CAPÍTULO

SISTEMA AUTOMATIZADO DE IDENTIFICACIÓN DE HUELLAS DACTILARES (AFIS)

KENNETH R. MOSES

AUTORES COLABORADORES:
PETER HIGGINS, MICHAEL MCCABE,
SALIL PRABHAKAR Y SCOTT SWANN

CONTENIDOS

3 **6.1 Introducción**

10 **6.2 Operaciones de AFIS**

16 **6.3 Estándares**

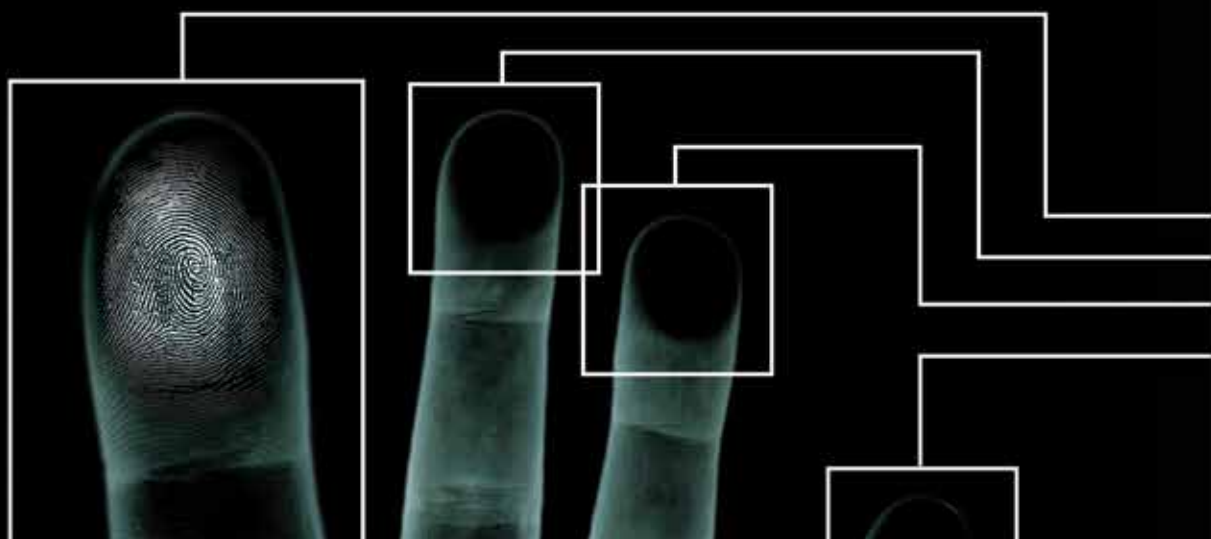
22 **6.4 Digitalización y Procesamiento de Huellas Dactilares**

35 **6.5 Resumen**

36 **6.6 Revisores**

36 **6.7 Referencias**

37 **6.8 Información adicional**



CAPÍTULO 6

SISTEMA AUTOMATIZADO DE IDENTIFICACIÓN DE HUELLAS DACTILARES (AFIS)

KENNETH R. MOSES

AUTORES COLABORADORES: PETER HIGGINS, MICHAEL MCCABE, SALIL PRABHAKAR Y SCOTT SWANN

6.1 Introducción

Antes de la revolución industrial y las migraciones masivas a las ciudades, las poblaciones vivían principalmente en las comunidades rurales, donde todos se conocían y había poca necesidad de identificación. De hecho, no había fuerzas policiales ni centros penitenciarios y había muy pocos tribunales. A medida que las ciudades se llenaron de gente, los índices de criminalidad se dispararon y los delincuentes florecieron en un mar de anonimato. La prensa se deleitaba con historias de la ilegalidad, las legislaturas respondieron rápidamente con más leyes y penas más severas (especialmente en el caso de reincidentes), y los departamentos de policía estaban a cargo de identificar y detener a los malhechores. Los sistemas de identificación—galería de rogues, antropometría, el "retrato hablado" de Bertillon, y el sistema de Henry—surgieron y rápidamente se esparcieron por todo el mundo a finales del siglo 19 y principios del 20.

El final de la década de 1960 y el principio de 1970 fueron testigos de otra época de agitación civil y un aumento sin precedentes en los índices de criminalidad, pero ésta coincidió con el desarrollo del chip de silicio. Los desafíos inherentes a los sistemas de identificación parecían ya hechos para las soluciones del procesamiento automático de datos, y el AFIS—Sistema Automatizado de Identificación de Huellas Dactilares—nació.

Durante este mismo período, la RAND Corporation, que operaba bajo una concesión nacional, publicó el Criminal Investigative Process (Greenwood et al., 1975), un amplio estudio y crítica del proceso por el que los crímenes son resueltos—o no. Generalmente, crítico de métodos tradicionales utilizados por los detectives, el estudio pone cualquier esperanza de mejorar en las pruebas físicas de impresiones generales y latentes en particular. En un estudio complementario, Joan Petersilia concluyó que:

> No importa que tan competente sea el técnico en evidencia durante el desempeño de su trabajo, recabar evidencias físicas en el lugar de los hechos es inútil a menos que dicha evidencia pueda ser procesada y analizada correctamente. Debido

> a que las huellas dactilares son por mucho la evidencia física recuperada con mayor frecuencia, hacer que ese sistema de análisis de dichas huellas sea efectivo contribuirá con un mayor éxito en la identificación de delincuentes mediante el uso de evidencia física. (Petersilia, 1975, pág. 12).

Aunque la nueva tecnología ya estaba en desarrollo en la Oficina Federal de Investigaciones (FBI), era un movimiento popular a nivel local y estatal que verdaderamente pondría a prueba la teoría de Petersilia.

6.1.1 Necesidad de automatización

En 1924, la División de Identificación del FBI se estableció por mandato de la ley de asignación de presupuestos del Congreso de los Estados Unidos al Departamento de Justicia. La División de Identificación fue creada para proporcionar un repositorio central de información de identificación penal para las fuerzas del orden público en todo Estados Unidos. La colección original de registros de huellas dactilares contenía 810,188 registros. Después de su creación, cada año se añadían cientos de miles de registros nuevos a esta colección, y para la década de 1960 el archivo criminal del FBI había aumentado a unos 15 millones de individuos. Eso era además de los 63 millones de registros en el archivo civil, muchos de los cuales eran el resultado de incorporaciones militares provenientes de la Segunda Guerra Mundial y el conflicto con Corea.

Casi todos los archivos criminales de las 15 millones de personas contenían la impresión decadactilar en las tarjetas para dar un total de 150 millones de huellas dactilares individuales. Los registros que llegaban se clasificaban de forma manual y se buscaban en este archivo utilizando el sistema de clasificación de Henry modificado por el FBI. Aproximadamente 30,000 tarjetas se buscaban diariamente. El tiempo y los recursos humanos para llevar a cabo este trabajo diario continuaban creciendo. Conforme una tarjeta ingresaba al sistema, una clasificación preliminar de patrón bruto se asignaba a cada huella dactilar por parte de los técnicos. Los técnicos podían completar aproximadamente 100 tarjetas de huellas dactilares por hora. Obviamente, como el tamaño del archivo criminal y la carga de trabajo diario incrementaron, la cantidad de recursos necesarios siguió creciendo. Finalmente, se añadieron extensiones de clasificación para reducir la parte del expediente que debía ser buscada y cotejada con cada tarjeta. No obstante, el sistema manual utilizado para la búsqueda y correspondencia de las huellas dactilares se acercaba al punto de ser incapaz de manejar la carga de trabajo diaria.

Aunque los organizadores de tarjetas perforadas podrían reducir el número de tarjetas con huellas dactilares necesarias para ser examinadas sobre la base de la clasificación de patrones y otros parámetros, todavía era necesario que los examinadores humanos inspeccionaran cada tarjeta de huellas dactilares en la lista de candidatos. Era necesario un nuevo paradigma para detener el incremento en la cantidad de recursos humanos necesarios para procesar dichas solicitudes de búsqueda. Se necesitaba un nuevo enfoque automatizado para (1) extraer cada imagen de huella dactilar de una tarjeta decadactilar, (2) procesar cada una de estas imágenes para producir una plantilla de tamaño reducido con información característica, y (3) buscar en una base de datos para producir automáticamente una lista muy reducida con coincidencias de probables candidatos (Cole, 2001, pág. 251-252).

6.1.2 Desarrollo temprano del AFIS

A principios de 1960, el FBI en los Estados Unidos, el Ministerio del Interior del Reino Unido, la Policía de París en Francia y la Policía Nacional de Japón iniciaron proyectos para desarrollar sistemas automatizados de identificación de huellas dactilares. La idea central de esta investigación era utilizar computadoras digitales electrónicas emergentes para ayudar o sustituir los procesos de trabajo intensos de clasificar, buscar y empatar coincidencias de las tarjetas decadactilares utilizadas para la identificación personal.

6.1.3 Iniciativa AFIS del FBI

Para 1963, el Agente Especial Carl Voelker de la División de Identificación del FBI se dio cuenta de que la búsqueda manual en el archivo criminal no seguiría siendo viable durante mucho más tiempo. En un intento de resolver este problema, buscó la ayuda de los ingenieros Raymond Moore y Joe Wegstein del Instituto Nacional de Estándares y Tecnología (NIST)[1]. Después de describir su problema pidió asistencia en la automatización del proceso de identificación de huellas dactilares del FBI.

[1] El NIST era conocido como la Oficina Nacional de Estándares cuando el FBI se encontró con Moore y Wegstein.

Los ingenieros del NIST primero estudiaron los métodos manuales utilizados por los técnicos en huellas dactilares humanas para hacer las identificaciones. Estos métodos se basaban en la comparación de minucias (es decir, finales y bifurcaciones de las crestas) en las crestas de la huella dactilar. Si las minucias de dos huellas dactilares se declaraban topológicamente equivalentes, ambas huellas dactilares eran determinadas como idénticas—es decir que se habían registrado a partir del mismo dedo de la misma persona. Después de esta revisión y después de estudiar los problemas adicionales inherentes al proceso de entintado, creían que una solución computarizada para hacer coincidir y emparejar automáticamente las minucias podría desarrollarse y ésta podría funcionar de manera similar a las técnicas utilizadas por los examinadores humanos para hacer identificaciones de huellas dactilares. Pero para lograr este objetivo, tres tareas principales tenían que llevarse a cabo. Primeramente, se tuvo que desarrollar un escáner que pudiera leer de forma automática y capturara electrónicamente la imagen de la huella entintada. En segundo lugar, era necesario detectar e identificar de forma exacta y consistente las minucias que existían en la imagen capturada. Por último, fue necesario desarrollar un método para comparar dos listas de descriptores de minucias para determinar si ambas tenían la probabilidad de venir del mismo dedo y de la misma persona.

La División de Identificación del FBI decidió que debía seguirse el enfoque sugerido por Moore y Wegstein. Para abordar las primeras dos de las tres tareas, el 16 de diciembre de 1966, el FBI emitió una solicitud de cotización (RFQ) "para desarrollar, demostrar y probar un dispositivo de lectura de ciertas minucias dactilares" (FBI, 1966). El contrato era para un dispositivo que automáticamente localizara y determinara la posición y orientación relativas de las minucias especificadas en huellas dactilares individuales contenidas en tarjetas de huellas dactilares estándar, y que se utilizarían en pruebas del FBI. Los requisitos declaraban que el lector debía ser capaz de medir y localizar minucias en unidades de no más de 0.1 mm y que la dirección de cada minucia debía medirse y presentarse como salida en unidades de no más de 11.25 grados (1/32 de un círculo completo). Los requisitos iniciales pedían un modelo prototipo para procesar 10,000 huellas dactilares individuales (1,000 tarjetas). Los contratistas también fueron instruidos para desarrollar una propuesta para un contrato subsecuente que procesara 10 veces ese número de huellas dactilares.

Las 14 propuestas recibidas como respuesta a esta solicitud de cotización se dividieron en 5 enfoques técnicos generales. Al concluir la evaluación de las propuestas, dos propuestas separadas fueron financiadas para proporcionar un modelo básico para la lectura de imágenes de huellas dactilares y la extracción de minucias. Ambos propusieron usar un "escáner de punto móvil" para capturar imágenes. Pero cada uno ofreció un enfoque diferente para el procesamiento de la información de la imagen capturada y ambos parecían prometedores. Un contrato se adjudicó a Cornell Aeronautical Labs, Inc., que proponía el uso de una computadora digital de uso general para procesar pixeles binarios y desarrollar programas para detectar y proporcionar parámetros de medición para cada minucia identificada. El segundo contrato fue adjudicado a la Autonetics Division de North American Aviation, Inc., la cual propuso la utilización de un proceso digital de propósito especial para comparar las marcas lógicas y fijas con la imagen que identifica, detecta y codifica cada minucia.

Mientras se desarrollaban los dispositivos de escaneo de huellas dactilares y detección de minucias, la tercera tarea de comparar dos listas de minucias para determinar una correspondencia de candidato fue abordada por Joe Wegstein (Wegstein, 1969a, 1970, 1972a/b, 1982; Wegstein y Rafferty, 1978, 1979; Wegstein et al., 1968). Él desarrolló los algoritmos iniciales para determinar coincidencias de huellas dactilares basándose en el proceso y comparación de las dos listas que describían la ubicación y orientación de minucias. Durante los siguientes 15 años, continuó desarrollando software más fiable al comparar huellas dactilares, el cual se hizo cada vez más complejo con el fin de justificar tales cosas como la distorsión plástica y la elasticidad de la piel. Los algoritmos que desarrolló fueron incorporados en los AFIS que finalmente se pusieron en funcionamiento en el FBI y otras dependencias policiales.

Para 1969, tanto Autonetics como Cornell habían hecho progresos significativos en sus modelos para la demostración de viabilidad. En 1970, se emitió una solicitud de propuesta (RFP) para la construcción de un prototipo de lector de huellas dactilares que reflejara la experiencia adquirida de los modelos originales de demostración con un requisito adicional para la velocidad y precisión. Cornell se adjudicó el contrato para entregar el prototipo del lector al FBI en 1972. Después de un año de experiencia con el prototipo de sistema, el FBI emitió una nueva solicitud de propuesta que contenía requisitos adicionales, tales como un subsistema de la tarjeta de manipulación de tarjetas con alta velocidad. En 1974, Rockwell International, Inc., se adjudicó un contrato para construir cinco sistemas modelo de producción de lectura automática de huellas dactilares. Este revolucionario sistema fue llamado Finder. Estos lectores se entregaron al

FBI en 1975 y 1976. Los siguientes 3 años se dedicaron al uso de dichos lectores en la conversión de 15 millones de tarjetas de huellas dactilares criminales (Moore, 1991, pág. 164-175).

Como se puso de manifiesto que los esfuerzos del FBI para automatizar el proceso de comparación de huellas dactilares tendrían éxito, las fuerzas del orden estatal y local comenzaron a evaluar esta nueva tecnología para sus propias aplicaciones. El sistema Minneapolis-St. Paul en Minnesota fue uno de los primeros sistemas automatizados de coincidencia de huellas dactilares (después de la del FBI) que se instalaría en los Estados Unidos. Además, mientras que los Estados Unidos desarrollaban su tecnología AFIS en la década de 1960, Francia, Reino Unido y Japón fueron también haciendo investigación acerca del procesamiento y coincidencia automáticos de imágenes de huellas dactilares.

6.1.4 Iniciativa francesa de AFIS

En 1969, M. R. Thiebault, Prefectura de Policía de París, informó sobre los esfuerzos franceses. (Las descripciones del trabajo realizado por Thiebault se pueden encontrar en las entradas que figuran en la sección de información adicional de este capítulo). El enfoque de Francia estaba en la solución al problema de huellas dactilares latentes en vez del problema general de identificación, la cual era la preocupación en los Estados Unidos. El enfoque francés incorporó un vidicon (un tubo de cámara de video) para escanear transparencias de película fotográfica de huellas dactilares. El escaneo se realizó a 400 píxeles por pulgada (ppi), que era menor a la velocidad de barrido óptima para el trabajo latente. Este enfoque para empatar minucias se basó en hardware de alta velocidad con fines especiales que utilizaba un conjunto de circuitos lógicos. Los franceses también estaban interesados en resolver el problema de la mala calidad de imagen de la huella. Con el fin de lograr una imagen de alto contraste que fuera fácil de fotografiar y procesar, se desarrolló una técnica para grabar imágenes de huellas dactilares fotográficamente en vivo, utilizando un principio de "reflexión interna total frustrada" (FTIR). Aunque no se produjo a gran escala en ese momento, 20 años más tarde el FTIR se convirtió en la piedra angular para el desarrollo de modernos escáneres livescan de huellas dactilares hoy en día. Estos están haciendo que la tinta y tarjetas sean obsoletas para la identificación no forense de hoy en día.

A principios de 1970, el personal responsable del desarrollo de tecnología de automatización de huellas dactilares de Francia había cambiado. Como resultado, había poco interés en perseguir la investigación de identificación automatizada de huellas dactilares para los próximos años. A finales de 1970, una subsidiaria de ingeniería en informática de la institución financiera más grande de Francia respondió a una solicitud del Ministerio de Interior francés para trabajar en un procesamiento automatizado de huellas dactilares para la Policía Nacional francesa. Más tarde, esta empresa se unió con el Laboratorio de Matemáticas Morfológicas de la Escuela de Minas de París para formar una filial denominada Sistemas Morpho la cual desarrollaría el funcionamiento. Actualmente, Sistemas Morpho es parte de Sagem (también conocido como Grupo SAFRAN).

6.1.5 Iniciativa AFIS del Reino Unido

Durante el mismo período de tiempo, el Ministerio del Interior del Reino Unido estaba haciendo la investigación sobre la identificación automática de huellas dactilares. Dos de las principales personas responsables de AFIS del Reino Unido fueron el Dr. Barry Blain y Ken Millard. (Los documentos producidos por Millard se encuentran en la sección de información adicional de este capítulo). Al igual que los franceses, su objetivo principal era el trabajo de impresión latente. Para 1974, la investigación se estaba haciendo en la empresa con la asistencia del contratista Ferranti, Ltd. El Ministerio del Interior desarrolló un lector para detectar minucias, posición y orientación del registro, y para determinar el número de crestas hacia los cinco vecinos más cercanos a la derecha de cada minucia. Éste fue el primer uso de información del conteo de crestas por parte de un proveedor AFIS (Moore, 1991).

6.1.6 Iniciativa japonesa de AFIS

Al igual que Francia y el Reino Unido, la motivación de Japón para tener un sistema de identificación de huellas dactilares fue dirigida hacia comparar imágenes latentes con un archivo maestro de huellas laminadas. Los investigadores japoneses creían que un sistema latente preciso naturalmente los llevaría al desarrollo de un sistema decadactilar exacto.

En 1966, el Departamento de Policía de la Prefectura de Osaka tenía casi 4 millones de huellas dactilares individuales. Un primer esfuerzo de automatización por parte de esta dependencia fue el desarrollo de un sistema de coincidencia de clasificación de patrones basado en un número de 17 a 20 dígitos codificado manualmente (Kiji, 2002, pág. 9). Aunque este enfoque mejoraba enormemente la

eficiencia del método totalmente manual, tenía problemas inherentes. Se requería de una gran cantidad de precisión humana y tiempo para clasificar las huellas dactilares latentes e individuales; no era totalmente adecuado para la coincidencia latente; y producía una larga lista de candidatos lo que resultaba en verificaciones caras.

