

SISTEMAS Y MÉTODOS PARA REALIZAR AUTENTIFICACIÓN DEL USUARIO A BASE DE HUELLAS DACTILARES USANDO IMÁGENES CAPTURADAS USANDO DISPOSITIVOS MÓVILES

CAMPO DE LA INVENCION

La presente invención se refiere a sistemas y métodos para capturar y caracterizar características biométricas, en particular, sistemas y métodos para capturar y caracterizar características biométricas usando imágenes de dedos capturados por una cámara integrada de un dispositivo móvil tal como un teléfono inteligente.

ANTECEDENTES DE LA INVENCION

Como una biométrica es una característica biológica (tal como una huella dactilar, la geometría de una mano, patrón de retina, textura del iris, etc.) de un individuo, las técnicas biométricas pueden ser usadas como un factor de verificación adicional puesto que las biométricas son usualmente más difíciles de obtener que otras credenciales no biométricas. Las biométricas pueden ser usadas para identificación y/o autenticación (también referido como afirmación y/o verificación de identidad).

La afirmación de identidad biométrica puede requerir un cierto nivel de seguridad como se dicta por la aplicación. Por ejemplo, la autenticación en conjunto con una transacción financiera u obtención de acceso a una ubicación segura requiere niveles de seguridad superior. Como un resultado, preferiblemente, la exactitud de la representación biométrica de un usuario es suficiente para asegurar que el usuario es autenticado con precisión y se mantiene la seguridad.

Sin embargo, la desaparición, el intercambio, mezclado, y adopción ilegal de recién nacidos es un desafío global y usar sistemas biométricos automatizados ha sido propuesto para identificar nuevos recién nacidos con base en su rostro, iris, huella dactilar, huella, y/o impresión de la palma.

Sin embargo, en la medida en que existan sistemas de afirmación de identidad de iris, rostro, dedos, y voz, y proporcionen el nivel requisito de precisión, tales sistemas requieren dispositivos dedicados y aplicaciones y no son fácilmente implementados en teléfonos inteligentes convencionales, los cuales tiene resolución de cámara y capacidades de emisión de luz limitadas.

Los sensores electrónicos de huellas dactilares ya han sido agregados a

dispositivos de teléfonos inteligentes, el teléfono inteligente iPhone 6 por Apple Inc. de Cupertino California y el teléfono inteligente Samsung S5 por Samsung Co. de Samsung Korea son ejemplos de esto. En estos dispositivos, el usuario debe registrar sus datos de huella dactilar colocando su dedo sobre el sensor, en una fecha posterior el usuario puede verificar su identidad reposicionando su dedo sobre el sensor, los datos de la huella dactilar se comparan con los datos registrados y si coinciden se confirma la identidad del usuario. Si la huella dactilar no coincide entonces el usuario puede ser identificado como un impostor. Una desventaja de estos sistemas es que el sensor de huella dactilar agrega tamaño, peso y costo al dispositivo. Además, por estas razones es ventajoso minimizar el tamaño del sensor de huella dactilar, y como tal el sensor de huella dactilar típicamente captura solamente una porción de la huella dactilar lo cual reduce la efectividad de la identificación. A más pequeña la región de captura para el sensor de huella dactilar, más oportunidad existe de que otro dedo coincidirá por oportunidad, y más probable que cualquier error en los datos de la huella dactilar causará un rechazo falso del usuario auténtico.

Sin embargo, capturar las huellas dactilares de recién nacidos usando los sensores tradicionales de huellas dactilares es desafiante debido al tamaño del dedo y la dificultad de sostener la mano del recién nacido y colocarla sobre el sensor.

En términos prácticos esto significa que los usuarios (es decir, adultos y recién nacidos) sufren de un nivel superior de inconveniencia de rechazos falsos, y la aplicación del sensor está limitada a empleo no crítico tal como pagos de bajo valor. Los sensores de huellas dactilares pueden también ser sujeto de ataques de falsificación, donde por ejemplo, un molde de la huella dactilar de los usuarios auténtica se coloca en el sensor de huella dactilar para permitir a un impostor pasar la autenticación. Esto proporciona una razón adicional para restringir el empleo a aplicaciones no críticas.

