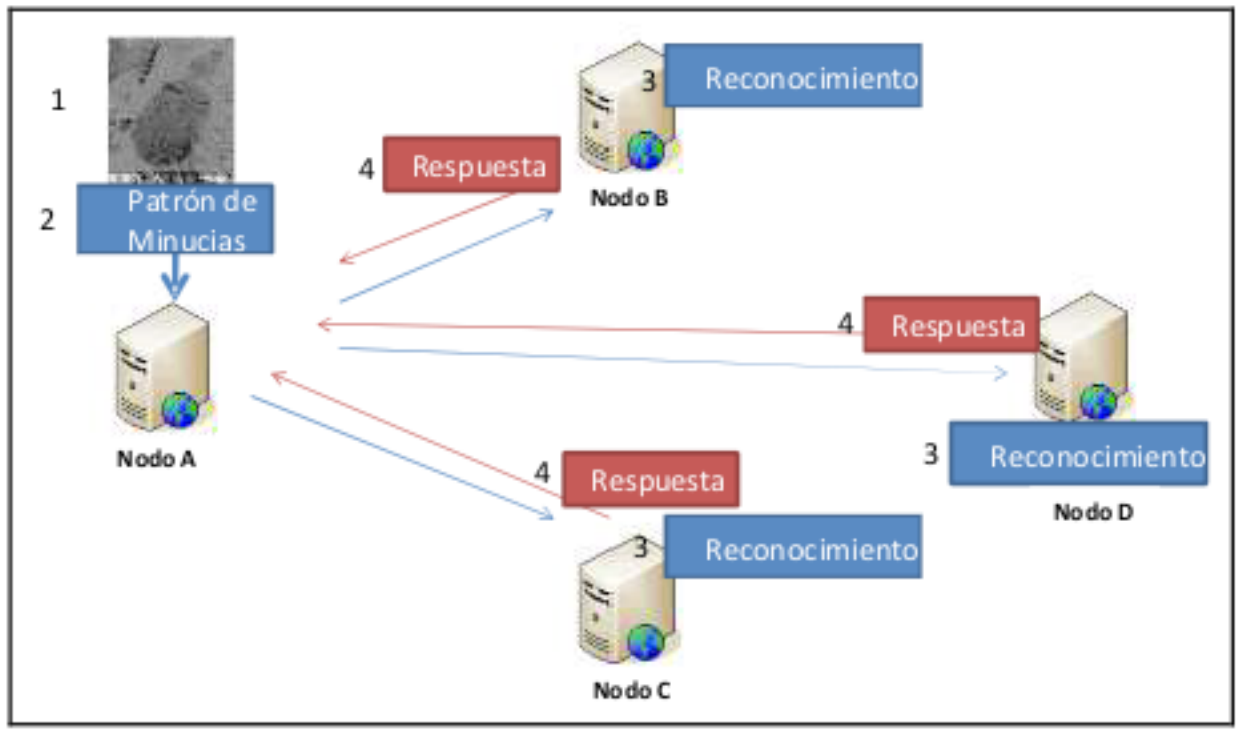
En nuestro caso la ejecución del proceso de reconocimiento debe ser simultaneo para cada nodo, el paradigma 2, queda descartada, por motivos de privacidad al necesitar dividir la información, el paradigma 3 parece tener cualidades para acoplarse a la arquitectura que se requiere, pero tiene como inconvenientes que las tareas realizadas primero necesitan ser centralizadas por un maestro el cual divida una operación que deberá de ser resuelta en secciones por sus esclavos, para nuestro caso la centralización y división de tareas y datos no es posible, por último las aplicaciones autómatas celulares tiene propósitos no perseguidos por la arquitectura.

Como otra alternativa podemos considerar el paradigma cliente-servidor, en el cual la comunicación se realiza usualmente con llamadas a procedimientos remotos, y son usados para soportar servicios distribuidos [18].

Para propósitos de nuestra arquitectura el paradigma cliente servidor resuelve la problemática de poder trabajar en SOs heterogéneos así como diversas BD, permitiendo el diseño de componentes en un lenguaje de programación de propósito general y multiplataforma, como lo es java. El paradigma cliente servidor permite también respetar políticas de privacidad que restrinjan la partición y difusión de datos además de que factores físicos como la geografía no afectan el accionar del paradigma.