A los pocos años, el enfoque de automatización de huellas dactilares de los investigadores japoneses había cambiado. Para 1969, la Sección de Identificación de la Oficina de Investigación Criminal de la Agencia Nacional de Policía de Japón (NPA) se acercó a NEC para desarrollar un sistema para la automatización de la identificación de huellas dactilares. NEC determinó que podría construir un sistema automatizado de identificación de huellas dactilares que empleara un enfoque basado en minucias, similar al que se utilizaba en el sistema en desarrollo del FBI. En ese momento, se pensó que un sistema totalmente automatizado para la búsqueda de huellas dactilares no se llevaría a cabo durante 5 a 10 años. En 1969, representantes de NEC y NPA visitaron el FBI y comenzaron a aprender sobre el estado actual de la técnica para planes AFIS del FBI. Durante ese mismo período, representantes de NPA también colaboraron con Moore y Wegstein de NIST. Sitios AFIS adicionales fueron visitados, donde se adquirió información sobre enfoques útiles e inútiles que habían sido intentados. Toda esta información se evaluó y se utilizó en el desarrollo del sistema de NEC.

Durante los siguientes 10 años, NEC trabajó para desarrollar su AFIS. Además de la ubicación y orientación de minucias, este sistema también incorporó información del número de crestas presentes en los cuadrantes que rodeaban los cuatro locales de cada minucia bajo consideración de emparejamiento. En 1982, NEC había instalado con éxito su sistema en el NPA y comenzó el proceso de conversión de la tarjeta. Al año, comenzaron las búsquedas de información sobre latentes.

En 1980, NEC recibió una patente estadounidense para la detección automática de minucias. Comenzó a comercializar sus sistemas automatizados de identificación de huellas dactilares en los Estados Unidos unos años más tarde.

6.1.7 La politización de las huellas dactilares y el experimento San Francisco

El desarrollo e implementación tempranos de sistemas automatizados de huellas dactilares se limitaban a las dependencias policiales nacionales en Europa, América del Norte y Japón. Pero los problemas relacionados con enormes bases de datos nacionales y la situación recién nacida de la tecnología de informática en la década de 1970 limitaban la utilidad de estos sistemas. La inversión gubernamental en AFIS se justificaba en gran medida por la promesa de la eficiencia en el procesamiento de expedientes decadactilares entrantes. Sin embargo, el financiamiento de estos sistemas costosos a nivel local exigiría un poco de creatividad (Wayman, 2004, pág. 50-52).

Tras el éxito del Buscador del FBI, Rockwell tomó su sistema para comercializarlo a mediados de la década de 1970. Rockwell organizó un grupo de usuarios para su sistema Printrak y patrocinó una conferencia anual para clientes y posibles clientes. A partir de un sitio beta en San José, California, más de una docena de instalaciones se completaron en una rápida sucesión. Peggy James del Departamento de Policía de Houston, Joe Corcoran de Saint Paul, Donna Jewett de San José, y otros dedicaban sus energías a la educación de la comunidad internacional de huellas dactilares sobre el milagro del sistema Printrak basado en minucias. Cada sistema que entró en funcionamiento anunciaba con bombo y platillo la solución a los crímenes que de otro modo no se habían resuelto, además de la identidad de los delincuentes detenidos. Se publicó y distribuyó un boletín informativo de un grupo de usuarios, éste destacó algunos de los mejores casos, y enumeró las estadísticas de búsqueda de las dependencias miembro.

Ken Moses del Departamento de Policía de San Francisco había asistido a varias de las conferencias de Printrak y se convirtió en un defensor acérrimo de la automatización de la huella dactilar. En los tres años sucesivos, persuadió al Jefe de Policía para incluir un sistema Printrak en el presupuesto de la ciudad, pero cada vez era vetada por el alcalde. Después del tercer veto del alcalde, una propuesta de votación fue organizada por otros políticos. La propuesta pedía a los ciudadanos que votaran si querían un sistema automatizado de huella dactilar. En 1982, la Propuesta E pasó con una pluralidad del 80%.

El alcalde se negó a aprobar la compra de una única fuente de Rockwell, a pesar de que era el único sistema en el mundo que se comercializaba. Insistió en una oferta competitiva con estrictos criterios de evaluación y pruebas. Mientras estaba en una misión comercial en Japón, el alcalde aprendió que la Policía Nacional de Japón estaba trabajando con NEC para instalar un sistema de huellas dactilares, pero NEC declaraba que el sistema estaba en desarrollo como un servicio público y la compañía no tenía

planes de comercializarlo. Después de reunirse con funcionarios japoneses clave, NEC cambió de parecer y aceptó una oferta en el AFIS de San Francisco.

Cuando se abrieron las licitaciones, Printrak y NEC no eran las únicas que habían presentado propuestas, un caballo negro llamado Logica también había entrado al combate. Logica había estado trabajando con el Ministerio del Interior británico para desarrollar un sistema para New Scotland Yard.

San Francisco retuvo al consultor en sistemas Tim Ruggles para llevar a cabo las primeras pruebas de referencia competitivas en el uso de sistemas de huellas dactilares. La prueba tuvo mayor peso en la precisión de impresiones latentes y un conjunto de 50 impresiones de huellas latentes calificadas de pobre a buena a partir de casos reales anteriores, se registraron contra una base de datos decadactilar prescrita. Todas las pruebas se llevaron a cabo en el hogar del proveedor correspondiente.[2] NEC se adjudicó el contrato y la instalación se completó en diciembre de 1983.

Además de ser la primera oferta competitiva en tecnología de la década de 1980, lo que diferenciaba al sistema de San Francisco de los que se habían ido antes era el diseño organizacional. AFIS fue visto como un verdadero sistema que abarcaba todos los aspectos de la identificación de las crestas de fricción—del lugar de los hechos a la sala del tribunal. El presupuesto AFIS incluía equipo de laboratorio y para el lugar de los hechos, formación en todas las fases de evidencia forense, incluso la compra de vehículos. En 1983, una nueva unidad para el lugar de los hechos se organizó específicamente con el nuevo sistema como la pieza central. Cambios importantes de la organización fueron puestos en práctica:

1. Todas las latentes que cumplieran con los criterios mínimos debían ser buscadas en el AFIS.
2. Se creó una nueva unidad llamada Investigaciones del Lugar de los Hechos con personal que tenía un horario de 24/7.
3. Las políticas del departamento se cambiaron para ordenar que los oficiales de patrullaje notificaran a los investigadores del lugar de los hechos de todos los delitos con huellas latentes en potencia.
4. Todos los investigadores quienes procesaban el lugar de los hechos eran capacitados en el uso del sistema y eran alentados a buscar sus propios casos.
5. Las estadísticas de desempeño se guardaban desde el comienzo y los casos AFIS eran buscados del sistema de justicia penal hasta los tribunales.

El resultado del experimento de San Francisco generó un dramático aumento de 10 veces en las identificaciones de huellas latentes en 1984. El fiscal de distrito exigió y obtuvo cinco nuevos puestos para procesar los casos AFIS. La tasa de condenas en casos de robo derivados de AFIS era tres veces mayor que en los casos de robo sin este tipo de evidencia (Figura 6-1; Bruton, 1989).

En momentos en que las tasas de robo estaban aumentando considerablemente en las ciudades de todo el país, la tasa de robo se desplomó en San Francisco (Figura 6-2; Bruton, 1989). Los reporteros, académicos y administradores de la policía de todo el mundo inundaron el Departamento de Policía de San Francisco para obtener demostraciones e información.

La importancia de la política y la publicidad no se perdió en otras dependencias. La ciudad de Los Ángeles incluso agregó a la lista el apoyo de estrellas de cine para promover el apoyo del público. La identificación del asesino en serie Richard Ramírez, el infame Night Stalker, a través de una búsqueda de la nueva California State AFIS fue noticia en todo el mundo y garantizaba el futuro financiamiento de los sistemas en California.

6.1.8 Proliferación AFIS

El éxito en San Francisco, difundido ampliamente, proporcionó la chispa para la rápida proliferación de las nuevas instalaciones AFIS, junto con una metodología de pruebas de referencia para evaluar las demandas de la creciente cantidad de proveedores de la competencia. Los gobiernos rápidamente proporcionaron fondos para que en 1999, *el Directorio de Usuarios AFIS* de la Asociación Internacional para la Identificación (IAI) identificara 500 sitios AFIS en todo el mundo (IAI, 1999).

El floreciente mercado de estos sistemas multimillonarios puso a la identificación forense en el mapa económico.

[2] Los primeros resultados de las pruebas de referencia competitivas fueron publicados por la Asociación Internacional para la Identificación en 1986 (Moisés, 1986). A partir de entonces, algunos vendedores a menudo exigían que los resultados de las pruebas de referencia se mantuvieran en secreto y las fuerzas del orden público en general accedieron a dichas demandas. Esto ha hecho que sea extremadamente difícil para los investigadores y los posibles compradores evaluar los sistemas de la competencia. El velo del secreto se ha mantenido en general en cuanto a compartir información del desempeño operativo AFIS por parte del personal de la dependencia, quienes frecuentemente desarrollan un fuerte sentido de lealtad a su proveedor AFIS.

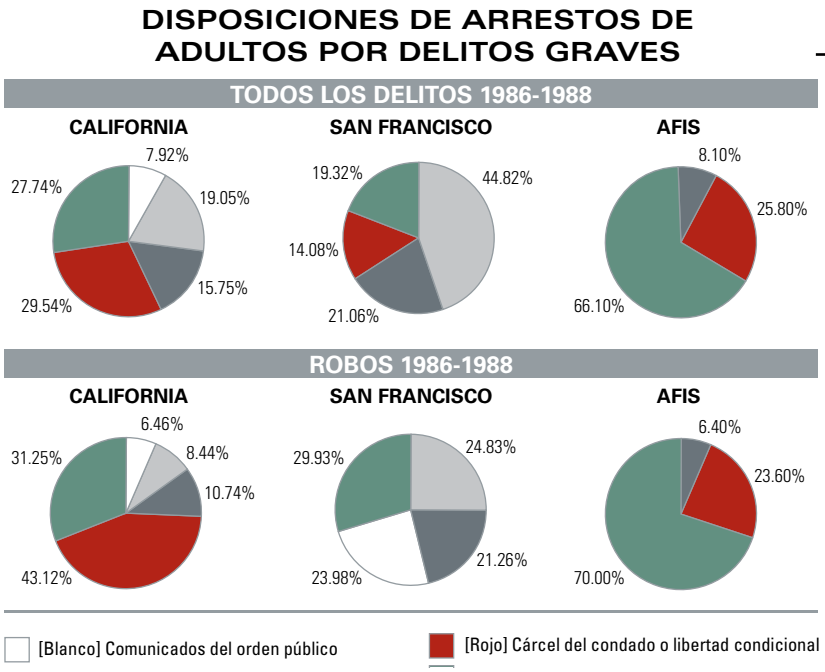


FIGURA 6–1

El seguimiento de éxitos de latentes a través de los tribunales. (Bruton, 1989).

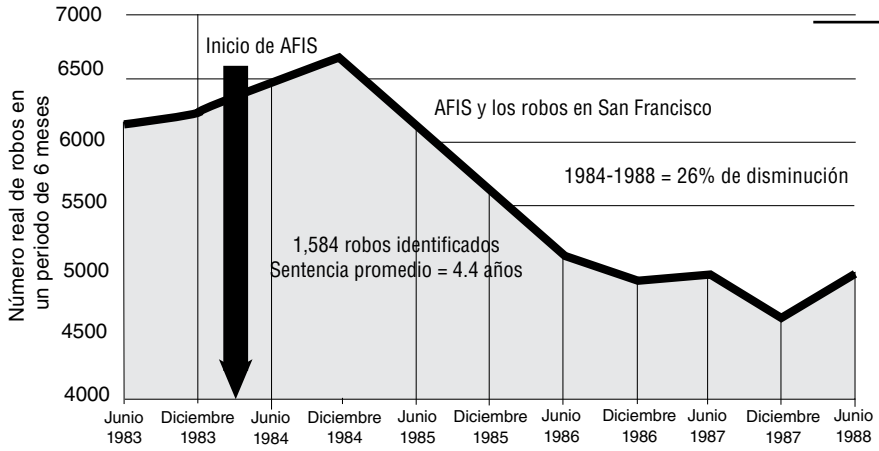


FIGURA 6–2

Estudio estadístico de logros de AFIS vs robos en San Francisco, 1984-1988. (Bruton, 1989).

Las exposiciones comerciales en las conferencias del IAI, en donde había empresas destacadas que anteriormente vendían cinta y polvo, ahora se habían expandido a las ampliaciones de imágenes digitales, láseres y fuentes de luz forense, y a lo último en desarrollos nuevos de Silicon Valley. El Laboratorio Criminal de San Francisco recibió su primer sistema de imagen digital en 1986. Este sistema 3M/Comtal estaba dedicado a la mejora de las crestas de fricción. Fingermatrix instaló el primer dispositivo livescan en la Oficina de Identificación de la Policía de San Francisco en 1988. AFIS sacó al lugar de los hechos y a la identificación forense del sótano; ningún administrador de la ley local o estatal quería ser acusado de quedarse atrás.

Sin embargo, la expansión desenfrenada de AFIS no siempre era lógica y racional. A principios de la década de 1990, los cuatro mayores proveedores—Printrak, NEC, Morpho y Cogent—estaban en competencia, cada uno ofrecía software patentado que era incompatible con los demás, sobre todo en la búsqueda de huellas latentes.

A menudo, la expansión se basa en consideraciones políticas y prioridades en la misión de la competencia. Las dependencias locales y estatales expresaron diferencias en las prioridades en términos de diseño del sistema, con los estados generalmente haciendo énfasis en las funciones decadactilares o de identificación criminal, mientras que

las ciudades y condados se centraron en la resolución de crímenes o funciones de huellas latentes. En general, las demandas de procesamiento de las impresiones latentes en los recursos computacionales superaron con creces los requisitos de procesamiento decadactilar y los estados se opusieron al gasto adicional y la complejidad técnica. Como resultado, las ciudades, condados y estados a menudo se fueron por su lado, instalando sistemas diferentes que no podían comunicarse con las jurisdicciones vecinas o con el repositorio estatal central. Los vendedores animaban con entusiasmo esta fragmentación en un intento de ganar participación en el mercado y desplazar a los competidores cuando fuera posible. La evolución de las normas de transmisión electrónica (ver sección 6.3) mejoraron este problema para la búsqueda decadactilar, pero no para la búsqueda de latentes.

6.2 Operaciones de AFIS

6.2.1 Funciones y capacidades de AFIS

Las oficinas de identificación están legalmente obligadas a mantener los registros de antecedentes penales. Históricamente, esto significaba requisitos de almacenamiento de archivos enormes y cuadros de secretarias que los cuidaran y buscaran. Las computadoras demográficamente basadas en antecedentes penales se establecieron muy por delante de AFIS, primero como sistemas para ordenar las tarjetas IBM y luego como sistemas de información totalmente digitales, con terminales por todo el estado a través del Centro Nacional de Información Penal (NCIC) y el National Law Enforcement Teletype Sistem (Nlets) en toda la nación. Estos sistemas automatizados de antecedentes penales se hicieron aún más laboriosos que los sistemas de registro en papel a los que supuestamente reemplazaron. En muchos sistemas, se generó más papel y se colocó en las cubiertas del historial junto con las tarjetas de huellas dactilares, fotos policiales, órdenes de arresto y otros documentos requeridos.

AFIS revolucionó a las oficinas de identificación estatales ya que eliminó de los archivos de papel el último tipo de documento que antes no podía ser digitalizado—la tarjeta de huellas dactilares. Las oficinas de identificación estatales ahora podían llevar a sus legislaturas los análisis del costo-beneficio que fácilmente justificaban la compra de un sistema automatizado de huellas dactilares a través de la reducción del personal de oficina.

Las jurisdicciones locales y del condado no solían gozar de los beneficios económicos de los sistemas estatales. Los niveles del personal antes de AFIS eran a menudo más bajos y estaban controlados más por las exigencias del proceso de ingreso que por el mantenimiento de archivos. En general, AFIS aumentó las demandas de personal del lado latente y el procesamiento del lugar de los hechos porque hizo que el procesamiento del lugar de los hechos fuera dramáticamente más productivo. Las compras locales y del condado de AFIS normalmente se justificaban sobre la base de su potencial para resolver crímenes.

6.2.1.1 Funciones técnicas. Las AFIS policiales se componen de dos subsistemas interdependientes: el subsistema decadactilar (es decir, la identificación penal) y el subsistema latente (es decir, la investigación penal). Cada subsistema opera con una cantidad considerable de autonomía y ambos son vitales para la seguridad pública.

El subsistema decadactilar tiene la tarea de identificar conjuntos de incidentes de huellas dactilares entintadas o por livescan en un arresto o citación o como parte de un proceso de solicitud para determinar si una persona tiene un registro existente.

En muchos sistemas, el personal de identificación también se encarga de mantener la integridad de las bases de datos de huellas dactilares y antecedentes penales. El personal de la oficina de identificación en general está compuesto de técnicos en huellas dactilares y personal de apoyo de oficina.

Una investigación decadactilar automatizada normalmente requiere de una búsqueda de minucias solo de pulgares o dedos índice. Las huellas dactilares presentadas suelen tener claridad y detalle suficientes para hacer que la búsqueda de más de dos dedos sea innecesaria. La AFIS de hoy con frecuencia puede realizar una búsqueda de un millón de registros en menos de un minuto. Debido a que las bases de datos se han expandido en todo el mundo, algunos ingenieros AFIS se han ampliado para buscar cuatro dedos o más en un esfuerzo por aumentar la precisión.

El subsistema de identificación penal o de impresión latente tiene la tarea de resolver crímenes a pesar de la identificación de impresiones latentes desarrolladas en el lugar de los hechos y la evidencia física. Las terminales utilizadas dentro del subsistema latente a menudo están especializadas para dar cabida a la captura y mejora digitales de las huellas latentes individuales. El subsistema latente

puede estar compuesto de examinadores de impresiones latentes, investigadores del lugar de los hechos, o personal de laboratorio o administrativo. El personal del subsistema latente está frecuentemente bajo una estructura de mando diferente a la del subsistema decadactilar, y con frecuencia se le asocia con el laboratorio del crimen.

La búsqueda de una huella latente es muy tediosa y consume más tiempo que una búsqueda decadactilar. Las impresiones latentes son a menudo fragmentarias y tienen mala calidad de imagen. Las características de las minucias normalmente son revisadas una por una antes de que inicie la búsqueda. Dependiendo de la porción de la base de datos seleccionada para revisión y la carga de búsqueda del sistema, la respuesta puede tardar de unos pocos minutos hasta varias horas en reflejarse.

La mayoría de las instalaciones policiales AFIS tienen la capacidad de realizar las siguientes funciones:

- Comparar un juego de huellas dactilares conocidas (impresiones decadactilares) y una base de datos decadactilar existente (TP-TP) y volver con resultados que sean mejores que el 99% de precisión.[3]
- Comparar una impresión latente en el lugar de los hechos con evidencia penal y una base de datos decadactilar (LP-TP).
- Comparar una latente del lugar de los hechos y latentes en los archivos de otras escenas del crimen (LP-LP).
- Comparar una nueva adición decadactilar a la base de datos y todas las huellas latentes sin resolver en el archivo (TP-LP).