Un desafío adicional es que solamente unos pocos dispositivos móviles están equipados con sensores de huellas dactilares los cuales limitan los números de personas quienes tienen acceso a los sistemas de autorización de huella dactilar, y causan una inconsistencia en el método de autenticación entre los dispositivo.

Los sistemas han sido propuestos que analizan la imagen de un dedo único usando la cámara de un dispositivo móvil, estos sistemas son potencialmente más convenientes, sin embargo, los índices de aceptación falsa más bajos y los índices de rechazo falso para tales sistemas para formar la imagen y analizar un dedo único son todavía no suficientemente confiables para aplicaciones que requieren seguridad

elevada tales como compras de alto valor y sistemas de empresas (es decir, sistemas a gran escala).

Como tal, existe la necesidad de un sistema de reconocimiento de dedos más confiable y más ubicuo.

BREVE DESCRIPCIÓN DE LA INVENCION

Se presentan en la presente tecnologías en apoyo de un sistema y método para realizar reconocimiento de huella dactilar.

De conformidad con un primer aspecto, se proporciona un método para realizar reconocimiento de huella dactilar. El método incluye la etapa de capturar, por un dispositivo móvil que tiene una cámara, un medio de almacenamiento, instrucciones almacenadas en el medio de almacenamiento, y un procesador configurado ejecutando las instrucciones, imágenes que representan una pluralidad de dedos de un sujeto. El método también incluye detectar, usando un algoritmo de detección de dedos, una pluralidad de dedos representados en una o más de las imágenes. El método también incluye procesar al menos una imagen usando un algoritmo de segmentación para identificar un segmento de punta de dedo respectivo para uno o más dedos representados en al menos una imagen. Además, el método incluye extraer características de uno o más dedos a partir del segmento de la punta del dedo respectivo identificado para uno o más dedos, generar un identificador biométrico con base en las características extraídas y almacenar el identificador biométrico en la memoria.

De conformidad con otro aspecto, se proporciona un método para realizar reconocimiento de huella dactilar. El método incluye la etapa de capturar, por un dispositivo móvil que tiene una cámara, un medio de almacenamiento, instrucciones almacenadas en el medio de almacenamiento, y un procesador configurado ejecutando las instrucciones, imágenes que representan una pluralidad de dedos de un sujeto. El método también incluye detectar, usando un algoritmo de detección de dedos, uno o más dedos representados en al menos una de las imágenes. El método también incluye procesar al menos una imagen usando un algoritmo de segmentación para identificar un segmento de la punta del dedo respectivo por al menos un dedo representado en este. Además, el método incluye medir una o más características de al menos un dedo a partir del segmento de la punta del dedo respectivo identificado y escalar al menos una imagen con base en la característica medida. Además, el método incluye la etapa de generar un identificador biométrico que comprende al menos una porción de la imagen a

escala que representa el segmento de la punta del dedo respectivo y almacenar el identificador biométrico en la memoria.

Estos y otros aspectos, características, y ventajas pueden ser apreciados a partir de la descripción acompañante de ciertas modalidades de la invención y las figuras de dibujos y reivindicaciones.

BREVE DESCRIPCIÓN DE LAS FIGURAS

La Figura 1 es un diagrama de alto nivel de un sistema de computadora para autenticar a un usuario de conformidad con las características biométricas del usuario de conformidad con al menos una modalidad descrita en la presente;

La Figura 2A es un diagrama de bloque de un sistema de computadora para autenticar a un usuario de conformidad con las características biométricas del usuario de conformidad con al menos una modalidad descrita en la presente;

La Figura 2B es un diagrama de bloque de módulos de software para autenticar a un usuario de conformidad con las características biométricas del usuario de conformidad con al menos una modalidad descrita en la presente;

La Figura 2C es un diagrama de bloque de un sistema de computadora para autenticar a un usuario de conformidad con las características biométricas del usuario de conformidad con al menos una modalidad descrita en la presente;

La Figura 3 es un diagrama de flujo que muestra una rutina para generar un identificador biométrico de conformidad con las características biométricas del usuario y registrar o autenticar al usuario de conformidad con al menos una modalidad descrita en la presente;

La Figura 4A es un diagrama de flujo que muestra una rutina para detectar los dedos a partir de imágenes visuales e imágenes correspondientes de conformidad con al menos una modalidad descrita en la presente;