La Figura 13.2 muestra un esquema que describe el modelo de procesamiento Cliente-Servidor aplicado al reconocimiento de individuos. El primer paso es que un nodo dé origen a la petición de reconocimiento, el nodo cliente, (ver Nodo A) lleve a cabo la caracterización, es decir, la imagen de huella dactilar se introduce al módulo de extracción de características. Una vez caracterizado, de acuerdo al modelo de procesamiento cliente-servidor, el patrón de las minucias es enviado y transportado a nodos restantes para su reconocimiento. La tarea de reconocimiento consiste en que el patrón de huellas dactilares recibido por cada nodo se debe contrastar contra los patrones derivados de las BDHD encontradas en ellos, y se debe responder si existe alguna coincidencia o no, regresando al nodo origen la respuesta.

Figura 13.2 Descripción del proceso de petición de reconocimiento



Arquitectura de comunicación:El objetivo en esta etapa es analizar estrategias de comunicación entre los diferentes nodos de procesamiento, de tal manera que se puedan resolver los problemas de escalabilidad y comunicación ligera.Existe un mecanismo para resolver la necesidad de enviar mensajes a todos los nodos conectados a una red, a esta operación se le conoce como multicast de capa de aplicación.

Entre las estrategias con las que se puede desarrollar la tarea de comunicación se encuentran la multicast a nivel de aplicación [19 20], los cuales independientemente de la red implementan la funcionalidad de multicast exclusivamente entre hosts, también existe el multicast con jerarquías [21] que plantea jerarquías en capas las cuales permiten dividir el envío de información de acuerdo al planteamiento de las capas, y la Difusión Epidémica [22], la cual es una estrategia aleatoria de comunicación basada en la teoría Epidemiológica, que no es más que es el estudio de la propagación de una enfermedad o infección en términos de individuos infectados/no infectados y sus razones de cambio [7], es utilizada comúnmente para lograr una transferencia de información rápida y ligera. Entre las estrategias mencionadas cabe resaltar que todas ofrecen una alta escalabilidad, sin embargo en materia del número de mensajes enviados podemos hallar variaciones. El método de multicast clásico puede generar un tráfico considerable en la red porque no implementa estrategias que minimicen el número de mensajes enviados, para el caso de multicast jerárquico se logra una disminución del tránsito de la red de acuerdo a las jerarquías preestablecidas en el diseño de la red, sin embargo la implementación de jerarquías no sería viable en para la arquitectura propuesta por el hecho de que hay que tener definido un numero de nodos y su ubicación para el diseño de la misma, la arquitectura propuesta debe contemplar una constante adición de bases de datos, y por lo tanto de nodos, además en principio el número de nodos y sus ubicaciones esta en incertidumbre.Para el caso de la difusión epidémica, la naturaleza aleatoria de la estrategia permite comenzar con un número pequeño de mensajes independientemente del número de nodos contemplados en la red, asegurando economía en la conexión, además de tener una baja latencia, dado el tiempo para que el mensaje llegue se propague a la totalidad de la red es logarítmico.El diseño de la arquitectura basada en difusión epidémica se explica a continuación.

En la Figura 13.3 se ejemplifica el accionar de la difusión epidémica, la difusión de la información comienza con un nodo infectado (Figura 4.a), que representará el nodo que inicia una petición de reconocimiento, el cual infectara a un número *b* nodos elegidos de manera aleatoria. El total de nodos en el sistema será definido como *(n+1)* donde, inicialmente, n es el número de elementos no infectados y 1 es agregado por el primer elemento que tendrá la infección. Los estados que puede tener un nodo son infectado, representado con *x*, y no-infectado, representado con *y*. En cada tiempo T los individuos pueden tener dos estados, infectado o no infectado, después de que un individuo cambia su estado a infectado permanece infectado [8].