Se han hecho mejoras para permitir que otras funciones expandan las capacidades de AFIS, incluyendo:

- La adición de registros de la huella palmar a la base de datos para permitir la búsqueda de huellas palmares latentes provenientes de los lugares de los hechos.
- Interfaz de AFIS con otros sistemas de información de justicia penal para agregar eficiencia y la operación "Lights Out".[4]
- Interfaz de los sistemas AFIS con sistemas digitales de fichas policiales y dispositivos de captura de huellas dactilares livescan.
- Incorporación de dispositivos portátiles de mano para su uso en consultas de identidad en campo. La consulta se inicia mediante la exploración de uno o más de los dedos del sujeto, extrayendo las minucias dentro del dispositivo y transmitiéndolas a AFIS, la cual después arroja un resultado de éxito o sin éxito (luz roja, luz verde). Una notificación de éxito podrá estar acompañada de la imagen en miniatura de la ficha policial del sujeto.
- Los sistemas de identificación multimodales, incluyendo la huella dactilar, huella palmar, iris y el reconocimiento facial ya están disponibles ahora.

6.2.2 Precisión del sistema

La mayoría de los sistemas informáticos dedicados al gobierno se basan en información demográfica como nombre, dirección, fecha de nacimiento y otra información proveniente de letras y números. Por ejemplo, para buscar un registro en la base de datos de vehículos de motor, se puede introducir un número de placa o los datos del operador. El éxito de la búsqueda dependerá de la precisión con la que las letras y números fueron percibidos e ingresados originalmente. La investigación es sencilla y muy precisa para encontrar el registro deseado.

Los sistemas automatizados de huellas dactilares se basan en datos extraídos de imágenes. Aunque hay una única forma correcta de deletrear un nombre en la base de datos de vehículos de motor, una imagen de huella dactilar puede ser escaneada en un número casi infinito de formas. El éxito en la búsqueda de huellas dactilares depende de la claridad de la imagen y el grado de correspondencia entre la huella de búsqueda y la impresión en la base de datos (compresión y algoritmos son otros dos factores que pueden afectar la precisión). En el caso de la búsqueda de una nueva tarjeta decadactilar en la base de datos de decadactilares, por lo general hay información de imagen lo suficientemente presente para encontrar su coincidencia el 99,9% del tiempo en los sistemas con operadores a la mano para comprobar las listas de los encuestados (en lugar de las verdaderas operaciones "Lights Out").

Una impresión latente por lo general consiste de una porción fragmentaria de un solo dedo o un pedazo de la palma, aunque la calidad de algunas impresiones latentes puede exceder sus imágenes correspondientes del

[3] Esta cifra está basada en los requisitos encontrados en documentos de concesión y pruebas de puntos de referencia, en lugar de la observación operativa.

[4] "Lights out" (a luz apagada) normalmente se refiere a la habilidad del sistema para operar sin la intervención humana.

registro. La cantidad de información presente en la imagen es generalmente de menor calidad y a menudo está contaminada con interferencia de fondo. Ingresar latentes a la computadora tiene un elemento subjetivo que se basa en la experiencia del operador. Sobre la base de los requisitos para pruebas de aceptación de impresiones latentes que normalmente se encuentran en las propuestas y contratos AFIS, las probabilidades de que una huella latente encuentre su coincidencia son de 70% a 80%. Naturalmente, cuanto mejor sea la imagen latente, mayores serán las posibilidades de éxito. De forma inversa, la posibilidad de perder una identificación, incluso cuando el sujeto esté en la base de datos, es de 25%. Especialmente en las búsquedas de huellas latentes, la falla al producir una identificación o un éxito no significa que el sujeto no esté en la base de datos. Otros factores que escapan al conocimiento y control del operador, tales como impresiones de bases de datos de mala calidad, afectarán negativamente las posibilidades de una coincidencia.

Debido a la variabilidad de las imágenes y la subjetividad del operador de la terminal, a menudo el éxito mejora mediante la realización de búsquedas múltiples mientras se varía la imagen, se cambian los operadores o se busca en otros sistemas que puedan contener diferentes copias de las impresiones del sujeto. Es común que el éxito venga después de múltiples intentos.

6.2.3 Beneficios periféricos

6.2.3.1 Seguridad comunitaria. No existe un mecanismo de informes nacionales para la recopilación de estadísticas AFIS (o huellas latentes), por lo que los beneficios cuantificables son ilusorios. Sin embargo, para proporcionar un cierto reconocimiento de esos beneficios, el autor de este capítulo realizó una encuesta de éxitos latentes en los 10 estados con mayor población en el año 2005 (Tabla 6-1). Los intentos anteriores de proporcionar este tipo de información han puesto de manifiesto las inconsistencias de cómo se cuentan las identificaciones y cómo se determina la tasa de aciertos (Komarinski, 2005, pág. 184-189).

Con base en la encuesta del autor, se estima que 50,000 sospechosos por año en los Estados Unidos están identificados a través de búsquedas de latentes AFIS. En la realización de la encuesta, si las oficinas de estado contactadas no tenían cifras a nivel estatal, entonces también se intentaba con alguna de las cinco ciudades más grandes en ese estado.

Tabla 6–1

Aciertos mínimos (casos o personas identificadas) de los 10 estados con mayor población en el año 2005

Rank by Population	State	AFIS Latent Hits
1	California	8,814
2	Texas	3,590
3	New York	2,592
4	Florida	6,275
5	Illinois	1,224
6	Pennsylvania	1,463
7	Ohio*	1,495
8	Michigan**	1,239
9	Georgia	980
10	New Jersey	1,506
	Total	29,178

* Cleveland no está disponible.
** Detroit no está disponible.

(En ningún caso fue posible contactar cada jurisdicción equipada con AFIS en un estado, por lo que los aciertos totales son el número mínimo de aciertos.) Además, sólo se contaron casos de aciertos o éxitos de sospechosos, en función de los datos que mantiene cada dependencia. (Cuando las dependencias reportaron múltiples aciertos a una sola persona, esto no fue incluido en la información presentada).

Al extrapolar la tabla, si cada uno de los 40 estados restantes y todas las dependencias del gobierno federal tuvieran un solo acierto latente por día, el estimado total de accesos latentes para todos los Estados Unidos superaría los 50,000.

Pocos estudios se han realizado para medir qué efecto, si hubiese, ha tenido un aumento dramático en la tasa de identificaciones de huellas latentes sospechosas de AFIS sobre la seguridad pública en general. El robo de datos en San Francisco a finales de 1980 (Figura 6-2) es probatorio, pero debe interpretarse de manera restrictiva. Los Informes de Crímenes Uniformes del FBI muestran una disminución constante de los delitos más graves que coinciden con la proliferación de AFIS, pero no hay una relación de causa y efecto que haya sido explorada por la academia o el gobierno. Durante la década de 1990, muchos estados

aprobaron las leyes "tres strikes" que aumentaron el castigo para delitos graves que algunos teóricos han sostenido ser responsables de la disminución de la delincuencia. Pero antes de que penas más severas se puedan aplicar, los autores deben ser identificados y detenidos.

El robo es el delito más impactado por AFIS. Supongamos que un ladrón activo está cometiendo dos delitos por semana al momento de ser detenido sobre la base de un éxito AFIS. Se le condena y con base en las leyes de sentencias severas, es enviado a prisión por 5 años. En este caso, ese acierto de AFIS habría evitado 100 delitos por cada año del transcurso de la sentencia de 5 años. Si este arresto se multiplica por una fracción de los totales de la tabla anterior, se puede obtener una apreciación más real del impacto que está teniendo AFIS en la sociedad.

6.2.3.2 Validación de la ciencia de crestas de fricción. Hay muchas maneras de probar la eficacia de una propuesta teórica. Los laboratorios corporativos y académicos vierten gran cantidad de recursos en la construcción de modelos que esperan casi dupliquen su desempeño en el mundo real. Incluso después de pasar con éxito estas pruebas, las teorías fallan y los productos son retirados después de superar los rigores del mundo real. Los modelos en uso invariablemente superan a los modelos de laboratorio.

Durante los últimos 100 años, muchos modelos se han construido para probar la teoría de que no hay dos imágenes de crestas de fricción de diferentes áreas de las superficies palmares iguales y para determinar la mínima cantidad de minucias es suficiente con apoyar la decisión de individualización.

Los sistemas automatizados de huellas dactilares han probado con efectividad la teoría de la identificación millones de veces al día todos los días durante más de 20 años. Estos sistemas tienden a validar lo que los examinadores de crestas de fricción han propuesto desde que Galton establece por primera vez sus normas. AFIS también ha servido como catalizador para ayudar a los examinadores a ampliar sus conocimientos y habilidades en el procesamiento de imágenes.

Algunos errores se producen cada año, tanto en sistemas manuales como automatizados y es a través del estudio de los errores el que ambos sistemas puedan ser mejorados en el futuro. De acuerdo con el Dr. James Wayman, Director del Centro Nacional de Pruebas de Biometría, "las tasas erróneas (en la identificación de crestas de fricción) son difíciles de medir, precisamente porque son muy bajas" (Wayman, 2000).

6.2.4 IAFIS

El Sistema Automatizado e Integrado de Identificación de Huella Dactilar, más comúnmente conocido como IAFIS, es la mayor colección de información de antecedentes penales en el mundo. En pleno funcionamiento desde el 28 de julio de 1999, el IAFIS se mantiene por la División de Servicios de Información de Justicia Penal (CJIS) del FBI en Clarksburg, WV, y contiene imágenes de huellas dactilares de más de 64 millones de individuos. La arquitectura del sistema de la División CJIS del FBI y los servicios de identificación e investigación proporcionados por la división forman un concepto de sistema-de-servicios integrados (SoS). Estos servicios de identificación e información permiten a comunidades de aplicación de la ley a nivel local, estatal, federal, tribal e internacional, así como organizaciones civiles, acceder de manera eficiente o intercambiar información crítica las 24 horas del día, los 365 días al año. El SoS proporciona una identificación avanzada y tecnologías de justicia penal auxiliares utilizadas en la identificación de sujetos.

Los sistemas dentro de CJIS SoS, incluyendo el IAFIS, han evolucionado con el tiempo, tanto individual como colectivamente, para agregar nuevas capacidades tecnológicas, adoptar directrices legislativas y mejorar el rendimiento y precisión de sus servicios de información. Durante su primer año de creación, el IAFIS procesó cerca de 14.5 millones de entregas de huellas dactilares. Hoy en día, IAFIS procesa volúmenes decadactilares similares en muy poco tiempo, como 3 a 4 meses. Aunque ha sido diseñado para responder a las transacciones penales electrónicas dentro de 2 horas y transacciones civiles en 24 horas, IAFIS ha superado estas demandas, proporcionando a menudo solicitudes de búsqueda penales en menos de 20 minutos y verificación de antecedentes civiles en menos de 3 horas. Del mismo modo, IAFIS ofrece a los examinadores de huellas latentes una herramienta de investigación superlativa, permitiendo que la evidencia de huellas dactilares del lugar de los hechos se pueda buscar en aproximadamente 2 horas en lugar de las 24 horas del tiempo de respuesta estipulado. Aunque declarado como un sistema exitoso a inicios de su lanzamiento, IAFIS continúa mejorando como un activo vital para las fuerzas del orden después de más de 10 años. La sociedad transitoria de hoy magnifica la necesidad de un proceso de identificación que sea económico, rápido y positivo tanto para la verificación de

antecedentes penales como los no penales. Los procesos IAFIS se mejoran periódicamente para permitir una rápida y precisa verificación de los registros basados en huellas dactilares, ya sea en relación con los terroristas que intentan ingresar a los Estados Unidos o los aspirantes a puestos de confianza. La Figura 6-3 ilustra los estados que actualmente interactúan con IAFIS electrónicamente.

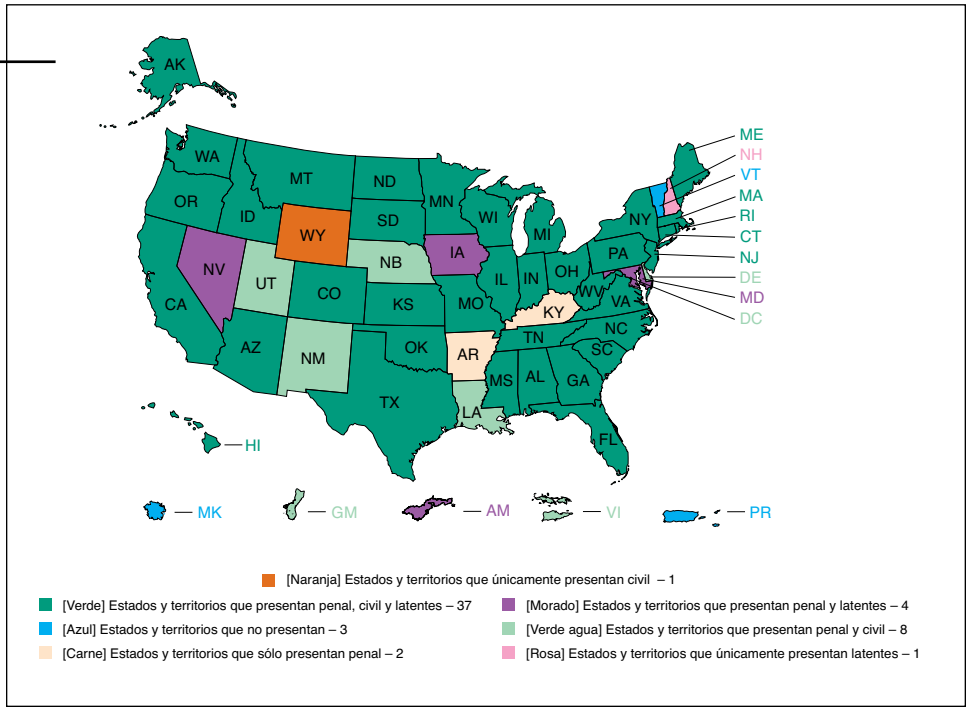
Los requisitos cada vez más complejos de la arquitectura SoS exigen un proceso bien estructurado para sus operaciones y mantenimiento. Cada uno de estos sistemas tiene varios segmentos que constan de hardware y software, los cuales proporcionan sistemas operativos y utilidades, gestión de bases de datos, gestión del flujo de trabajo, gestión de transacciones o la mensajería, redes internas y externas, el balance de la carga de comunicaciones, y la seguridad del sistema. IAFIS consta de tres segmentos integrados: segmento de Identificación de Asignación de Tareas y Funciones de Red (ITN), el Índice de Identificación Interestatal (III), y el AFIS (Figura 6-4).

Dentro de IAFIS, el segmento ITN actúa como un "policía de tránsito" para el sistema de huellas dactilares, proporcionando manejo del flujo de trabajo/carga de trabajo decadactilar, huellas latentes y el procesamiento de documentos. El ITN proporciona las interfaces hombre-máquina, las interfaces internas para las comunicaciones dentro del elemento de comunicaciones troncales IAFIS, el almacenamiento y recuperación de imágenes de huellas dactilares, las interfaces de comunicaciones externas, el elemento de comunicaciones de segundo plano de IAFIS y la facturación de tasas de usuario. El III ofrece búsqueda por temas, historial penal automatizado y almacenamiento y recuperación de fotos policiales. El AFIS busca en el repositorio de huellas dactilares del FBI coincidencias con huellas decadactilares y las huellas dactilares latentes. Apoyando a IAFIS está la red CJIS de área amplia (WAN), que proporciona la infraestructura de comunicaciones para el intercambio seguro de información de huellas dactilares de y hacia sistemas externos. Los sistemas externos son las dependencias terminales de control estatal, oficinas de identificación estatales y los coordinadores de servicios federales.

Asimismo, la presentación de información de huellas dactilares a IAFIS es el Servicio de Escaneo de la Tarjeta (CSS). El CSS actúa como un conducto para las dependencias que todavía no presentan huellas dactilares electrónicamente. El CSS hace la conversión de la información de huellas dactilares del formato papel al formato electrónico y envía esta información a IAFIS. Otro sistema que proporciona comunicaciones externas para IAFIS es Nlets. El propósito de Nlets es proporcionar comunicaciones interestatales a la policía, la justicia penal y otras dependencias que participan en la aplicación de las leyes. La Figura 6-5 muestra la arquitectura IAFIS de alto nivel. Los usuarios que deseen

FIGURA 6–3

Presentaciones electrónicas al IAFIS. (Ilustración de la Oficina Federal de Investigaciones).



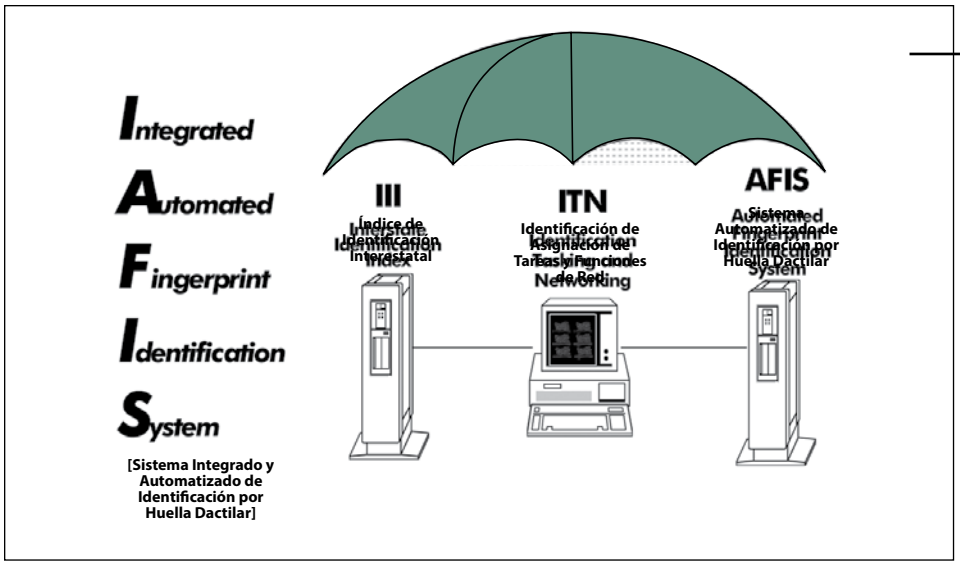


FIGURA 6–4

Segmentos IAFIS. (Ilustración de la Oficina Federal de Investigaciones)

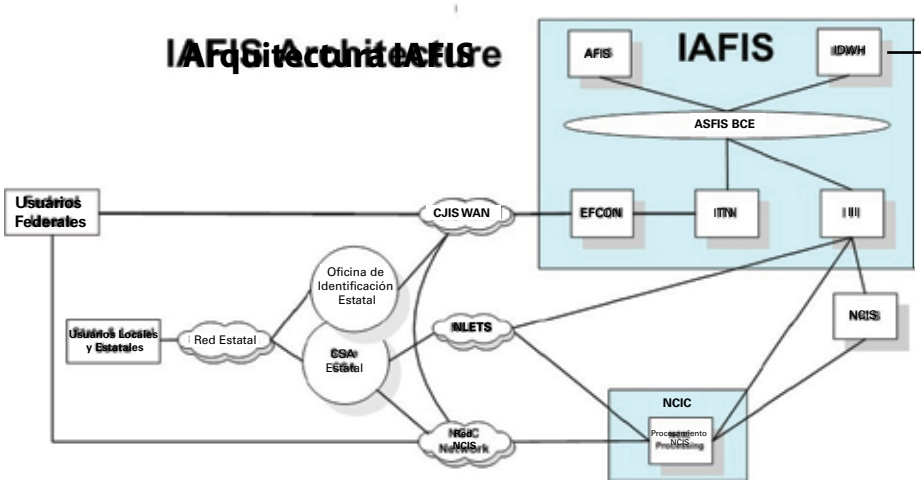


FIGURA 6–5

Arquitectura de redes IAFIS. (Ilustración de la Oficina Federal de Investigaciones).

interactuar con IAFIS electrónicamente deben cumplir con la Especificación de Transmisión Electrónica de Huellas Dactilares (EFTS) del FBI.