La Figura 4B es un diagrama de flujo que muestra una rutina para filtrar regiones de la punta de los dedos detectadas dentro de las imágenes visuales de conformidad con al menos una modalidad descrita en la presente;

La Figura 4C representa imágenes capturadas y generadas de conformidad con la rutina para filtrar regiones de la punta del dedo de la Figura 4B;

La Figura 5A es un diagrama de flujo que muestra una rutina para detectar vida a partir de imágenes visuales de los dedos de conformidad con al menos una modalidad descrita en la presente;

La Figura 5B es una serie de imágenes capturadas de conformidad con la rutina para detectar vida a partir de imágenes visuales de los dedos;

La Figura 5C es una serie de imágenes capturadas de conformidad con la rutina para detectar vida a partir de imágenes visuales de los dedos;

La Figura 6A representa una imagen capturada de los dedos e imágenes de reflectividad de cresta correspondientes generadas de conformidad con al menos una modalidad descrita en la presente;

La Figura 6B representa una imagen capturada de los dedos e imágenes de reflectividad de cresta correspondientes generadas de conformidad con al menos una modalidad descrita en la presente;

La Figura 6C representa una imagen capturada de los dedos e imágenes de reflectividad de cresta correspondientes generadas de conformidad con al menos una modalidad descrita en la presente;

La Figura 6D representa una imagen capturada de los dedos e imágenes de reflectividad de cresta correspondientes generadas de conformidad con al menos una modalidad descrita en la presente;

La Figura 6E representa una imagen capturada de los dedos e imágenes de reflectividad de cresta correspondientes generadas de conformidad con al menos una modalidad descrita en la presente; y

La Figura 6F representa una imagen capturada de los dedos e imágenes de reflectividad de cresta correspondientes generadas de conformidad con al menos una modalidad descrita en la presente.

La Figura 7A representa una imagen capturada de los dedos y puntos minuciosos correspondientes que pueden ser falsamente detectados entre dedos de conformidad con al menos una modalidad descrita en la presente;

La Figura 7B representa una imagen capturada de los dedos y datos de imagen procesada a través de una fuente de información ejemplar para selección minuciosa de conformidad con al menos una modalidad descrita en la presente;

La Figura 8A representa (a) Dos imágenes de dedos recolectadas a partir del usuario en diferentes ubicaciones (cambio a lo largo del dedo); (b) mapas de borde vertical son generados para alinear dedos correspondientes; (c) mapas de borde horizontal son generados para alinear dedos correspondientes; (d) Recortar y mejorar los dedos medios a partir de las dos imágenes de conformidad con al menos una modalidad descrita en la presente;

La Figura 8B representa mapas de disparidad para un dedo real y una fotografía 2D de falsificación de conformidad con al menos una modalidad descrita en la presente;

La Figura 8C representa un mapa de disparidad y superficie ajustada para una imagen de un dedo real de conformidad con al menos una modalidad descrita en la presente;

La Figura 8D representa un mapa de disparidad y superficie ajustada para una fotografía 2D de falsificación de conformidad con al menos una modalidad descrita en la presente;

La Figura 9 representa modificaciones de series de datos usando rotación de conformidad con al menos una modalidad descrita en la presente; y

La Figura 10 representa imágenes de “centro”, “izquierda”, y “derecha” capturadas en la etapa de registro de conformidad con al menos una modalidad descrita en la presente.

DESCRIPCIÓN DETALLADA DE LA INVENCION

Por medio del ejemplo solamente y para el propósito de descripción general e introducción, se describen abajo modalidades de la presente invención las cuales se refieren a un sistema y método para capturar características biométricas del usuario y genera un identificador que distingue las características biométricas del usuario usando un dispositivo móvil tal como un teléfono inteligente. El identificador biométrico es preferiblemente generado usando imágenes capturadas de una pluralidad de dedos de un usuario con el propósito de autenticar/identificar al usuario de conformidad con las biométricas capturadas y determinar la vida del usuario. La presente descripción también describe técnicas adicionales para prevenir la autenticación errónea causada por la falsificación. En algunos ejemplos, las técnicas anti-falsificación pueden incluir capturar una o más imágenes de la biométrica de un usuario y analizar las imágenes capturadas para indicaciones de vida.