Figura13.3 Ejemplo de difusión epidémica

Después de la infección de los primeros *b* nodos, todos los nodos que ahora estén infectados, es decir, el nodo que inicio la infección y los *b* nodos recién infectados, volverán a infectar cada uno a *b* nodos más (Figura 13.3.b). Este proceso se repetirá un tiempo *t* el cual, tendrá un límite *c*, esperando que al llegar a la última iteración el mensaje sea entregado a todos los nodos conectados (Figura 13.3.c).

13.4 Resultados

Como resultado de la integración de los 3 componentes mencionados se obtuvo la arquitectura mostrada en la Figura 13.3, la cual permitirá integrar de manera bases de datos diversas a procesos de reconocimiento. Las principales características que se identifican en un Sistema Distribuido implementado a partir de la arquitectura propuesta son las siguientes:

Identificación de individuos. Con el uso de los algoritmos de caracterización, reconocimiento y la arquitectura mencionados, la identificación de individuos es posible en todos los nodos de la red.

Baja latencia. Con el método elegido de difusión epidémica se logra una baja latencia dado que el tiempo estimado para la difusión de mensaje al total de nodos conectados es logarítmico.

Escalabilidad. La difusión epidémica permite tener sistemas de alta escalabilidad, contempla la inclusión de un gran número de nodos sin afectar el rendimiento de la comunicación.

Confiabilidad. La difusión epidémica permite establecer estadísticamente que solo un número muy pequeño de nodos quedaran sin recibir el mensaje.

Comunicación ligera. El número de mensajes enviados usando el método evolutivo será también logarítmico por lo cual tránsito en la red será optimizado. Permita además conectar nodos al sistema en redes convencionales.

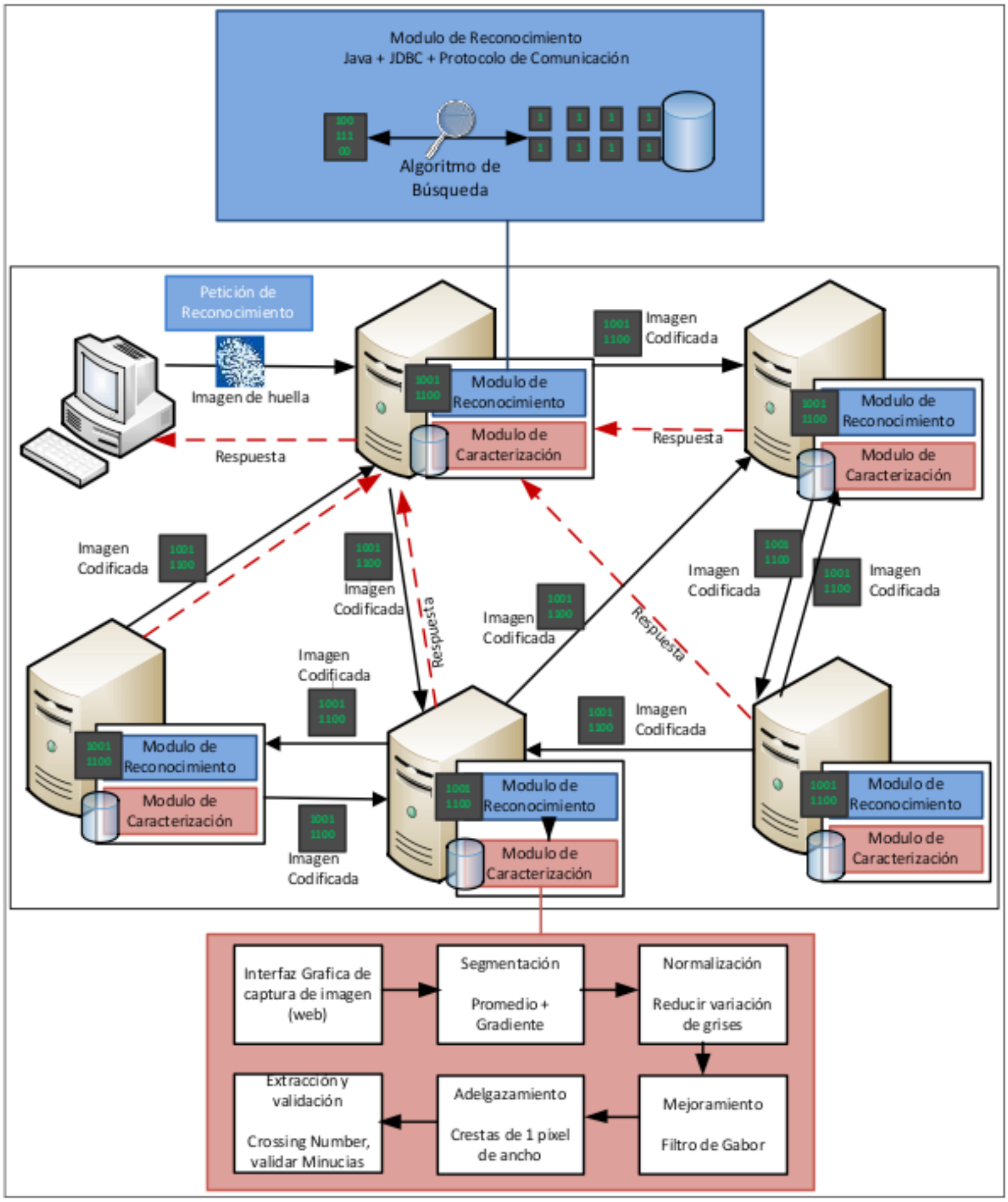
Bajo costo. La arquitectura puede incluir computadoras convencionales en como nodos reduciendo el costo de hardware y funcionar también en redes convencionales.