El acceso electrónico y el intercambio de información de huellas dactilares del repositorio nacional más grande del mundo, en cuanto a antecedentes penales y civiles automatizados, están cumpliendo con la misión de CJIS:

> La misión de la División CJIS es reducir las actividades terroristas mediante la maximización de la capacidad de proporcionar información oportuna y relevante de justicia penal al FBI y al cumplimiento calificado de la aplicación de la ley, justicia penal, civil, académica, empleo y dependencias autorizadoras relativas a las personas, bienes robados, organizaciones y actividades criminales y cualquier otra información relacionada con la aplicación de la ley.

6.2.4.1 Estado de IAFIS a principios de 2006. Debido a los cambios evolutivos en el American National Standards Institute (ANSI)/estándar NIST en 1997, 2000 y 2006, el FBI no siempre ha tenido los recursos financieros o el compromiso corporativo para actualizar el IAFIS y mantenerlo al día. Una de las áreas donde se ha avanzado es la aceptación y procesamiento de las "bofetadas segmentadas" para las transacciones civiles. Estas transacciones utilizan una platina livescan modificada que mide 3 pulgadas de alto, de tal forma que los cuatro dedos de cada mano se pueden colocar como una "bofetada" en una posición recta de arriba hacia abajo. Del mismo modo, los dos pulgares se pueden capturar al mismo tiempo para obtener un total de tres imágenes (de tipo 4 o de tipo 14, como se

define en las secciones 6.3.2.1 y 6.3.3). Los archivos de tres imágenes de la transacción resultante son fáciles de segmentar con el software del dispositivo de captura. Las tres imágenes y localización relativa de los dedos segmentados dentro de las imágenes se transmiten. Esto reduce drásticamente el tiempo de recolección y mejora la calidad de la imagen capturada desde una perspectiva de contenido debido a la colocación plana, recta, de 3 pulgadas.

Un inconveniente del IAFIS es que no puede almacenar y buscar huellas palmares, aunque varios AFIS de producción pueden hacerlo. Además, al menos una producción extranjera y varios sitios AFIS nacionales aceptan y almacenan imágenes decadactilares de 1,000 pixeles por pulgada—IAFIS aún no puede hacer esto.

El FBI reconoce la necesidad de expandir sus servicios y ha (1) ensayado sistemas de palmas pequeñas y ha (2) iniciado un proyecto conocido como el Programa de Identificación de la Siguiente Generación (NGI). Impulsada por los avances en tecnología, los requisitos del cliente y la creciente demanda de servicios IAFIS, este programa va a avanzar aún más los servicios de identificación biométrica del FBI, proporcionando un reemplazo gradual de las capacidades técnicas actuales de IAFIS mientras introduce nuevas funcionalidades. Las mejoras y nuevas capacidades de NGI serán introducidas a través de un marco de tiempo de varios años dentro de un enfoque por etapas. El sistema NGI ofrecerá servicios de identificación biométrica vanguardistas y proporcionará un marco flexible de capacidades básicas que servirán como plataforma para la funcionalidad multimodal.

6.2.4.2 Estación de trabajo latente universal. Los AFIS que son totalmente compatibles con ANSI/NIST pueden enviar transacciones basadas en imágenes de un sitio a otro. Pero en la comunidad latente, la mayoría de los profesionales quieren editar las imágenes y extraer las minucias ellos mismos, es decir llevar a cabo búsquedas remotas en lugar de las entregas. Este modelo también se lleva bien con la capacidad de la mayoría de las dependencias para proporcionar mano de obra calificada necesaria para las entregas basadas en imágenes de otras dependencias.

La División CJIS del FBI abordó este tema trabajando estrechamente con Mitretek y los cuatro proveedores principales de AFIS para desarrollar un conjunto de herramientas que permitan la creación de búsquedas remotas para cualquiera de sus sistemas automatizados de identificación dactiloscópica, y para IAFIS. El resultado es un producto de software libre llamado Universal Latent Workstation (ULW). Este software se puede ejecutar en una PC independiente, ya sea con un escáner plano o una interfaz de cámara digital. También se puede ejecutar en estaciones de trabajo latentes proporcionadas por el vendedor. Como mínimo, al especificar un AFIS en una compra, se debe ordenar que el AFIS sea capaz de generar búsquedas remotas a IAFIS. Se recomienda además, que el comprador pida la capacidad de realizar la función ULW para que los proveedores puedan integrar el ULW a sus sistemas.

El ULW también proporciona la capacidad de lanzar búsquedas de impresión de imágenes latentes en el IAFIS, sin necesidad de codificar manualmente las minucias cuando se trabaja con impresiones de huellas latentes de alta calidad.

6.3 Estándares

6.3.1 Antecedentes

Los estándares son acordados mutuamente con base en los atributos de los productos, sistemas, protocolos de comunicación, etc. Los estándares son lo que permite a la gente comprar focos hechos en Hungría, Estados Unidos o Japón y saber que van a encajar en un tomacorriente estándar. Las industrias y los gobiernos establecen estándares no sólo para conveniencia del consumidor, sino para permitir la competencia por el mismo producto.

Cada nación tiene su propia oficina o grupo administrador de estándares. En los Estados Unidos, es ANSI. A nivel internacional, hay varios organismos. Estos incluyen a la Organización Internacional del Trabajo (OIT) y la Organización Internacional de Aviación Civil (OACI) de Naciones Unidas, la Organización Internacional de Policía Criminal (Interpol), la Organización de Estándares Internacionales (ISO) y la Comisión Electrotécnica Internacional (IEC).

Aparte de Naciones Unidas e Interpol, estos organismos de estandarización no "inventan" o "crean" estándares, más bien proporcionan procesos que cuerpos autorizados pueden utilizar para proponer estándares para la aprobación a nivel nacional y luego, a nivel internacional. Las Naciones Unidas y la Interpol tienden a basarse en estos estándares de organismos de estándares nacionales e internacionales en lugar de empezar desde cero.

ANSI tiene oficinas en Nueva York y Washington, DC. ANSI ha autorizado a más de 200 dependencias el proponer estándares. Si todos los procedimientos se

siguen correctamente y no hay objeciones sin dirección, a continuación, los resultados de los esfuerzos de estas dependencias se convierten en estándares ANSI. Las 200 organizaciones incluyen a las siguientes:

- El NIST del Departamento de Comercio
- IAI
- La Asociación Americana de Administradores de Vehículos Motorizados
- El Comité Internacional de Estándares en Tecnologías de la Información (INCITS)

6.3.2 Estándares de huellas dactilares

Las fuerzas de seguridad de todo el mundo han tenido por décadas estándares para el intercambio local de huellas dactilares entintadas. En 1995, la Interpol llevó a cabo una reunión para abordar la transferencia de tarjetas de huellas dactilares en papel y tinta (también conocidas como formas) entre países. Los estándares locales naturalmente tenían diferentes campos de texto, tenían diferentes diseños de campos de texto, se encontraban en diferentes idiomas, y estaban en muchos diferentes tamaños de papel. Antes de que el esfuerzo pudiera llevar a una forma internacionalmente aceptada de huella dactilar, la Interpol se trasladó al intercambio electrónico de huellas dactilares.

En la era de la tinta y el papel, los estándares incluían contenido de fibra y grosor en el papel, durabilidad de la tinta, el tamaño de las "cajas de dedo", y así sucesivamente. Con el cambio a principios de 1990 hacia respuestas en tiempo real para entregar huellas criminales llegó un nuevo conjunto de estándares.

La única forma de presentar, investigar y determinar el estado de las huellas dactilares en pocas horas desde un lugar remoto es a través de la presentación electrónica y de respuestas electrónicas. La fuente aún puede ser en tinta y papel, pero las imágenes necesitan estar digitalizadas y ser presentadas electrónicamente para abordar la creciente demanda de un resultado rápido de las transacciones de las huellas dactilares.

El FBI fue la primera dependencia en migrar la presentación electrónica a gran escala de huellas dactilares desde lugares remotos. Como parte del desarrollo del IAFIS, el FBI trabajó de forma muy cercana con NIST para desarrollar los estándares apropiados para la transmisión electrónica de imágenes de huellas dactilares.

En 1991, NIST llevó a cabo una serie de talleres con expertos forenses, administradores de repositorios de huellas dactilares, representantes industriales y consultores para desarrollar un estándar bajo los lineamientos de ANSI, para el intercambio de imágenes de huellas dactilares. Se aprobó en noviembre de 1993 y el título formal fue "Formato de Datos para el Intercambio de Información de Huellas Dactilares (ANSI NIST-CSL 1-1993)". Este estándar se basó en el estándar de la minuta del Buró Nacional de Estándares de ANSI en 1986 y el estándar ANSI/NBS-ICT 1-1986, el cual no abordó archivos de imagen.

Este estándar NIST de 1993 (y las revisiones posteriores) se volvió conocido en el mundo de la tecnología de huellas dactilares como el "estándar ANSI/NIST". Si se implementa correctamente (por ejemplo, en completo cumplimiento con el estándar y la implementación del FBI), permitiría que las huellas dactilares recolectadas en un escaneo en tiempo real sea compatible para que cualquier proveedor lo pueda leer por medio de otro estándar AFIS y del FBI compatible que llegase a ser construido (en el momento).

El estándar se abrió deliberadamente para permitir que las comunidades de usuarios (también conocidas como dominios de interés) lo personalizaran de acuerdo con el cumplimiento de sus necesidades. Algunas de las áreas personalizables fueron la densidad de imagen (escala de grises de 8 bits o binaria) y campos de texto asociados con una transacción (por ejemplo, nombre, delito). La idea fue que diferentes comunidades de usuarios escribirían sus propios planes de implementación. Las partes obligatorias del estándar ANSI/NIST fueron las definiciones de los tipos de registro, los formatos binarios para las huellas dactilares y las imágenes de firmas, y dentro de ciertos tipos de registro, la definición de campos "encabezado" tales como el tipo de compresión de imagen.

6.3.2.1 Tipos de registro. Para que una transacción sea considerada compatible con ANSI/NIST, los datos deben enviarse de manera estructurada con una serie de registros que se alineen con los tipos de registro de ANSI/NIST tal como se implementaron en un dominio de usuario específico (por ejemplo, Interpol).

- Todas las transmisiones (también conocidas como transacciones) tienen que empezar con un registro tipo 1 que es básicamente una tabla de contenidos para la transmisión, el campo del tipo de transacción (por ejemplo, AUTO para "presentación de la ficha decadactilar

delictiva—respuesta requerida") y la identidad tanto de los organismos emisores y receptores.

- Los registros tipo 2 pueden contener información definida por el usuario, asociada con el sujeto de la transmisión de las huellas dactilares (tales como nombre, fecha de nacimiento, etc.) y el propósito de la transacción (ciclo de arresto, revisión de antecedentes del solicitante, etc.). Estos campos se definen en el estándar de implementación del dominio de interés (por ejemplo, los EFTS del FBI). Cabe aclarar que los registros de tipo 2 también son utilizados para respuestas por parte de las AFIS. Estas caen en dos categorías: mensajes de error y resultados de búsqueda. Su uso real se define en la especificación dominio.

- Los tipos 3 (escala de grises de baja resolución), 4 (escala de grises de alta resolución), 5 (binarios de baja resolución) y 6 (binarios de alta resolución) se ajustaron para la transmisión de las imágenes de huellas dactilares en diferentes estándares (500 ppi para alta resolución y 256 ppi para baja resolución) y densidad de imagen (8 bits por pixel en escala de grises) o binario (1 bit por pixel en blanco y negro). Cabe destacar que todas las imágenes para los registros del tipo 3 al 6 se adquirirán a un mínimo de 500 ppi; sin embargo, las imágenes en baja resolución se rebajan para muestra a 256 ppi para la transmisión. Hay pocas implementaciones ANSI/NIST, si es que las hay, que soporten imágenes de tipo 3, 5 ó 6 (ver la explicación más adelante). Ninguno de estos tres tipos de registro se recomiendan para el uso mediante examinadores latentes o técnicos de huellas dactilares.

- El tipo 7 se estableció para imágenes definidas por el usuario (por ejemplo, imágenes latentes, rostros) y, hasta la actualización del estándar ANSI/NIST en 2000, fue el tipo de registro para el intercambio de imágenes latentes. Este tipo de registro puede ser utilizado para enviar copias escaneadas de documentos de identidad y así sucesivamente. De nuevo, la especificación de dominio determina los usos legítimos del registro tipo 7.

- El tipo 8 se definió para firmas (del sujeto o persona que toma las huellas) y no se utiliza en muchos dominios.

- El tipo 9 se definió para un conjunto mínimo de nimiedades que pudieran ser enviadas a cualquier AFIS que fuera compatible con ANSI/NIST.

El primer plan de implementación tal fue el EFTS del FBI emitido en 1994. Los EFTS delimitaron qué tipo de registros, de los nueve definidos en el estándar ANSI/NIST, utilizaría el FBI y definieron los campos de datos tipo 2. La decisión clave que el FBI hizo fue que sólo aceptaría imágenes de 500 ppi en escala de grises o, en lenguaje ANSI/NIST, imágenes tipo 4. Como resultado de esa decisión, todos los sistemas de procuración de justicia desde entonces han especificado las imágenes tipo 4 y no aceptan las de tipo 3, 5 ó 6, las cuales han caído en desuso a causa de estas demandas en los Estados Unidos.

Los registros tipo 4 comienzan con la información del encabezado al frente de la imagen. Los encabezados le dicen a la computadora qué dedo corresponde a qué imagen, ya sea de un escaneo en tiempo real o de una tarjeta entintada, el tamaño de la imagen en número de pixeles de ancho y alto, y ya sea que la imagen sea de una impresión en rollo o de una impresión plana.

6.3.2.2 Calidad de imagen. Tanto el estándar ANSI/NIST y el EFTS carecieron de medidas o estándares de calidad de imagen. El FBI añadió después los EFTS con un Estándar de Calidad de Imagen (IQS) conocido como Apéndice F (más tarde, un reducido conjunto de especificaciones de calidad de imagen se añadieron como Apéndice G porque la industria no se estaba uniformemente preparada para cumplir con los estándares de la Apéndice F). El IQS define los estándares mínimamente aceptables para el equipo utilizado en la captura de huellas dactilares. Hay seis términos de ingeniería especificados en el IQS. Estos son:

1. Exactitud de imagen geométrica—la habilidad del escáner para mantener las distancias relativas entre los puntos en un objeto (por ejemplo, dos nimiedades) iguales a las distancias relativas a la imagen saliente.

2. Función de transferencia de modulación (MTF)—la habilidad del aparato de escaneo para capturar información de baja frecuencia (las crestas mismas) y de alta frecuencia (detalles de los bordes de las crestas), dentro de los estándares mínimos de las huellas dactilares.

3. Relación señal-ruido—la habilidad del aparato de escaneo para digitalizar la información sin introducir demasiada interferencia electrónica (eso es, con las partes de la imagen blanca pura apareciendo en blanco puro y las partes de la imagen negra pura apareciendo totalmente negras).

4. Rango de escala de grises de los datos de imagen—evitando imágenes de bajo contraste excesivo al asegurar que los datos de imagen se dispersen a través del número mínimo de sombras de gris.

5. Linealidad de la escala de grises—a medida que el nivel de gris cambia en la captura de una huella dactilar, la imagen digital refleja una relación de nivel de gris a través de las sombras de gris.

6. Uniformidad de salida del nivel de grises—la habilidad del aparato de escaneo para crear una imagen con una escala continua de gris a través de un área en la imagen de entrada (examinada utilizando una imagen de prueba especial) que tenga un solo nivel de gris.

Curiosamente, solo dos de estos seis estándares de calidad de imagen aplican a aparatos de escaneo latentes: exactitud de imagen geométrica y MTF. De hecho, el FBI no certifica (ver más adelante la discusión de productos certificados) escáneres para uso latente pero recomienda que los examinadores latentes compren el equipo con el que se sientan cómodos usando desde una perspectiva de calidad de imagen. Pero el Apéndice F del EFTS no ordena que las imágenes latentes se capturen a 1000 ppi.

No existen estándares para la calidad de la huella dactilar real, pero el escaneo en tiempo real y los proveedores de AFIS han clasificado la calidad de las huellas dactilares por años. Ellos saben que la calidad de las huellas dactilares es posiblemente el factor más fuerte en la confiabilidad de un AFIS que exitosamente empareje una huella dactilar con otra en el repositorio. Estas clasificaciones se factorizan a menudo en algoritmos AFIS.

En un escrito titulado "El papel de la Calidad de Datos en los Sistemas Biométricos" (Hicklin y Khanna, 2006), los autores escribieron lo siguiente:

> Cabe destacar que esta definición de la calidad de datos va más allá de la mayoría de discusiones sobre la calidad biométrica, la cual se enfoca en el concepto de la calidad de muestra. La calidad de muestra trata con la fidelidad de captura de las características físicas del sujeto y el contenido de los datos intrínsecos de esas características. Sin embargo, un asunto de igual importancia para cualquier sistema operativo es la calidad de metadatos: las bases de datos necesitan estar al tanto de las relaciones erróneas entre los elementos de los datos, los cuales generalmente se generan por causas administrativas más que por causas biométricamente específicas.

Aunque no existen estándares para la calidad de la imagen de las huellas dactilares, NIST ha investigado la relación entre la calidad de imagen calculada (usando algoritmos similares a aquellos empleados por los proveedores de AFIS), emparejada exitosamente con las relaciones en sistemas de identificación de huellas dactilares. Esto llevó a que NIST desarrollara y publicara un software para medir la calidad de imagen de las huellas dactilares.

El software se llama NIST Finerprint Image Software 2. Fue desarrollado por el grupo de imagen de NIST para el FBI y el Departamento de Seguridad Nacional de los EE.UU. y se encuentra disponible de manera gratuita en las dependencias de procuración de justicia así como para los fabricantes e investigadores biométricos. El CD contiene un código fuente para 56 servicios y una guía de usuario.