En algunas implementaciones, el sistema incluye una plataforma servidora del sistema a base de nube que comunica con PC fijas, servidores, y dispositivos tales como computadoras portátiles, tabletas y teléfonos inteligentes operados por usuarios. Como el usuario intenta acceder a un ambiente de red que es de acceso controlado, por ejemplo, un sitio de red el cual requiere un inicio de sesión seguro, el usuario es alentado a autenticarse usando el dispositivo móvil preregistrado del usuario. La autenticación puede incluir verificar la identidad del usuario y/o verificar que el usuario esté vivo (por ejemplo, determinar la vida) capturando información biométrica en la forma de al menos imágenes de los dedos del usuario, extrayendo las características únicas y codificando las características como un identificador biométrico que es indicativo de las características biométricas del usuario y/o vida usando el dispositivo

móvil. Por consiguiente, la identidad y/o vida de los usuarios puede ser verificada por el dispositivo móvil y/o el servidor del sistema o una combinación de lo anterior analizando las imágenes, el identificador biométrico generado y/o comparando las imágenes y/o identificador biométrico con un identificador biométrico generado durante el registro inicial del usuario con el sistema.

De conformidad con un aspecto de la solicitud objetivo, las modalidades descritas proporcionan un medio confiable de identificación/autenticación del usuario usando reconocimiento biométrico a base de dedos en dispositivos móviles que son ubicuos y convenientes de usar. Las modalidades descritas realizan reconocimiento a base de cuatro dedos usando cámaras que están típicamente presentes en dispositivos móviles, de manera que no se incurre volumen, costo, o peso adicional en el diseño, y el empleo puede ser ubicuo. Un objetivo adicional del sistema es proporcionar una defensa contra los ataques de falsificación.

La presente invención captura información biométrica a partir de dedos múltiples simultáneamente, y captura grandes áreas de huellas a partir de cada dedo. Además, la presente invención también puede ser usada para capturar información impresa a partir de otras regiones de la mano, que incluyen impresiones de la palma e impresiones de la mano para incrementar además la confiabilidad del sistema. También en el caso de identificación de recién nacidos, la presente invención puede ser usada para capturar los dedos de los pies. Sin embargo, la innovación propuesta puede ser combinada con los sistemas de reconocimiento de rostro móviles existentes. Por medio de ejemplo no limitante, los sistemas y métodos ejemplares para autenticación del usuario a base de biométricas a partir de imágenes de características faciales se describen en la presente y en la Solicitud de Patente Estadounidense copendiente y comúnmente asignada Serie No. 14/668,352, titulada "SISTEMA Y MÉTODO PARA AUTENTIFICAR EL ACCESO PARA ACCESO A AMBIENTES CONTROLADOS", presentada el 13 de Mayo de 2015 y Patente Estadounidense No. 9,208,492, titulada "SISTEMAS Y MÉTODOS PARA AUTENTIFICACIÓN BIOMÉTRICA DE TRANSACCIONES" presentada el 7 de Marzo de 2014. Además, la presente invención puede ser usada para procesar la fotografía del dedo adquirida usando la cámara presentada en los dispositivos móviles con el fin de generar imágenes de huellas dactilares que corresponde a fotografías de dedos adquiridas y que pueden ser coincidadas con las imágenes de la huella dactilar enrolladas y planas que son usadas en los Sistemas de Identificación de Huellas Dactilares Automatizados Integrados (IAFIS, por sus siglas en inglés). Los IAFIS son

un sistema nacional de historial criminal y de identificación de huellas dactilares automatizadas mantenido por la Oficina Federal de Investigación (FBI). Los IAFIS proporcionan capacidades de búsqueda automatizada de huella dactilar, e intercambio electrónico de huellas dactilares y respuestas.

Las modalidades descritas pueden ser referidas como un sistema de autenticación biométrica multimodal. Por lo tanto, la presencia de piezas independientes, múltiples de biométricas (es decir, 4-10 dedos) ofrece las siguientes ventajas sobre los sistemas de reconocimiento móviles de dedo único ya sea usando imágenes de los dedos o huellas dactilares capturadas por sensores integrados en teléfonos inteligentes.