Heterogeneidad en BD. La comunicación con la base de datos se establece mediante el uso del lenguaje de programación java, y con el uso JDBC se logra interactuar con una variedad de bases de datos.

Privacidad. La implementación del reconocimiento en el modelo cliente servidor permite que las bases de datos sean procesadas sin difundir elementos de las bases de datos.

Limitaciones geográficas. Se podrán integrar bases de datos en diversas ubicaciones con la única condición de que se cuente con una conexión de red.

Figura 13.4 Esquema de la arquitectura propuesta con todos los módulos integrados



13.5 Conclusiones e investigación futura

Dentro de este documento se presenta el diseño de una arquitectura que permite describir cómo implementar un Sistema Distribuido para el Reconocimiento de Huellas Dactilares (SDRHD).

La arquitectura contempla elementos como bases de datos heterogéneas, sistemas operativos heterogéneos, escalabilidad, comunicación ligera, privacidad, bajo costo en hardware, entre otros.

Se distinguen tres componentes principales que todo SDRHD debe considerar en su implementación, los cuales son, caracterización de huellas dactilares, reconocimiento de individuos, y comunicación entre nodos de procesamiento físicamente separados.

Para lograr la tarea de caracterización se propone el uso de métodos cómo [3 4 5 6 9], los cuáles en conjunto resuelven las tareas de segmentación, normalización, mejoramiento de la imagen, adelgazamiento, detección y validación de minucias.El componente de reconocimiento involucró decidir el modelo de procesamiento adecuado para el problema. En este caso, el elemento más adecuado para la arquitectura que se diseñó fue un modelo cliente-servidor, debido a que es apta para trabajar con servicios distribuidos, respetar políticas de privacidad ya que no requiere la distribuciones datos, además de que nos permite operar en diversos SOs y BD . Finalmente el componente de comunicación que nos permitía abordar problemas como la necesidad de una comunicación ligera, escalabilidad y confiabilidad fue la difusión epidémica, y la razón fue por que, basándonos en la naturaleza estadística de la estrategia de comunicación epidémica, podemos decir que la arquitectura es apta para trabajar en redes las cuales no cuenten con un gran ancho de banda debido a que envía un número pequeño de paquetes por cada nodo, además de que estadísticamente es muy poco probable que existan nodos los cuales no reciban paquetes, por último la arquitectura permite la adición constante de nodos sin ver afectado el rendimiento. Como trabajo futuro queda el implementar el SDRHD tomando la arquitectura propuesta, y analizar efectos en el sistema derivado de cambios pequeños en su diseño.

13.6 Referencias

Mehtre, B. M. (1993). Fingerprint image analysis for automatic identification.
Machine Vision and Applications, 6(2), 124–139.