El siguiente resumen es de la página Web de NIST en 2007:

> Nueva a este lanzamiento hay una herramienta que evalúa la calidad del escaneo de una huella dactilar al momento en que es realizada. Problemas tales como piel reseca, el tamaño de los dedos y la calidad y condición del equipo utilizado puede afectar la calidad de la impresión y su habilidad para emparejarse con otras impresiones. La herramienta clasifica cada escaneo en una escala del 1, para una impresión de alta calidad, al 5, para una que no se puede utilizar. "Aunque la mayoría de los sistemas de huellas dactilares comerciales ya incluyen un software propietario de calidad de imagen, el software de NIST por primera vez permitirá a los usuarios que comparen directamente la calidad de imagen de las huellas desde los escáneres hechos por diferentes fabricantes", dijo la dependencia.

6.3.2.3 Lista de productos certificados. Para ayudar a que la comunidad forense compre equipo compatible con IQS, el FBI estableció un programa de certificación. Los proveedores podrán probar por sí mismos su equipo y presentar los resultados al FBI donde, con la asistencia técnica de Mitretek, los resultados serán evaluados. Si los resultados son aceptables, se enviará una carta de certificación al proveedor. Es importante saber que, para los aparatos de captura, hay una combinación de las ópticas (escáner), software de procesamiento de imagen y el sistema operativo que se está probando. Por lo consiguiente, las cartas de certificación no se emiten para

un escáner sino para una configuración de un escáner y una PC que incluya un modelo de escáner específico, conectado a una PC que corra un sistema operativo específico y cualquier controlador de escaneo de mejora de imagen que sean utilizados.

Razón por la cual los fabricantes mejoran los escáneres, puede ser difícil comprar piezas de equipo certificadas previamente. Una lista completa de todo el equipo certificado se mantiene en el sitio web del FBI bajo la sección CJIS.

6.3.2.4 Compresión. Casi al mismo tiempo de la escritura de los EFTS, el FBI optó por el estándar de compresión para las transmisiones de ANSI/NIST. Dado que la relación de datos (ancho de banda) de los sistemas de telecomunicación era muy bajo en 1993, comparada con las relaciones de hoy en día, y que el costo de almacenamiento en disco era un tanto alto, el FBI eligió comprimir las imágenes de huellas dactilares usando una técnica llamada Cuantificación Escalar Ondícula (WSQ).

El plan inicial fue que las transmisiones decadactilares se comprimieran mediante una WSQ a 20:1 y que las imágenes latentes permanecieran sin comprimir. Una tarjeta de huellas dactilares del FBI a principios de los años 90 tenía un área de superficie para las huellas dactilares que tenía 8 pulgadas de ancho y 5 pulgadas de alto para un total de 40 pulgadas cuadradas. Escanear a 500 ppi en la dirección de 8 pulgadas (X) y en la de 5 pulgadas (Y) arrojaron un total de 10 millones de bytes de información (10 MB). La compresión a 20:1 produciría un archivo con la mitad del peso (0.5 MB) que fuera mucho más fácil de transmitir y almacenar.

En la Conferencia Anual de Entrenamiento de IAI de 1993 en Orlando, FL., la Junta Directiva de IAI expresó sus preocupaciones al director del programa IAFIS sobre la relación de compresión propuesta de 20:1. El FBI accedió a apoyar un asesoramiento independiente del impacto de la compresión en la ciencia de la identificación de huellas dactilares por parte del comité de IAI AFIS, bajo el Mando de Mike Fitzpatrick de Illinois (Comité de IAI AFIs, 1994). Como resultado del estudio, el FBI acordó reducir la compresión promedio a 15:1 (Higgins, 1995, pág. 409-418).[5]

[5] The study showed that expert latent print examiners were unable to differentiate original images from those compressed at either 5:1 or 10:1 when presented with enlargements on high-quality film printers. One possible implication of that study was that latent images might safely be compressed at 2:1 (or possibly even more) for transmission, with no loss of information content. Currently, there are no agencies reporting the use of compression with latent images.

Mientras otros dominios de interés adoptaron el estándar ANSI/NIST alrededor del mundo (los primeros que lo adoptaron incluían a la Real Policía Montada de Canadá y al Ministerio de Interior del Reino Unido), todos usaron el EFTS como un modelo y todos incorporaron los estándares de IQS por referencia. Con una o dos excepciones, también adoptaron la compresión WSQ a 15:1.

Con la migración hacia relaciones de escaneo más altas para las transacciones decadactilares, la tecnología de compresión preferente es JPEG 2000, la cual es una técnica de compresión basada en Ondícula. Actualmente (desde 2007), existen al menos cinco sistemas de identificación automática de huellas decadactilares basadas en imagen a 1000 ppi. Tanto Cogent como Motorola han sacado sistemas de 1000-ppi. Se anticipa que otros proveedores sacarán dichos sistemas a medida que la demanda incremente. Dado que los sistemas de escaneo en tiempo real más antiguos que operaban a 500 ppi pueden presentar transacciones a estos nuevos sistemas de identificación de huellas dactilares, es importante que sean capaces de trabajar en un ambiente de densidad mezclada (500-ppi y 1000-ppi).

Los cuatros proveedores más importantes de AFIS demostraron la capacidad de adquirir, almacenar y procesar huellas decadactilares y huellas palmares de 1000-ppi durante el Parámetro de AFIS de la Real Policía Montada de Canadá, en 2005. Es importante señalar que estos sistemas adquieren las imágenes decadactilares y palmares a 1000 ppi para archivarlas pero las reducen para su muestra a 500 ppi para buscar y crear una imagen que se utilice en AFIS. Actualmente, las imágenes a 1000-ppi se usan primariamente como muestra en estaciones de trabajo del examinador latente. A medida que los sistemas de identificación de huellas dactilares automáticos migran al uso de características de tercer nivel, se asume que las imágenes de resolución más grandes desempeñarán un papel en los algoritmos.

6.3.3 Actualizaciones del estándar ANSI/NIST

Desde 1993, el estándar ANSI/NIST ha sido actualizado tres veces, las más recientes en 2007 y 2008. Los cambios clave fueron los siguientes:

- En 1997, se añadieron transacciones tipo 10 para permitir que las imágenes de marcas faciales, cicatrices y tatuajes se transmitieran con transacciones de huellas

dactilares. El título del documento fue cambiado por: "Formato de Datos para el Intercambio de Información de Huella Dactilar, Facial y CMT (Cicartiz, Marca y Tatuaje) (ANSI / NIST-ITL 1a-1997)".

- En 2000, los tipos 13 al 16[6] se añadieron para apoyar imágenes de mayor densidad, imágenes latentes en un nuevo formato, imágenes de palma e imágenes de prueba, respectivamente (ANSI/NIST-ITL 1-2000).
- NIST realizó dos talleres en 2005 para determinar si había nuevas áreas que se debían agregar. Los principales cambios deseados eran la adición de tipos de registro estándar para tipos de datos biométricos más allá de los dedos y rostros (por ejemplo, imágenes del iris) y la introducción de datos XML en los registros tipo 2. También se propusieron varios cambios y adiciones. (Ver las revisiones de 2007 y 2008, ANSI/NIST-ITL 1 2007 y 2-2008.)

6.3.4 Primeras demostraciones de interoperabilidad

Para 1996, el Comité IAI AFIS estaba organizando y gestionando (bajo las presidencias de Mike Fitzpatrick, Peter Higgins y Ken Moses) una serie de demostraciones de interoperabilidad de las transacciones de imágenes decadactilares procedentes del software Aware, Comnetix Live Scan e Identix Live Scan, que se convirtieron en Cogent Systems, Printrak (ahora Motorola) y Sagem Morpho, todos eran sistemas automáticos de identificación dactilar. El segundo año de estas manifestaciones (1998) vio la misma entrada que se presentó entre los sitios operacionales AFIS, por parte de los mismos tres proveedores de AFIS a lo largo de toda la red Nlets (Informe del Comité AFIS, 1998, pág. 490).

6.3.5 Interoperabilidad latente

Cuando se desarrollaba IAFIS, el FBI estableció (en el EFTS) dos maneras para que funcionaran las impresiones latentes a través de IAFIS desde fuera de las dependencias.

6.3.5.1 Presentaciones remotas. La dependencia con la impresión latente puede enviar (electrónicamente o por correo) la impresión (como una imagen en el caso de la presentación electrónica) al FBI, y el personal del FBI realizará la edición, codificación, búsqueda y evaluación de candidatos. El FBI tomará cualquier decisión de identificación y devolverá los resultados a la dependencia de presentación. Este proceso imita el flujo de trabajo de pre-IAFIS, pero añade la opción de presentación electrónica.

6.3.5.2 Búsquedas remotas. La dependencia con la impresión latente realiza la edición y codificación y luego envía (electrónicamente) una búsqueda de características de huella latente (LFFS) a IAFIS para la búsqueda. IAFIS devuelve una lista de candidatos, incluyendo imágenes de los dedos, a la dependencia de origen para realizar la evaluación de candidatos. La dependencia de presentación hace cualquier decisión de identificación. Para apoyar la capacidad de búsqueda remota de LFFS, el FBI publicó la definición "nativa" del conjunto de características de IAFIS.

Muchas dependencias y departamentos civiles han querido ser capaces de ofrecer búsquedas decadactilares remotas, pero los conjuntos de características de los principales proveedores de AFIS son propietarios. En 2006, el NIST realizó un estudio sobre la interoperabilidad del nivel conjunto de características nativas de muchos AFIS y empresas de escaneo en tiempo real y comparó a los que tienen el rendimiento de minucias del estándar de la plantilla de huellas dactilares de INCITS 378 (el conjunto básico A y el conjunto más rico B).

El Reporte MINEX (Grother et al., 2006) muestra que la interoperabilidad basada en minucias es posible (con alguna pérdida de confiabilidad y exactitud) por medio de sistemas de verificación de un solo dedo. El reporte es cuidadoso al puntualizar que el uso de las plantillas INCITS 378 para las búsquedas de fichas decadactilares criminales remotas y latentes es desconocido y no puede ser extrapolado con seguridad a partir de ese reporte.

Ya que la mayoría de los AFIS (otros que no sean IAFIS) no poseen funcionalidad LFFS remota (hasta 2007), la interoperabilidad latente en el nivel de imagen usualmente requiere trabajo por parte de la dependencia de búsqueda. El deseo de mover esa carga de trabajo a una dependencia de presentaciones es natural porque la mayoría tienen algún nivel de exceso de capacidad que podría posiblemente soportar las búsquedas latentes remotas durante las horas no laborales.

[6] Los tipos 11 y 12 se pusieron de lado para un proyecto que nunca rindió frutos y no se utilizan en el Informe del Comité del estándar AFIS, 1998.

6.4 Digitalización y Procesamiento de Huellas Dactilares

6.4.1 Algoritmos

Las demandas impuestas por la esmerada atención, necesaria para que a la vista coincidan las huellas dactilares de cualidades diversas, el tedio de la naturaleza monótona del trabajo manual y el aumento de las cargas de trabajo debido a una mayor demanda de servicios de reconocimiento de huellas dactilares impulsaron a las dependencias de cumplimiento de la ley para iniciar la investigación sobre la adquisición de huellas dactilares a través medios electrónicos y a automatizar la individualización de éstas basados en la representación digital de las huellas dactilares. Como resultado de esta investigación, un gran número de algoritmos informáticos se han desarrollado durante las últimas tres décadas para procesar automáticamente las imágenes de huellas dactilares. Un algoritmo es un conjunto finito de instrucciones bien definidas para llevar a cabo alguna tarea que, dado un estado inicial y de entrada, terminará en un estado final correspondiente reconocible y de salida. Un algoritmo de computadora es un algoritmo codificado en un lenguaje de programación para funcionar en un ordenador. Dependiendo de la aplicación, estos algoritmos informáticos, podrían ayudar a los expertos humanos o bien, operar en el modo de apagado de luz. Estos algoritmos han mejorado en gran medida la productividad de las operaciones de las dependencias de cumplimiento de la ley y han reducido el número de técnicos de huellas dactilares necesarios. Aun así, los diseñadores de algoritmos identifican e investigan los siguientes cinco problemas principales en el diseño de los sistemas automatizados de procesamiento de huellas dactilares: la adquisición de huella dactilar, la mejora de imagen, la extracción de características (por ejemplo, las minucias), el emparejamiento y la indexación/recuperación.

6.4.2 Adquisición de la imagen

Los datos de huellas dactilares conocidos se pueden recolectar mediante la aplicación de una fina capa de tinta sobre un dedo y el balanceo del dedo de un extremo de la uña hasta el otro extremo de la uña, mientras se pulsa el dedo contra una tarjeta de papel. Esto daría lugar a un entintado "laminado" de impresión de huellas dactilares en la tarjeta de huellas dactilares. Si el dedo se presiona simplemente hacia abajo en contra de la tarjeta de papel en vez de rodar, la impresión de la huella dactilar resultante sólo contendría una zona central más pequeña del dedo en lugar de la huella dactilar completa, resultando en una impresión "plana" o "normal" de huellas dactilares entintadas.

La transpiración y los contaminantes en la piel resultan en la impresión de un dedo que se deposita sobre una superficie que es tocado por ese dedo. Estas impresiones "latentes" pueden ser química o físicamente reveladas, y electrónicamente capturadas o manualmente "levantadas" desde la superficie mediante el uso de ciertas técnicas químicas, físicas y de iluminación. La huella dactilar revelada puede ser levantada con cinta o fotografiada. A menudo, estas huellas dactilares latentes contienen sólo una parte del detalle en las crestas de fricción que está presente en el dedo, es decir, una huella dactilar "parcial".

Las impresiones de huellas dactilares se desarrollan y conservan usando cualquiera de los métodos anteriores, y pueden digitalizarse mediante el escaneo de la tarjeta de entintado, levantamiento, artículo o una fotografía. Las imágenes digitales adquiridas por este método se conocen como imágenes "off-line". (Por lo general, los escáneres no están diseñados específicamente para aplicaciones de huellas dactilares).

Desde principios de la década de 1970, los sensores de huellas dactilares se han construido para que puedan adquirir una imagen de la huella dactilar por "escaneo en tiempo real (*livescan*)" directamente desde un dedo sin el uso intermedio de tinta y una tarjeta de papel. Aunque las imágenes "off-line" están todavía en uso en ciertas aplicaciones forenses y gubernamentales, se utilizan cada vez más las imágenes de huellas dactilares "on-line". Los principales parámetros que caracterizan una imagen de la huella dactilar son el área de resolución, el número de píxeles, la precisión geométrica, el contraste y la distorsión geométrica. La CJIS liberó las especificaciones, conocidas como Apéndice F y Apéndice G, que regulan la calidad y el formato de imágenes de las huellas dactilares y los escáneres compatibles con el FBI. Todos los dispositivos *livescan* fabricados para su uso en aplicaciones forenses y gubernamentales de cumplimiento de la ley son compatibles con el FBI. La mayoría de los dispositivos *livescan* fabricados para ser utilizados en aplicaciones comerciales, como el inicio de sesión en la computadora, no cumplen con las especificaciones del FBI, pero, por otro lado, suelen ser más fáciles de utilizar, compactos y mucho menos costosos. Hay una serie de mecanismos de detección *livescan* (por ejemplo, ópticos, capacitivos, térmicos, basados

en presión, ultrasonidos, etc.) que pueden ser utilizados para detectar las crestas y valles presentes en la yema del dedo. Sin embargo, muchos de estos métodos no proporcionan imágenes que contengan la misma representación de detalles necesarios para algunas comparaciones de huellas dactilares latentes. Por ejemplo, una imagen capacitiva o térmica puede representar los bordes y poros de una manera muy diferente a una impresión de tinta enrollada. La Figura 6-6 muestra una imagen de la huella "off-line" adquirida con la técnica de tinta, una imagen de la huella latente y algunas imágenes *livescan* adquiridas con diferentes tipos de dispositivos *livescan* comerciales.

Los dispositivos *livescan* suelen capturar una serie de imágenes de huellas dactilares a partir de una sola exploración en lugar de una sola imagen. Dependiendo de la aplicación para la que el dispositivo livescan fue diseñado, puede ejecutar uno o varios algoritmos utilizando un microprocesador incorporado de recurso limitado (memoria y potencia de procesamiento) o mediante una computadora conectada. Por ejemplo, las estaciones de reserva *livescan* generalmente ejecutan un algoritmo que puede presentar en forma de mosaico (puntada) con múltiples imágenes adquiridas como un video durante una sola rodadura de un dedo sobre el escáner en una gran imagen laminada. Los algoritmos también suelen ejecutar un sistema de gestión de reserva integrada para proporcionar vistas previas en tiempo real (interfaz gráfica de usuario y zoom) para ayudar al operador en la colocación o alineación correcta de los dedos o las palmas de las manos. Normalmente, un algoritmo de revisión de calidad de la imagen de una huella dactilar también se ejecuta para alertar al operador sobre

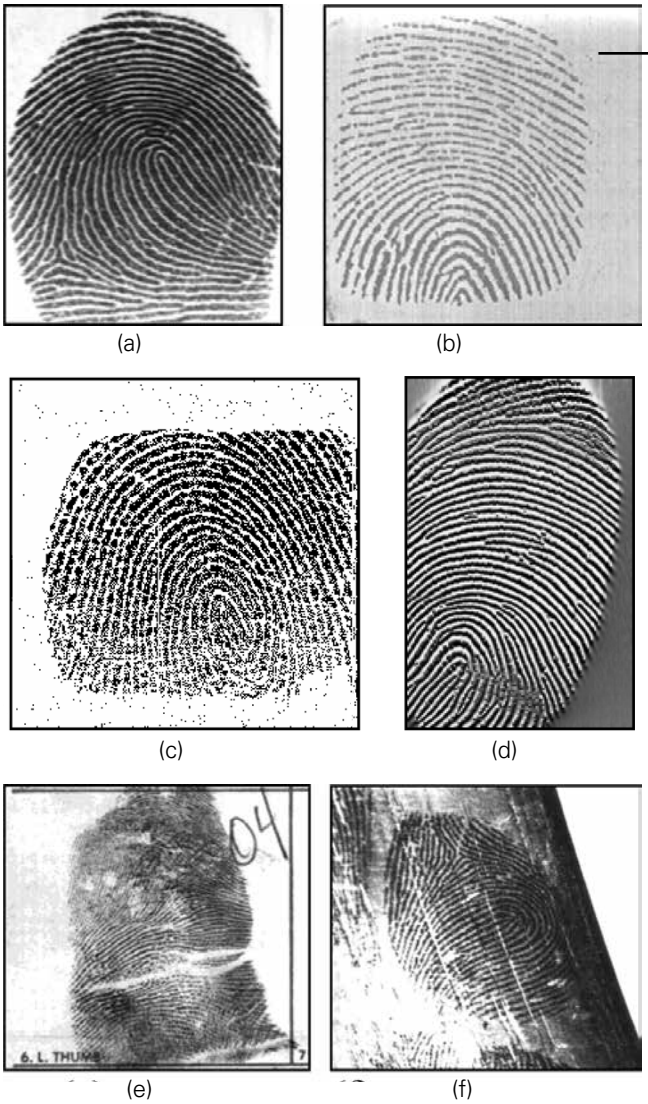


FIGURA 6–6

Imágenes de huellas dactilares de
(a) un escáner óptico livescan basado en FTIR;
(b) un escáner capacitivo livescan;
(c) un escáner pieza eléctrica livescan:
(d) un escáner térmico livescan;
(e) una impresión entintada "off-line";
(f) una huella dactilar latente.

la adquisición de una imagen de la huella con mala calidad, para que una de mejor calidad se pueda volver a adquirir del dedo o la palma. La salida típica de un algoritmo automático de corrector de calidad de este tipo se muestra en la Figura 6-7.