Modalidades descritas pueden ser referidas como

1. Desempeño: Una combinación de modalidades no correlacionadas (por ejemplo, cuatro dedos de una persona y diez dedos de un recién nacido) puede resultar en un mejor mejoramiento en el desempeño de un sistema de reconocimiento de dedo único. Este mejoramiento de precisión ocurre debido a dos razones. Primero, la fusión de evidencias biométricas a partir de diferentes dedos incrementa efectivamente las características discriminatorias y reduce el traslape entre las características de diferentes usuarios. En otras palabras, una combinación de dedos múltiples es más discriminativa para un individuo que a un dedo único. Segundo, el ruido (causado por factores como suciedad o tinta manchada) e imprecisión durante la adquisición de una subserie de dedos puede ser atendida por la información proporcionada por los dedos restantes.
2. Universalidad: Resolver el problema sin universalidad y reducir la falla para registrar errores. Por ejemplo, si una persona no puede registrar un dedo particular debido a un dedo amputado, un dedo cortado, lesión, o crestas desgastadas (es decir, las crestas desgastadas pueden ocurrir físicamente en uno o más dedos de los sujetos), todavía puede ser identificada usando sus otros dedos.
3. Ataque de falsificación: Usando las modalidades descritas, en las cuales se realiza registro de dedos múltiples de un usuario, mejorará la resistencia de sistemas de autenticación a los ataques de falsificación. Esto es debido a que llega a ser cada vez más difícil evitar o falsificar múltiples dedos simultáneamente.

Un sistema ejemplar para autenticar a un usuario y/o determinar la vida del usuario de conformidad con las imágenes de las características biométricas del usuario 100 se muestra como un diagrama de bloque en la Figura 1. En un arreglo, el sistema consiste de un servidor del sistema 105 y dispositivos del usuario que incluyen

un dispositivo móvil 101a y un dispositivo de computación del usuario 101b. El sistema 100 también puede incluir uno o más dispositivos de computación remotos 102.

El servidor del sistema 105 puede ser prácticamente cualquier dispositivo de computación y/o aparato de procesamiento de datos capaz de comunicarse con los dispositivos del usuario y dispositivos de computación remota y recibir, transmitir y almacenar información electrónica y petición de procesamiento como se describe además en la presente. De manera similar, el dispositivo de computación remota 102 puede ser prácticamente cualquier dispositivo de computación y/o aparato de procesamiento de datos capaz de comunicar con el servidor del sistema y/o los dispositivos del usuario y recibir, transmitir y almacenar información electrónica y petición de procesamiento como se describe además en la presente. Se debe entender también que el servidor del sistema y/o dispositivo de computación remota puede ser un número de dispositivos de computación a base de nube o de red.

En algunas implementaciones, el dispositivo de computación 102 puede ser asociado con una organización empresarial, por ejemplo, un banco o un sitio de red, que mantiene las cuentas del usuario ("cuentas empresariales") y proporciona servicios a titulares de cuentas empresariales y requiere autenticación del usuario previo a proporcionar el acceso al usuario a tales sistemas y servicios.

Los dispositivos del usuario, dispositivo móvil 101a y dispositivo de computación del usuario 101b, pueden ser configurados para comunicar entre sí, el servidor del sistema 105 y/o dispositivo de computación remota 102, que transmite información electrónica a este y que recibe información electrónica a partir de este como se describe además en la presente. Los dispositivos del usuario también pueden ser configurados para recibir entradas del usuario así como también capturar y procesar información biométrica, por ejemplo, imágenes digitales y grabaciones de voz de un usuario 124.

El dispositivo móvil 101a puede ser cualquiera de los dispositivos de computación móviles y/o aparato de procesamiento de datos capaz de incluir los sistemas y/o métodos descritos en la presente, que incluyen pero no se limitan a una computadora personal, computadora de tableta, asistente digital personal, dispositivo electrónico móvil, teléfono celular o dispositivo de teléfono inteligente y similares. El dispositivo de computación 101b está propuesto para representar varias formas de los dispositivos de computación que un usuario puede interactuar con, tal como estaciones de trabajo, una computadora personal, una computadora portátil, sistemas de punto de venta dedicados, terminales ATM, dispositivos de control de acceso u

otras computadoras digitales apropiadas.