Sudiro, S.A., Paindavoine, M. ; Kusuma, T.M. (2007),Simple Fingerprint Minutiae Extraction Algorithm Using Crossing Number On Valley Structure. 2007 IEEE Workshop on Automatic Identification Advanced Technologies , 41 – 44.

M. E. Ruiz Echartea (2011). Sistema de Identificación Automática de Huellas Dactilares. Universidad Politécnica de Victoria. Ciudad Victoria: México.

Asker M. Bazen and Sabih H. Gerez (2001). Segmentation of Fingerprint Images. ProRISC 2001 Workshop on Circuits, Systems and Signal Processing.

A.J. Willis and L. Myers (2001). A cost-effective fingerprint recognition system for use with low-quality prints and damage fingertips. Pattern Recognition, 34(2), 255- 270.
Hong, L., Wan, Y., and Jain, A. K. (1998). Fingerprint image enhancement: Algorithm and performance evaluation. IEEE Transactions on Pattern Analysis and Machine Intelligence, 20, 8, 777–789.

U.S. Department of Health and Human Services (2006), Principles of Epidemiology in Public Health Practice. Recuperado de http:// cdc.gov/osels/scientific_edu/ss1978/SS1978.pdf

L. Bailey, K. Vardulaki, J. Langham, D. Chandramohan (2006). Introduction to epidemiology, Open University Press.

Anil Jain, Lin Hong, Sharath Pankanti, Ruud Boll (1997). An Identity Authentication System Using Fingerprints. Proceedings of the IEEE, 85. 1365 – 1388.

FBI Quality Improvement Unit Statistical Trending, Analysis & Reporting Group (2013). IAFIS Facts Sheet. The Federal Boureou of Investigation. Recuperado de http://fbi.gov/about-us/cjis/fingerprints_biometrics/iafis/iafis_facts

FBI (2013), IAFIS. The Federal Boureou of Investigation. Recuperado de http://fbi.gov/about-us/cjis/fingerprints_biometrics/iafis

Kristi Mayo (2008). AFIS Interoperability. Evidence Technology Magazine, 6(1). Recuperado de http://evidencemagazine.com/index.php?option=com_content&task=view&id=89&Itemid=49

Policía Federal (2012). Informe de Rendición de Cuentas 2006-2012. Recuperado de http://ssp.gob.mx/portalWebApp/ShowBinary?nodeId=/BEA%20Repository/1206068//archivo

Secretaria de Seguridad Pública (2009). Tercer informe de labores, Recuperado de http://.ssp.gob.mx/portalWebApp/ShowBinary?nodeId=/BEA%20Repository/550126//archivo

Innovatrics (2012). Innovatrics ExpressID AFIS Datasheet. Recuperado de http://download.innovatrics.com/download/innovatrics_EXPRESSID.pdf

D. Pritchard (1988). Mathematical Models of Distributed Computation. In Proceedings of OUG-7, Parallel Programming on Transputer Based Machines (25-36). Amsterdam, Springfield : IOS.

P. B. Hansen (1993). Model Programs for Computational Science: A Programming Methodology for Multicomputers. Concurrency: Practice and Experience, 5(5), 407-423.

Luis Silva, Rajkumar Buyya (1999). Parallel Programming Paradigms, High Performance Cluster Computing: Programming and Applications (4-27), Rajkumar Buyya: Prentice Hall.
Y. Chawathe (2000). Scattercast: An Architecture for Internet Broadcast Distribution as an Infrastructure Service. University of California, Berkeley.

Y.-H. Chu, S. G. Rao, and H. Zhang (2002). A Case for End System Multicast. IEEE Journal on Selected Areas in Communications, 20(8), 1456-1471.

Suman Banerjee, Bobby Bhattacharjee, Christopher Kommareddy, Scalable Application Layer Multicast, SIGCOMM'02.

Colmenares G. Luis E. y Solís L. Eder (2012). Una aproximación epidémica para el problema de direccionamiento de consultas semánticas en redes p2p estructuradas. Revista de ingeniería eléctrica, electrónica y computación, 10, 16-21.