Aunque los escáneres ópticos tienen la historia más larga y la más alta calidad, los nuevos sensores de estado sólido están ganando gran popularidad debido a su tamaño compacto y la facilidad con la que pueden ser incorporados en las computadoras portátiles, teléfonos celulares, bolígrafos inteligentes, asistentes digitales personales (PDA) y similares. Los sensores Swipe, donde se requiere un usuario que deslice su dedo por un sensor *livescan* que es amplia pero muy corta, pueden ofrecer el costo y el tamaño más bajo. Dichos sensores crean una imagen de una sola línea o sólo unas pocas líneas (lámina) de una huella dactilar y un algoritmo de costura de imagen que se utiliza para unir las líneas o láminas para formar una imagen bidimensional de la huella dactilar (Figura 6-8).

Dependiendo de la aplicación, puede ser deseable implementar uno o más de los siguientes algoritmos en el aparato *livescan*:

- Algoritmo de detección automática del dedo—El escáner automáticamente sigue buscando la presencia de un dedo en su superficie y, tan pronto como se determina que hay presente un dedo en su superficie, éste alerta al sistema.
- Algoritmo de captura automática de huellas dactilares—Inmediatamente después de que el sistema ha sido alertado de que un dedo está presente en la superficie del escáner, se inicia la recepción de una serie de imágenes y el algoritmo de captura automática de huellas

FIGURA 6–7

(a) Una huella dactilar de buena calidad; (b) Una huella dactilar de calidad media con pliegues; (c) Una huella dactilar de baja calidad; (d) Una huella dactilar de muy baja calidad que contiene mucho ruido.

(a) Índice de calidad = 0.9 (b)) Índice de calidad = 0.7

(c) Índice de calidad = 0.4 (d) Índice de calidad = 0.2

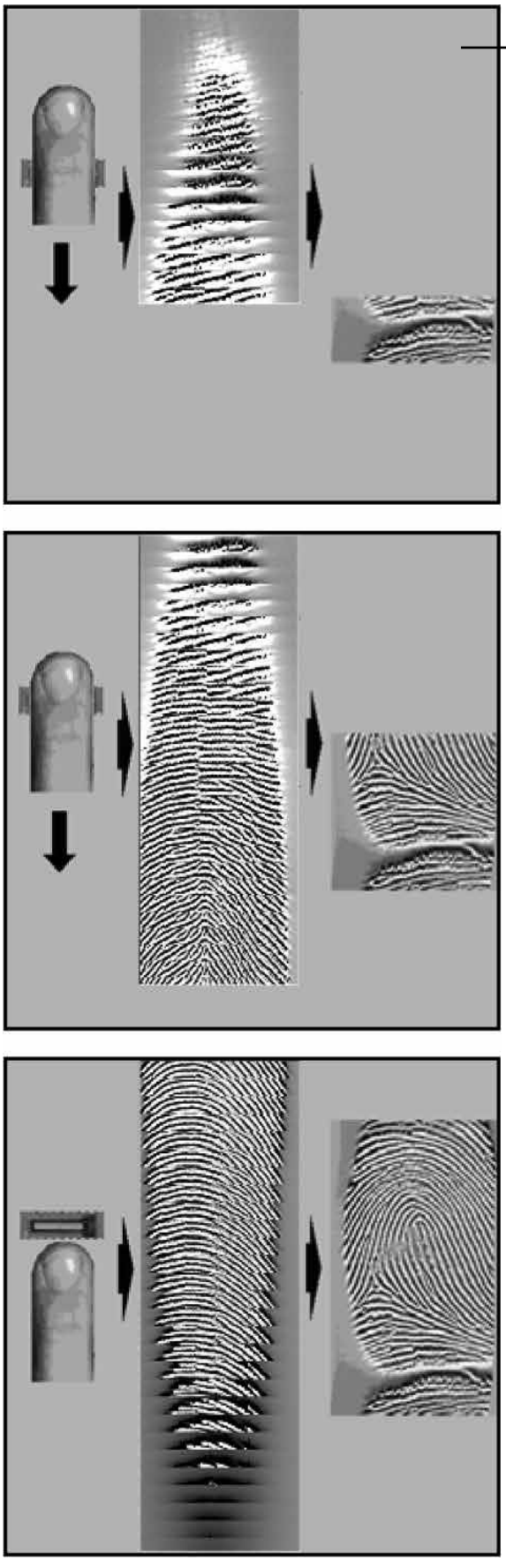


FIGURA 6–8

A medida que el usuario desliza su dedo en el sensor, el sensor entrega nuevas láminas de imagen, las cuales se combinan en una imagen bidimensional.

dactilares determina automáticamente qué fotograma de la secuencia de imágenes tiene la mejor calidad de imagen y elige esa toma del video para su posterior procesamiento de imágenes y emparejamiento.

- Algoritmo de detección de vitalidad—El escáner puede determinar si el dedo es consistente con la deposición de un ser humano vivo.
- Algoritmo de compresión de datos de imagen—La imagen comprimida requerirá menos capacidad de almacenamiento y ancho de banda cuando se transfiera al sistema.
- Algoritmos de procesamiento de imágenes—Ciertas aplicaciones se beneficiarán de la función de extracción llevada a cabo en el propio sensor; la transferencia de las características de huellas dactilares también requerirá menos ancho de banda que la imagen.
- Algoritmo de emparejamiento de imagen—Ciertas aplicaciones desearán que el emparejamiento de huellas dactilares se realice en el sensor por razones de seguridad, sobre todo para el control de la secuencia a bordo.
- Algoritmos y protocolo (s) criptográficos -Implementados en el escáner para llevar a cabo una comunicación segura.

6.4.3 Mejora de imagen

Las imágenes de huellas dactilares procedentes de diferentes fuentes pueden tener diferentes características de ruido y por lo tanto pueden requerir algunos algoritmos de mejora basados en el tipo de ruido. Por ejemplo, las imágenes de huellas dactilares latentes pueden contener una variedad de artefactos y ruido. Las huellas dactilares entintadas pueden contener manchas o crestas rotas que se deben a una cantidad excesiva o inadecuada de tinta. Las tarjetas de papel archivadas pueden contener inscripciones superpuestas y demás a las huellas dactilares. El objetivo de los algoritmos de mejora de la huella dactilar es producir

una imagen que no contenga una estructura de cresta generada artificialmente, la cual más tarde podría dar lugar a la detección de características de falsas minucias, mientras se captura la estructura máxima de la cresta disponible para permitir la detección de la verdadera minucia. Adaptar el proceso de mejora para el método de captura de huellas dactilares puede producir un rendimiento de adaptación óptimo a través de una gran colección de huellas dactilares.

Una huella dactilar puede contener dichas áreas de baja calidad en las que los algoritmos de orientación de la cresta y de estimación de frecuencia están completamente equivocados. Un algoritmo de mejora que puede localizar de forma fiable (y enmascarar) estas áreas de extremadamente mala calidad es muy útil para las etapas posteriores de detección de características y las etapas de individualización al prevenir que se creen características falsas o no confiables.

Las imágenes de huellas dactilares a veces pueden ser de mala calidad debido al ruido introducido durante el proceso de adquisición. Por ejemplo: un dedo puede estar sucio, una huella latente puede ser levantada desde una superficie difícil, el medio de adquisición (tarjeta de papel o livescan) puede estar sucio o el ruido puede introducirse durante la interacción del dedo con la superficie de detección (por ejemplo, como el deslizamiento u otro contacto inconsistente). Cuando se presenta una imagen de mala calidad, un experto forense usaría una lupa y trataría de descifrar las características de las huellas dactilares en presencia de ruido. Los algoritmos de mejora automática de imagen de huellas dactilares pueden optimizar significativamente la calidad de las crestas de las huellas dactilares en la imagen de las mismas y hacer la imagen más adecuada para su posterior procesamiento manual o automático. Los algoritmos de mejora de imagen no añaden ninguna información externa a la imagen de la huella. Los algoritmos de mejora utilizan sólo la información que ya está presente en la imagen de la huella. Los algoritmos de mejora pueden suprimir diferentes tipos de ruido (por ejemplo, otra huella latente, el color de fondo) en la imagen de la huella y poner en relieve las características útiles existentes. Estos algoritmos de mejora de imagen pueden ser de dos tipos.

***6.4.3.1 Mejora de las impresiones latentes para la búsqueda de AFIS.*.** En el caso de búsquedas latentes en el AFIS forense, el algoritmo de mejora es interactivo, es decir, la retroalimentación en vivo sobre la mejora se proporciona al experto forense a través de una interfaz gráfica de usuario. A través de esta interfaz, el experto forense es capaz de utilizar varios algoritmos para elegir la región de interés en la imagen de la huella, recortar la imagen, invertir el color, ajustar la intensidad, voltear la imagen, ampliar la imagen, cambiar el tamaño de la ventana de la imagen y aplicar algoritmos de compresión y descompresión. El experto forense puede aplicar selectivamente muchos de los algoritmos de mejora disponibles (o seleccionar los parámetros del algoritmo), basado en la retroalimentación visual. Tales algoritmos pueden incluir la ecualización del histograma, cambio en la escala de intensidad de imagen, ajustes de intensidad de imagen con umbrales altos y bajos, aumento del contraste local o global, sustracción del fondo local o global, ajustes de nitidez (aplicando filtros de paso alto), supresión de fondo (filtro de paso bajo), ajustes de gamma, ajustes de brillo y contraste, y así sucesivamente. Un ejemplo de mejora del contraste de área local se muestra en la Figura 6-9. En este ejemplo, el algoritmo de mejora de imagen de la huella aumenta sólo una pequeña área local, cuadrada, de la imagen a la vez, pero atraviesa en toda la imagen de una forma de exploración de trama de tal manera que toda la imagen se mejora.

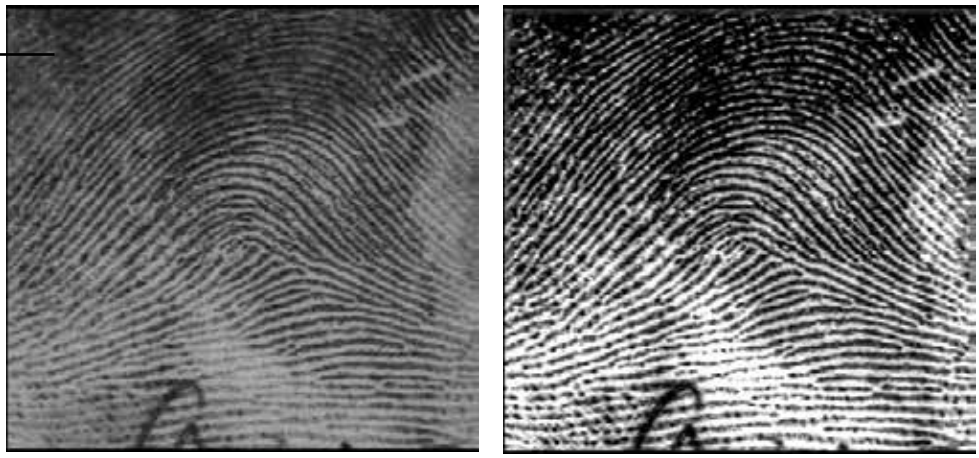


FIGURA 6–9

Un ejemplo de la mejora en el contraste de área local. El algoritmo mejora la imagen completa al optimizar un gran número de pequeñas áreas locales cuadradas.

La extracción de las características de huellas dactilares subsecuente entonces puede ser realizada ya sea de forma manual o por medio de algoritmos automáticos de extracción de características de huellas dactilares.

6.4.3.2 Mejora automática de las imágenes de huellas dactilares. En el caso de las aplicaciones a luz apagada (frecuentemente usadas en revisiones de antecedentes automatizadas y en aplicaciones comerciales para el control del acceso físico), la ayuda humana no sucede en el proceso de individualización de la huella dactilar. Los algoritmos de mejora se usan en modo completamente automático para mejorar las estructuras de las crestas de las huellas dactilares en imágenes de baja calidad de las mismas.

Un ejemplo de un algoritmo de mejora totalmente automatizado de la imagen de huella dactilar se muestra en la figura 6-10. En este ejemplo, se utiliza el filtrado contextual que tiene un efecto de paso bajo (suavizado) a lo largo de las crestas en huellas dactilares y un efecto de paso de banda (diferenciación) en la dirección ortogonal a las crestas para aumentar el contraste entre éstas y los valles. A

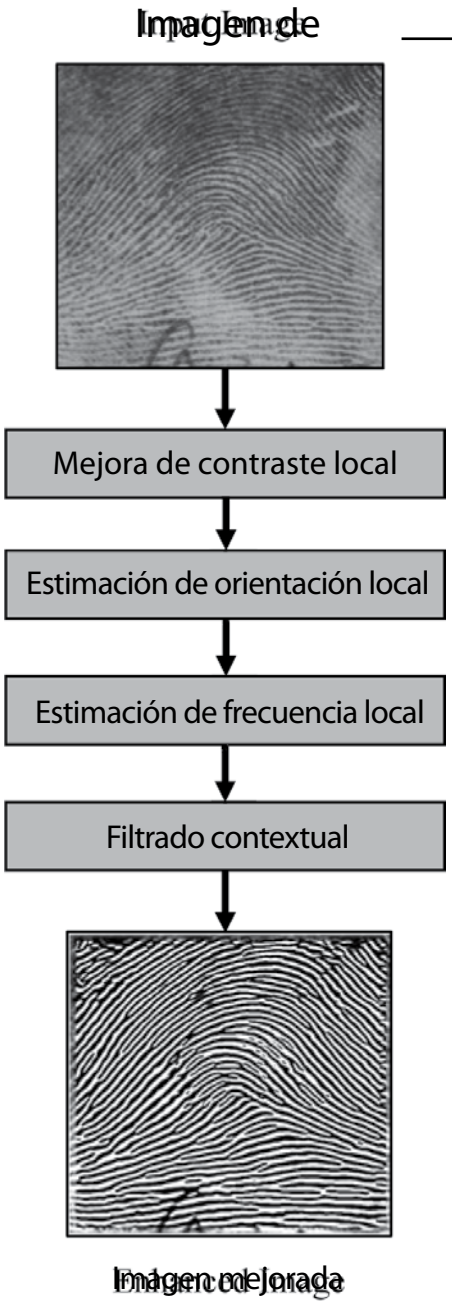


FIGURA 6–10

Etapas de un algoritmo de mejora de imagen de la huella dactilar basada en un filtrado contextual típico.

menudo, los filtros orientados al paso de banda se utilizan para tales filtrados. Uno de dichos tipos de filtros usados comúnmente se conoce como filtros de Gabor. El contexto local es proporcionado a tales filtros contextuales en términos de orientación local y la frecuencia de la cresta local.

6.4.4 Extracción de características

Las singularidades de la cresta de huellas dactilares locales, comúnmente conocidas como *puntos de minucia*, se han utilizado tradicionalmente por los expertos forenses como características discriminantes en imágenes de huellas dactilares. Las singularidades locales más comunes son las terminaciones de las crestas y las bifurcaciones de la cresta. Otros tipos de minucias mencionadas en la lectura, como el lago, isla, estímulo, cruce y así sucesivamente (con la excepción de puntos), son simplemente materiales compuestos de terminaciones de crestas y bifurcaciones. Las minucias compuestas, formadas por dos a cuatro puntos característicos se producen muy cerca unas de otras, también se han utilizado. En el proceso de impresión latente manual, un experto forense localizaría visualmente las minucias en una imagen de huella dactilar y señalaría su ubicación, la orientación de la cresta en la que reside y el tipo de minucias. Los algoritmos de extracción automática de características de las huellas dactilares fueron desarrollados para imitar la ubicación de las minucias realizada por expertos forenses. Sin embargo, la mayoría de los algoritmos de extracción automática de minucias de las huellas dactilares sólo consideran las terminaciones de las crestas y las bifurcaciones porque otros tipos de detalles de las crestas son muy difíciles de extraer automáticamente. Además, la mayoría de los algoritmos no diferencian entre las terminaciones de las crestas y las bifurcaciones, ya que pueden ser indistinguibles como resultado de las diferencias de presión del dedo durante la adquisición o de los artefactos introducidos durante la aplicación del algoritmo de mejora.

Un enfoque común seguido por los algoritmos de extracción de características de huellas dactilares es utilizar primero un algoritmo de binarización para convertir la imagen de la huella mejorada en escala de gris en forma binaria (blanco y negro), donde todos los píxeles negros corresponden a las crestas y los píxeles blancos corresponden a los valles. El algoritmo de binarización va desde un simple umbral de la imagen mejorada hacia algoritmos de localización de la cresta muy sofisticados. Después de eso, un algoritmo de adelgazamiento se utiliza para convertir la imagen de la huella binaria en un único ancho de píxel sobre la línea central de la cresta. La idea central del proceso de adelgazamiento es realizar erosiones sucesivas (iterativas) de las capas exteriores de una forma hasta que se obtiene un conjunto de unidades de ancho conectado por líneas (o esqueletos). Existen varios algoritmos para el adelgazamiento. Los pasos adicionales en el algoritmo de adelgazamiento se utilizan para llenar los poros y eliminar el ruido que puede resultar en la detección de puntos minucia falsos.

A la imagen resultante del algoritmo de adelgazamiento se le llama imagen adelgazada o *imagen esquelética*. Un algoritmo de detección de minucias se aplica a esta imagen esquelética para localizar las coordenadas "x" y "y", así como la orientación (theta) de los puntos de minucias. En la imagen esquelética, por definición, todos los píxeles en una cresta tienen dos píxeles vecinos en la vecindad inmediata. Si un píxel tiene un solo píxel vecino, se determina que es una terminal de la cresta y si un pixel tiene tres píxeles vecinos, se determina que es una bifurcación de la cresta.

Cada uno de los algoritmos utilizados en la mejora de imagen de la huella y en la extracción de minucias tiene su propia limitación y resulta en un procesamiento imperfecto, especialmente cuando la imagen de la huella de entrada incluye ruido de la cresta de no fricción. Como resultado, muchas falsas minucias pueden ser detectadas por el algoritmo de detección de minucias. Para aliviar este problema, a menudo un algoritmo de post procesado de minucias se utiliza para confirmar o validar las minucias detectadas. Sólo aquellas minucias que pasan este algoritmo de post procesado se guardan y el resto se eliminan. Por ejemplo, si una longitud de la cresta que se extiende lejos del punto de minucias es suficiente o si la dirección de la cresta en el punto está dentro de los límites aceptables, las minucias se mantienen.

El post procesamiento puede incluir también una examinación de la calidad de la imagen local, detecciones vecinas u otros indicadores de estructura no relacionada con las huellas dactilares en el área. Más adelante, la imagen puede ser invertida en escala de grises, convirtiendo el blanco al negro y el negro al blanco. El reprocesamiento de esta imagen invertida debe dar paso a las terminaciones de minucias en lugar de las bifurcaciones y viceversa, permitiendo una revisión de validez en las minucias detectadas previamente. Las minucias detectadas al final son aquellas que cumplan todas las revisiones de validez. La Figura 6-11 muestra los pasos en un algoritmo típico de extracción de

características de la huella dactilar; las minucias extraídas se muestran unas sobre otras en la imagen de entrada para su visualización.

Cabe destacar que las etapas y algoritmos descritos en esta sección representan solo el algoritmo típico de extracción de características de la huella dactilar. Existe una amplia variedad de algoritmos de extracción de características de la huella dactilar y todas difieren unas de las otras, algunas veces en cómo se implementan en una cierta etapa y otras veces en las etapas que utilizan y el orden en el cual las utilizan. Por ejemplo, algunos algoritmos de extracción de minucias no utilizan una etapa de post procesamiento. Algunas otras no utilizan una etapa de adelgazamiento de la cresta y el algoritmo de detección de minucias trabaja directamente sobre el resultado del algoritmo de ubicación de minucias. Algunas trabajan directamente sobre la imagen mejorada y algunas otras incluso trabajan directamente en la imagen natural de entrada. Pueden llegar a utilizarse etapas y algoritmos adicionales.

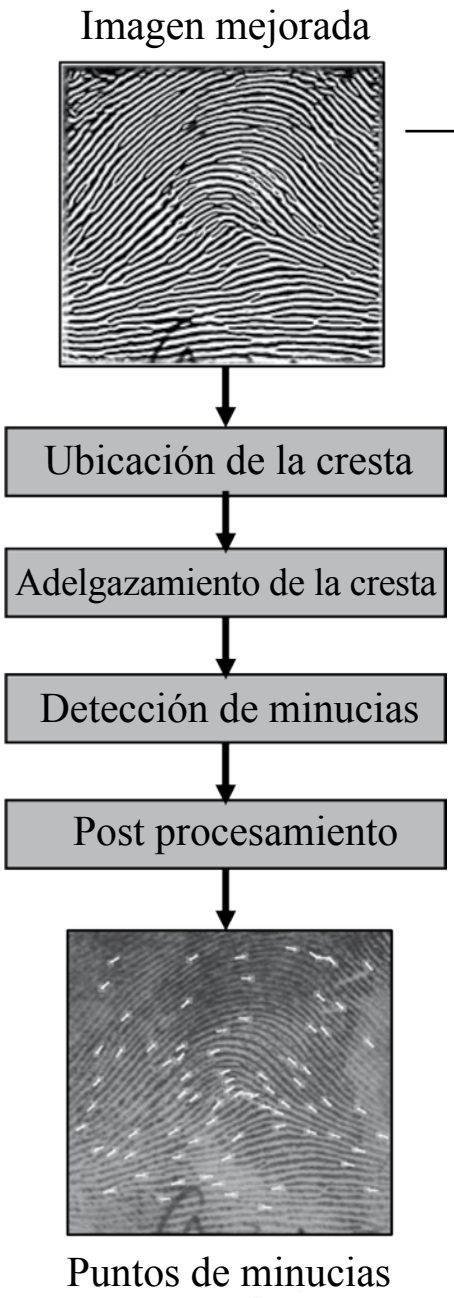


FIGURA 6–11

Etapas en un algoritmo típico de extracción de minucias de huella dactilar.

Muchas otras características pueden extraerse también aunadas a las minucias. Estas características adicionales a menudo proveen información útil que puede ser utilizada en las etapas de emparejamiento subsecuentes para mejorar la exactitud del emparejamiento de las huellas dactilares. Por ejemplo, la fiabilidad de las minucias, las cuentas de crestas entre las minucias, la fiabilidad de la cuenta de crestas, las ubicaciones del núcleo y delta, las medidas de calidad local y, que así sucesivamente, puedan ser extraídas. Estas características adicionales pueden ser útiles para alcanzar la selectividad añadida del proceso de emparejamiento de minucias. Su utilidad para este propósito puede mediarse a través de la fiabilidad asociada con cada una de las características. Por lo tanto, es importante recolectar datos de fiabilidad como parte del mejoramiento de imagen y del proceso de extracción de características para que sea posible calificar las minucias detectadas y las características asociadas.

Los primeros algoritmos de extracción de características de las huellas dactilares fueron desarrollados para imitar la extracción de características por parte de los peritos forenses. Recientemente, ha emergido un número de algoritmos automáticos de extracción (y emparejamiento) de características de huellas dactilares que utilizan información que no está basada en minucias de las imágenes de huellas dactilares. Por ejemplo, los poros sudoríparos, que son muy minuciosos en los de detalles de las huellas dactilares, más pequeños que los puntos de minucias, se han extraído exitosamente a través de los algoritmos de imágenes de huellas dactilares de alta resolución. Otras características que no están basadas en minucias a menudo son características de bajo nivel (por ejemplo, las características de textura) que no tienen un significado de alto nivel, tales como la terminación de la cresta o la bifurcación. Estas características son muy apropiadas para la representación y emparejamiento en máquina y pueden utilizarse en lugar de las características de minucias. Con frecuencia, una combinación de características de minucias y otras que no están basadas en éstas pueden proveer la mejor exactitud en el sistema automático de individualización de huella dactilar. Los peritos forenses utilizan tales características finas implícitamente, junto con las características de las terminaciones normales de la cresta y las bifurcaciones, durante la examinación.

6.4.5 Emparejamiento

El emparejamiento de la huella dactilar puede definirse como el ejercicio de encontrar la similitud o disimilitud en dos imágenes de huellas dactilares dadas. El emparejamiento de la huella dactilar puede visualizarse mejor tomando una copia de papel de una imagen de huella dactilar de archivo con sus minucias marcadas o superpuestas y una transparencia de una huella dactilar de búsqueda con sus minucias marcadas o superpuestas. Al colocar la transparencia de la impresión de búsqueda sobre la copia de papel de la huella dactilar de archivo y al trasladar y rotar la transparencia, se pueden localizar los puntos de minucias que son comunes en ambas impresiones. A partir del número de minucias comunes encontradas, su cercanía a coincidir, la calidad de las imágenes de la huella dactilar y cualquier información contradictoria de emparejamiento de minucias, es posible evaluar la similitud de los dos puntos. El emparejamiento manual de la huella dactilar es una tarea muy tediosa. Los algoritmos automáticos de emparejamiento de huellas dactilares trabajan en el resultado de los algoritmos de extracción de características de la huella dactilar y encuentran la similitud o disimilitud en dos conjuntos de minucias dadas. El emparejamiento automático de la huella dactilar puede realizar comparaciones de ésta a una velocidad de diez miles de veces cada segundo y los resultados pueden ser organizados de acuerdo al nivel de similitud y combinarse con cualquier otro criterio que pueda estar disponible para filtrar posteriormente los candidatos, todo sin la intervención humana.

Es importante destacar, sin embargo, que los algoritmos automáticos de emparejamiento de huella dactilar son significativamente menos exactos que un perito forense bien capacitado. Aun así, dependiendo de la aplicación y la calidad de imagen de la huella dactilar, los algoritmos automáticos de emparejamiento de huella dactilar pueden reducir significativamente el trabajo de los peritos forenses. Por ejemplo, en el caso del emparejamiento de las impresiones latentes donde solo una imagen de huella dactilar parcial, de muy baja calidad, está disponible para el emparejamiento, el algoritmo de emparejamiento puede no ser muy exacto. Aún, el algoritmo de emparejamiento puede generar una lista de candidatos coincidentes que sea mucho más pequeña que el tamaño de la base de datos; el perito forense entonces necesita emparejar solo manualmente un número mucho menor de huellas dactilares. En el caso del emparejamiento de impresiones latentes, donde la impresión latente es de buena calidad o en el caso del emparejamiento decadactilar a decadactilar en una aplicación de revisión de antecedentes, el emparejamiento es altamente exacto y requiere una involucración humana mínima.

Los algoritmos automáticos de emparejamiento de huella dactilar dan paso a resultados imperfectos debido al problema difícil impuesto por las variaciones dentro de las clases (variación en impresiones diferentes del mismo dedo) presentes en las huellas dactilares. Estas variaciones dentro de las clases surgen a parir de los siguientes factores que varían durante la adquisición diferente del mismo dedo: (1) desplazamiento, (2) rotación, (3) superposición parcial, (4) distorsión no lineal debido a la presión del dedo tridimensional elástico sobre una superficie de formación de imágenes de dos dimensiones rígidas, (5) presión, (6) condiciones de la piel , (7) ruido introducido por el entorno de imagen y (8) errores introducidos por los algoritmos automáticos de extracción de características.

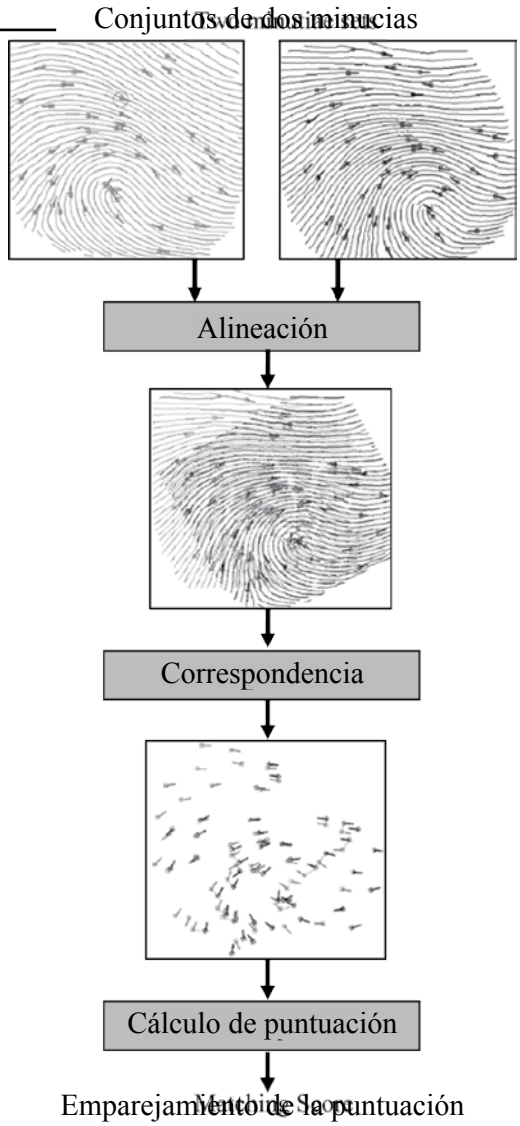
Un algoritmo sólido de emparejamiento de huella dactilar debe ser capaz de tratar con todas estas variaciones dentro de la clase en las diversas impresiones del mismo dedo. Las variaciones en el desplazamiento, rotación y superposición parcial son típicamente tratadas al utilizar un algoritmo de alineación. El algoritmo de alineación sebe ser capaz de alienar correctamente los dos conjuntos de minucias de las huellas dactilares de tal modo que las minucias correspondientes o emparejadas coincidan bien unas con las otras después de la alineación. Ciertos algoritmos de alineación también toman en cuenta la variabilidad causada por la distorsión no lineal. El algoritmo de alineación debe también ser capaz de tomar en consideración el hecho de que el algoritmo de extracción de características es imperfecto y pudo haber introducido puntos de minucias falsos y, al mismo tiempo, haber fallado al detectar algunos de los puntos de minucias genuinos. Existen muchos algoritmos de alineación de huella dactilar. Algunos pueden utilizar los puntos del núcleo y delta si es que son extraídos, para alinear las huellas dactilares. Otros utilizan algoritmos de emparejamiento de patrones tales como la transformada de Hough (una herramienta estándar en reconocimiento de patrones que permite el reconocimiento de patrones globales en el espacio característico por medio del reconocimiento de patrones locales en un espacio de parámetros transformado), relajación, soluciones de búsquedas algebraicas y operativas, "podada de árbol", minimización de energía y así sucesivamente, para alineas directamente los puntos de minucias. Otros utilizan emparejamiento de crestas adelgazadas o emparejamiento del campo de orientación para llevar a la alineación.

Una vez que se ha establecido la alineación, las minucias de las dos huellas dactilares no se sobreponen exactamente una en la otra debido a los errores residuales menores en el algoritmo de alineación y las distorsiones no lineales. La próxima etapa en el algoritmo de emparejamiento de minucias de la huella dactilar, el cual establece que las minucias en los dos conjuntos son correspondientes y aquellas que no son correspondientes, se basa en el uso de algunas tolerancias en las ubicaciones de las minucias y la orientación para declarar una correspondencia. Debido al ruido que se ha introducido a causa de la condición de la piel, el ambiente de registro, el ambiente de la imagen y la imperfección de los algoritmos automáticos de extracción de características de la huella dactilar, el número de minucias correspondientes usualmente se sabe que es menor que el número total de minucias en cualquiera de los conjuntos de minucias en el área de superposición. Así que, finalmente, un algoritmo de cálculo de puntuación se utiliza para contar una puntuación de emparejamiento. El puntaje de emparejamiento esencialmente transmite la fiabilidad del algoritmo de emparejamiento de la huella dactilar y puede ser visto como una indicación de la probabilidad de que dos huellas dactilares provengan del mismo dedo. Mientras más alto sea el puntaje de emparejamiento, más posible será que las huellas dactilares sean acopladas (y, a la inversa, mientras el puntaje sea más bajo, menos posible será que exista una coincidencia). Existen muchos algoritmos de cálculo de puntuación que son utilizados. Varían desde los simples que cuentan el número de minucias coincidentes normalizadas por el número total de minucias en ambas huellas dactilares en el área de superposición, para verificar los algoritmos muy complejos basados en la teoría de la probabilidad o los basados en patrones estadísticos de clasificación de reconocimiento que toman en cuenta un numero de características tales como el área de superposición, la calidad de las huellas dactilares, las distancias residuales entre las minucias coincidentes y así sucesivamente. La Figura 6-12 describe los pasos en un algoritmo típico de emparejamiento de huella dactilar.

Cabe destacar que las etapas y algoritmos descritos en esta sección representan solo un algoritmo típico de emparejamiento de minucias de la huella dactilar. Existen muchos algoritmos de este tipo y todos difieren unos de otros. Al igual que los varios algoritmos de extracción, los de emparejamiento utilizan diferentes implementaciones, diferentes etapas y diferentes órdenes de etapas. Por ejemplo, algunos algoritmos de emparejamiento de minucias no utilizan una etapa de alineación. Estos algoritmos en cambio intentan pre alinear las minucias de la huella dactilar para que la alineación no se requiera durante la etapa de emparejamiento. Otros algoritmos intentan evitar tanto la pre alineación como la alineación durante el

FIGURA 6–12

Etapas de un algoritmo típico de emparejamiento de minucias de la huella dactilar.



emparejamiento al definir un sistema coordinado intrínseco para las minucias de la huella dactilar. Algunos algoritmos de emparejamiento de minucias utilizan una alineación local, algunos utilizan una alineación global y algunos utilizan ambas. Finalmente, muchos de los nuevos algoritmos de emparejamiento son totalmente diferentes y están basados en características que no están basadas en minucias que fueron automáticamente extraídas del algoritmo de extracción de características de la huella dactilar, tales como los poros y las características de textura.

6.4.6 Indexación y recuperación

En la sección anterior, el problema del emparejamiento de la huella dactilar se definió al encontrar la similitud en cualquier par de huellas dactilares dado. Hay muchas situaciones, tales como el control de acceso físico dentro de una ubicación o la afirmación de la propiedad de un documento legal (tal como la licencia de manejo), donde una sola coincidencia entre dos huellas dactilares bastará. Sin embargo, en la gran mayoría de las aplicaciones forenses y gubernamentales, tales como en la individualización de huella dactilar latente y las revisiones de antecedentes, se requiere que múltiples huellas dactilares (de hecho, más de 10 huellas dactilares de los 10 dedos de la misma persona) sean emparejadas contra un gran número de huellas dactilares presentes en una base de datos. En estas aplicaciones, una gran cantidad de búsquedas de huellas dactilares y emparejamiento se

necesitará realizar para una sola individualización. Esto consume mucho tiempo, incluso para los algoritmos automáticos de emparejamiento de huella dactilar. Así que se vuelve deseable (aunque no necesario) utilizar el indexado de huella dactilar automático y algoritmos de recuperación para hacer la búsqueda más fácil.

Tradicionalmente, tal indexación y recuperación se ha llevado a cabo de manera manual por parte de peritos forenses a través de la indexación de tarjetas de papel para huellas dactilares en archiveros que están basados en la información de clasificación del patrón de la huella dactilar al definirse por un sistema de clasificación de huellas dactilares particular.

Similar al desarrollo de los primeros algoritmos automáticos de extracción de características y emparejamiento de la huella dactilar, los algoritmos automáticos iniciales de indexación de la huella dactilar fueron desarrollados para imitar a los peritos forenses. Estos algoritmos se construyeron para clasificar las imágenes de huella dactilar en típicamente cinco clases (por ejemplo, la presilla izquierda, la presilla derecha, el verticilo, el arco y el arco en forma de carpa) basadas en las muchas características que se extraen automáticamente de las imágenes de huella dactilar. (Muchos algoritmos utilizaron solo cuatro clases debido a que los tipos de arco y de arco en forma de carpa son con frecuencia difíciles de distinguir.)

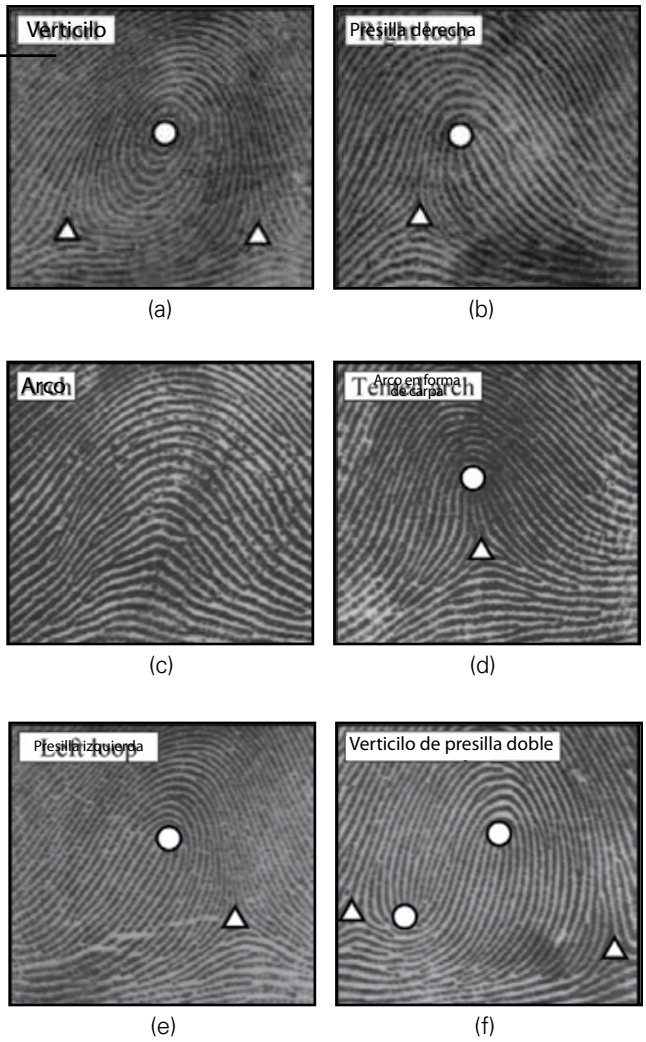
La clasificación de patrones de huellas dactilares puede determinarse mediante la caracterización explícita de las regiones de una huella dactilar tal y como sean pertenecientes a una forma particular o mediante la aplicación de uno de los muchos posibles clasificadores generalizados (por ejemplo, las redes neuronales), entrenados para reconocer los patrones específicos. Las formas singulares (por ejemplo, núcleos y deltas) de la imagen de una huella dactilar se detectan normalmente utilizando algoritmos basados en la imagen de orientación de huellas dactilares. Los sistemas explícitos de clasificación de huellas dactilares (basados en reglas) detectan primero las singularidades de las huellas dactilares (núcleos y deltas) y luego aplican un conjunto de reglas (por ejemplo, los arcos y los arcos en forma de carpa a menudo no tienen núcleos; las presillas tienen un núcleo y un delta; los verticilos tienen dos núcleos y dos deltas) para determinar el tipo de patrón de la imagen de la huella (Figura 6-13). Los sistemas de clasificación de huellas dactilares (por ejemplo, los basados en la red neural) generalizadamente más exitosos utilizan una combinación de varios clasificadores diferentes.

Tales algoritmos automáticos de clasificación de huellas dactilares se pueden utilizar para indexar todas las huellas dactilares en la base de datos en contenedores distintos (la mayoría de las implementaciones incluyen referencias de superposición o patrón) y las muestras presentadas se compararán entonces sólo con los registros de la base de datos con la misma clasificación (es decir, en el mismo recipiente). El uso de información del patrón de huella dactilar puede ser un medio eficaz para limitar el volumen de datos enviados al motor de búsqueda correspondiente, resultando en beneficios en el tiempo de respuesta del sistema. Sin embargo, los algoritmos automáticos de clasificación de huellas dactilares no son perfectos y resultan en errores en la clasificación. Estos errores de clasificación aumentan los errores en la individualización de huellas dactilares debido a que el esfuerzo de adaptación se llevará a cabo sólo en un recipiente equivocado. Dependiendo de la aplicación, puede ser factible confirmar manualmente la clase de huellas dactilares determinada automáticamente para algunas de las huellas dactilares en el que el algoritmo automático tiene poca fiabilidad. Aun así, la clasificación explícita de huellas dactilares en tan sólo unas pocas clases tiene sus limitaciones porque sólo se utilizan algunas clases (por ejemplo, cinco) y las huellas dactilares que se producen en la naturaleza no se distribuyen por igual en estas clases (por ejemplo, los arcos y arcos en forma de carpa son mucho más raros que las presillas y los verticilos).

Muchos de los nuevos algoritmos automáticos de clasificación de huellas dactilares no utilizan clases explícitas de huellas dactilares en distintas clasificaciones, sino más bien utilizan una clasificación continua de huellas que no es intuitiva para el procesamiento manual, pero es susceptible a los algoritmos de búsqueda automatizada. En la clasificación continua, las huellas dactilares están asociadas con vectores numéricos que resumen sus principales características. Estos vectores de características se crean a través de una transformación de semejanza de preservación, de manera que las huellas dactilares similares se asignan a puntos cercanos (vectores) en el espacio multidimensional. La recuperación se lleva a cabo haciendo coincidir la huella dactilar de entrada con las de la base de datos cuyos vectores correspondientes están cerca de la buscada. Las estructuras de datos espaciales se pueden utilizar para la indexación de grandes bases de datos. Un enfoque de clasificación continuo permite que el problema de la membresía exclusiva de las huellas dactilares ambiguas se evite y la eficiencia y precisión del sistema para ser equilibrada mediante el ajuste del tamaño de la vecindad considerada. La

FIGURA 6–13

Las seis clases de huella dactilar comúnmente utilizadas: (a) verticilo, (b) presilla derecha, (c) arco, (d) arco en forma de carpa, (e) presilla izquierda y (f) verticilo de presilla doble.



mayoría de las técnicas de clasificación continuas propuestas en la literatura utilizan la imagen de orientación como una función inicial, pero difieren en la transformación adoptada para crear los vectores finales y en la medida de distancia.

Algunos otros métodos de indexación continua se basan en las características de minucias de la huella dactilar utilizando técnicas tales como la función *hash* geométrica. Los algoritmos de indexación continua pueden construirse también utilizando características de la huella dactilar que no estén basadas en minucias, tales como las características de textura.

Elegir una técnica de indexación por separado por lo general no es suficiente; una estrategia de recuperación también se define usualmente de acuerdo a la aplicación de los requerimientos, tales como la exactitud y eficiencia deseada, el involucramiento de un revisor humano y así sucesivamente. En general, pueden definirse estrategias diferentes para el mismo mecanismo. Por ejemplo, la búsqueda puede detenerse cuando una porción fija de la base de datos ha sido explorada o tan pronto como se encuentre una huella dactilar coincidente. (En la individualización de la huella dactilar latente, un perito forense examina las huellas dactilares que se consideran suficientemente similares por parte del emparejador de minucias y termina la búsqueda cuando una verdadera correspondencia se encuentra.) Si una técnica de clasificación exclusiva se utiliza para la indexación, las siguientes estrategias de recuperación pueden utilizarse:

- Única clase de hipótesis—Únicamente se recuperan las huellas dactilares que correspondan a la clase de la cual la huella dactilar de entrada haya sido asignada.
- Orden de búsqueda fija—La búsqueda continúa hasta que se encuentre una coincidencia o hasta que la base de datos completa se haya explorado. Si una correspondencia no se encuentra dentro de la clase de hipótesis, la búsqueda continuará en otra clase y así sucesivamente.

- Orden de búsqueda variable—Se consultan las diferentes clases de acuerdo a las similitudes de clase producidas por el clasificador para la huella dactilar de entrada. La búsqueda puede detenerse tan pronto se encuentre una coincidencia o cuando la similitud de la relación entre la clase actual y la próxima a consultarse sea menor que el umbral establecido.

Finalmente, muchas selecciones de diseño del nivel del sistema pueden utilizarse para hacer rápida la recuperación. Por ejemplo, la búsqueda puede esparcirse a través de varias computadoras y se pueden utilizar aceleradores de hardware de propósito especial para llevar a cabo un emparejamiento de huella dactilar rápido contra una base de datos grande.

6.4.7 Caracterización de exactitud

Aunque el emparejamiento manual de huella dactilar es una tarea muy tediosa, es probable que un perito forense bien capacitado no cometa errores de individualizaciones, especialmente cuando la calidad de imagen de la huella dactilar es razonable. Los algoritmos automáticos de huella dactilar, por otro lado, no son tan exactos como los peritos forenses y tienen dificultad lidiando con las muchas fuentes de ruido en las imágenes de huella dactilar. La exactitud de los algoritmos de la huella dactilar es crucial en el diseño de sistemas de huella dactilar para el uso en la vida real. El resultado del emparejamiento debe ser confiable porque muchas decisiones de la vida real se basarán en él. Los diseñadores de algoritmos usualmente adquieren o recolectan su propia base de datos de huellas dactilares y evalúan la exactitud de sus algoritmos de huella dactilar en esta base de datos. Al evaluar nuevos algoritmos, o cambios en el viejo algoritmo, o cambios en los parámetros del algoritmo en la misma base de datos, ellos pueden saber si el nuevo algoritmo o cambios mejoran la exactitud del algoritmo. Más adelante, los desarrolladores de algoritmos observarán de manera cercana los errores falsos positivos y falsos no concordantes hechos por parte de sus algoritmos y tendrán un mejor entendimiento de las fortalezas y limitantes de sus algoritmos. Al comparar los errores hechos por diferentes algoritmos o cambios, los diseñadores de algoritmos tratarán de entender si un cambio mejora los falsos positivos, falsos no concordantes, ambos o ninguno y por qué. Los diseñadores de algoritmos pueden salir con técnicas algorítmicas para abordar los errores restantes y mejorar la exactitud de los algoritmos. Es deseable tener una base de datos de huellas dactilares tan grande como sea posible comparada con una demografía grande para que los algoritmos no se ajusten tanto a cierta variedad de huellas dactilares y la exactitud obtenida en el laboratorio se generalice bien en el campo. Las organizaciones públicas (por ejemplo, el Instituto Nacional de Estándares y Tecnología, NIST *por sus siglas en inglés*) llevan a cabo pruebas periódicas de algoritmos de huella dactilar por parte de diferentes proveedores en una base de datos común para juzgar su exactitud relativa.

Existe una compensación entre las relaciones de errores falsos positivos y falsos no concordantes dentro del emparejamiento de huella dactilar. Las diferentes aplicaciones tienen diferentes requerimientos para estos dos tipos de errores. Curiosamente, los algoritmos de huella dactilar diferentes pueden trabajar de manera diferente, dependiendo de las relaciones de errores. Por ejemplo, el algoritmo A puede ser mejor que el algoritmo B en una relación falsa positiva baja, pero el algoritmo B puede ser mejor que el algoritmo A en una relación falsa no concordante. En tales casos, los diseñadores de algoritmos pueden elegir cierto algoritmo o parámetros específicos para utilizarse, dependiendo de la aplicación.

6.5 Resumen

La tecnología de huella dactilar ha recorrido un largo camino desde sus inicios, hace más de 100 años. Los primeros lectores de huellas primitivas *livescan* introducidos en 1988 eran bestias difíciles de manejar con tantos problemas en comparación con los elegantes, baratos y relativamente minúsculos sensores disponibles en la actualidad. Durante las últimas décadas, la investigación y el uso activo de comparación de huellas dactilares e indexación también han provocado avances en nuestra comprensión de la individualidad, la información de las huellas dactilares y las formas eficientes de procesar esta información. Los poderes adquisitivos cada vez más baratos de computación, los sensores de huellas dactilares menos costosos y la demanda de seguridad, eficiencia y conveniencia han conducido a la viabilidad de los algoritmos automáticos de huellas dactilares para el uso diario en un gran número de aplicaciones.

Hay una serie de retos que quedan por superar en el diseño de un sistema de individualización de huella dactilar totalmente automática y fiable, en especial cuando las imágenes de las huellas dactilares son de mala calidad. Aunque los sistemas automáticos han mejorado significativamente, el diseño de sistemas automatizados todavía no coincide con la toma de decisiones compleja de un perito en huellas dactilares, bien capacitado para tomar decisiones para que

coincidan las huellas dactilares individuales (especialmente las huellas latentes). Sin embargo, los sistemas de emparejamiento de huellas dactilares automáticas mantienen una promesa real para el desarrollo de soluciones fiables, rápidas, consistentes y de costos efectivos en una serie de aplicaciones tradicionales y emergentes.

La investigación en el reconocimiento automático de huellas dactilares ha sido sobre todo un ejercicio de imitar el comportamiento de un perito en huellas dactilares humano sin acceso a las muchas características ricas en información subyacentes que un experto es capaz de recoger mediante un examen visual. La falta de tal conjunto de características informativas en los sistemas automáticos es principalmente debido a la ausencia de disponibilidad de técnicas de modelización y de procesamiento de imágenes complejas que pueden extraer características detalladas en presencia de ruido de manera fiable y consistente. Tal vez, utilizar el enfoque manual de reconocimiento de huella dactilar basada en la intuición humana no pueda ser la base más adecuada para el diseño de sistemas automáticos de reconocimiento de huellas dactilares. Puede haber una necesidad de explorar radicalmente diferentes características ricas en información discriminatoria, métodos robustos de comparación de huellas dactilares y métodos más ingeniosos para combinar la correspondencia de huellas dactilares y la clasificación que son susceptibles de automatización.

6.6 Revisores

Los revisores de este capítulo fueron Patti Blume, Christophe Champod, Wayne Eaton, Robert J. Garrett, Laura A. Hutchins, Peter D. Komarinski y Kasey Wertheim.

6.7 Referencias

AFIS Committee Report. International Association for Identification: Mendota Heights, MN, 1994.

AFIS Committee Report. *J. Forensic Ident.* 1998, *48* (4), 489–500.

American National Standards for Information Systems—Data Format for the Interchange of Fingerprint Information; ANSI/NIST-CSL 1-1993; National Institute of Standards and Technology, U.S. Government Printing Office: Washington, DC, 1993.

American National Standard for Information Systems—Data Format for the Interchange of Fingerprint, Facial & SMT (Scar, Mark, and Tattoo) Information; ANSI/NIST-ITL 1a-1997; National Institute of Standards and Technology, U.S. Government Printing Office: Washington, DC, 1997.

American National Standard for Information Systems—Data Format for the Interchange of Fingerprint, Facial, & & Scar Mark & Tattoo (SMT); ANSI/NIST-ITL 1-2000, NIST Special Publication #500-245; National Institute of Standards and Technology, U.S. Government Printing Office: Washington, DC, 2000.

American National Standards for Information Systems—Data Format for the Interchange of Fingerprint, Facial, & Other Biometric Information—Part 1 (Traditional Format); ANSI/NIST-ITL 1-2007, NIST Special Publication #500-271; National Institute of Standards and Technology, U.S. Government Printing Office: Washington, DC, 2007. Available online at http://www.nist.gov/customcf/get_pdf.cfm?pub_id=51174.

American National Standards for Information Systems—Data Format for the Interchange of Fingerprint, Facial, & Other Biometric Information—Part 2 (XML Version); ANSI/NIST-ITL 2-2008, NIST Special Publication #500-275; National Institute of Standards and Technology, U.S. Government Printing Office: Washington, DC, 2008. Available online at http://www.nist.gov/customcf/get_pdf.cfm?pub_id=890062.

Bruton, T. *Annual Report of the Crime Scene Investigations Unit;* San Francisco Police Department: San Francisco, CA, 1989.

Cole, S. *Suspect Identities;* Harvard University Press: Cambridge, MA, 2001.

FBI Request for Quotation No. 66-1, December 16, 1966.

Greenwood, P. W.; Chaiken, J. M.; Petersilia, J. *The Criminal Investigative Process* (Vols. 1–3); Technical Report R-1777-DOJ; RAND Corporation: Santa Monica, CA, 1975.

Grother, P.; McCabe, M.; et al. *MINEX: Performance and Interoperability of INCITS 378 Fingerprint Template;* NISTIR 7296; National Institute of Standards and Technology, March 21, 2006.

Hicklin, A.; Khanna, R. *The Role of Data Quality in Biometric Systems;* Mitretek Systems: Falls Church, VA, 2006.

Higgins, P. Standards for the Electronic Submission of Fingerprint Cards to the FBI. *J. Forensic Ident.* 1995, *45* (4), 409–418.

International Association for Identification. *AFIS Directory of Users;* IAI: Mendota Heights, MN, 1999.

Kiji, K. *AFIS 30-Year History;* NEC Internal Corporate Report; NEC Solutions: Tokyo, Japan, 2002.

Komarinski, P. *Automated Fingerprint Identification Systems;* Elsevier: New York, 2005.

Moore, R. T. Automatic Fingerprint Identification Systems. In *Advances in Fingerprint Technology,* 1st ed.; Lee, H. C.; Gaensslen, R. E., Eds.; Elsevier, NY, 1991; pp 163–191.

Moses, K. R. Consumer's Guide to Fingerprint Systems. *Ident. News* 1986, *36* (6), 5–7, 10.

National Institute for Standards and Technology. *MINEX: Performance and Interoperability of INCITS 378 Fingerprint Template (NISTIR 7296);* March 6, 2005.

Petersilia, J. *The Collection and Processing of Physical Evidence;* WN-9062-DOJ; RAND Corporation: Santa Monica, CA, 1975.

Wayman, J. *Biometric Systems.* Springer: New York, 2004.

Wegstein, J. H. *A Computer Oriented Single-Fingerprint Identification System;* Technical Note 443; National Bureau of Standards, U.S. Department of Commerce: Washington, DC, 1969a.

Wegstein, J. H. *A Semi-Automated Single Fingerprint Identification System;* Technical Note 481; National Bureau of Standards, U.S. Department of Commerce: Washington, DC, 1969b.

Wegstein, J. H. *Automated Fingerprint Identification;* Technical Note 538; National Bureau of Standards, U.S. Department of Commerce: Washington, DC, 1970.

Wegstein, J. H. *The M40 Fingerprint Matcher;* Technical Note 878; National Bureau of Standards, U.S. Department of Commerce: Washington, DC, 1972a.

Wegstein, J. H. *Manual and Automated Fingerprint Registration;* NBS Technical Note 730; National Bureau of Standards, U.S. Department of Commerce: Washington, DC, 1972b.

Wegstein, J. H. *An Automated Fingerprint Identification System;* NBS Special Publication 500-89; National Bureau of Standards, U.S. Department of Commerce: Washington, DC, 1982.

Wegstein, J. H.; Rafferty, J. F. *The LX39 Latent Fingerprint Matcher;* Special Publication 500-36; National Bureau of Standards, U.S. Department of Commerce: Washington, DC, 1978.

Wegstein, J. H.; Rafferty, J. F. The Automated Identification of Fingerprints. In *Dermatoglyphics—Fifty Years Later;* March of Dimes: Washington, DC, 1979.

Wegstein, J. H.; Rafferty, J. F.; Pencak, W. J. *Matching Fingerprints by Computer;* Technical Note 466; National Bureau of Standards, U.S. Department of Commerce: Washington, DC, 1968.

6.8 Información adicional

Asai, K.; Kato, Y.; Hoshino, Y.; Kiji, K. Automatic Fingerprint Identification; In *Proceedings of the SPIE, vol. 182—Imaging Applications for Automated Industrial Inspection and Assembly,* 1979; pág. 49–56.

Lee, H. C.; Gaensslen, R.E., Eds. *Advances in Fingerprint Technology;* 2nd ed.; CRC Press: Washington, D.C., 2001.

Millard, K. An Approach to the Automatic Retrieval of Latent Fingerprints; In *Proceedings of Carnahan Conference on Electronic Crime Countermeasures,* Lexington, KY, 1975; pág. 45–51.

Millard, K. Development on Automatic Fingerprint Recognition; In *Proceedings of the Carnahan Conference on Security Technology,* Zurich, Switzerland, 1983; pág. 173–178.

Prabhakar, S.; Jain, A.; Maltoni, D.; Maio, D. *Handbook of Fingerprint Recognition;* Springer-Verlag: New York, 2003.

Ratha, N.; Bolle, R., Eds. *Automated Fingerprint Recognition Systems;* Springer-Verlag: New York, 2004.

Roberts, D. F. Dermatoglyphics and Human Genetics. In *Dermatoglyphics—Fifty Years Later;* Birth Defects Original Article Series; Wertelecki, W., Plato, C., Paul, N. W., Eds.; Alan R. Liss Inc.: New York, 1979; pág. 475–494.

Thiebault, R. Automatic Process for Automated Fingerprint Identification; In *Proceedings of the International Symposium on Automation of Population Register Systems,* 1967; pág. 207–226.

Thiebault, R. An Automatic Procedure for Identifying Fingerprints. *International Criminal Police Rev.* 1970, *25,* 2–10.

Uchida, K. Fingerprint Identification. *NEC J. Advanced Technology* 2005, *2* (1), 19–27.

Wayman, J.; Jain, A.; Maltoni, D.; Maio, D., Eds. *Biometric Systems,* Springer-Verlag: New York, 2005.