Como se describe además en la presente, el sistema 100, facilita la autenticación de un usuario 124 de conformidad con las características biométricas del usuario usando un dispositivo móvil 101a. En algunas implementaciones, la identificación y/o autenticación de conformidad con las características biométricas del usuario utiliza una información biométrica del usuario en un proceso de dos etapas. La primera etapa es referida como un registro. En las muestras de etapa de registro (por ejemplo, imágenes) de biométrica(s) apropiadas es/son recolectadas a partir de un individuo. Estas muestras de biométricas son analizadas y procesadas para extraer rasgos (o características) presentes en cada muestra. La serie de características presentes en la biométrica de imagen de un individuo constituye un identificador para el personal y son utilizables para autenticar al usuario y en algunas implementaciones, determinar si el usuario es un sujeto vivo. Estos identificadores son entonces almacenados para completar la etapa de registro. En la segunda etapa se mide la misma biométrica del individuo. Las características a partir de esta biométrica son extraídas solo como en la fase de registro para obtener un identificador biométrico actual. Si la meta es determinar vida, las características pueden ser analizadas para determinar si son representativas de un sujeto vivo. Como se describe además en la presente, otros rasgos y características de las imágenes capturadas de las biométricas pueden ser analizados para determinar la vida. Si la meta es identificación, entonces este identificador es buscado en la base de datos de identificadores generados en la primera fase. Si una coincidencia ocurre, la identificación del individuo se revela, de otro modo falla la identificación. Si la meta es autenticación, entonces el identificador generado en la segunda etapa se compara con el identificador generado en la primera etapa para la persona particular. Si una coincidencia ocurre, la autenticación es exitosa, de otro modo la autenticación falla.

Se debe notar que mientras la Figura 1 representa el sistema para autenticar a un usuario 100 con respecto a un dispositivo móvil 101a y un dispositivo de computación del usuario 101b y un dispositivo de computación remota 102, se debe entender que cualquier número de tales dispositivos puede interactuar con el sistema en la manera descrita en la presente. Se debe notar también que mientras la Figura 1 representa un sistema para autenticar a un usuario 100 con respecto al usuario 124, se debe entender que cualquier número de usuarios puede interactuar con el sistema en la manera descrita en la presente.

Se debe entender además que mientras los varios dispositivos de computación

y máquinas referenciadas en la presente, que incluyen pero no se limitan a dispositivo móvil 101a y servidor del sistema 105 y dispositivo de computación remota 102 son referidos en la presente como dispositivos y/o máquinas únicos/individuales, en ciertas implementaciones los dispositivos y máquinas referenciados, y sus operaciones asociadas y/o acompañantes, características, y/o funcionalidades pueden ser combinados o arreglados o de otro modo empleados a través de un número de tales dispositivos y/o máquinas, tales como sobre una conexión de red o conexión alámbrica, como se conoce por aquellos expertos en la técnica.

Se debe entender también que los sistemas y métodos ejemplares descritos en la presente en el contexto del dispositivo móvil 101a (también referido como un teléfono inteligente) no son específicamente limitados al dispositivo móvil y pueden ser implementados usando otros dispositivos de computación habilitados (por ejemplo, el dispositivo de computación del usuario 102b).

Con referencia a la Figura 2A, el dispositivo móvil 101a del sistema 100, incluye varios componentes de hardware y software que sirven para permitir la operación del sistema, que incluye uno o más procesadores 110, una memoria 120, un micrófono 125, una pantalla 140, una cámara 145, una salida de audio 155, un almacenamiento 190 y una interfaz de comunicación 150. El procesador 110 sirve para ejecutar una aplicación del cliente en la forma de instrucciones de software que pueden ser cargadas en la memoria 120. El procesador 110 puede ser un número de procesadores, una unidad de procesamiento central CPU, una unidad de procesamiento de gráficos GPU, un núcleo multi-procesador, o cualquier otro tipo de procesador, dependiendo de la implementación particular.

Preferiblemente, la memoria 120 y/o el almacenamiento 190 son accesibles por el procesador 110, de este modo permitiendo al procesador recibir y ejecutar instrucciones codificadas en la memoria y/o en el almacenamiento para así causar que el dispositivo móvil y sus varios componentes de hardware lleven a cabo operaciones para aspectos de los sistemas y métodos como se describirá en mayor detalle abajo. La memoria puede ser, por ejemplo, una memoria de acceso aleatorio (RAM) o cualquier otro medio de almacenamiento legible por computadora volátil o no volátil. Además, la memoria puede ser fija o removible. El almacenamiento 190 puede tomar varias formas, dependiendo de la implementación particular. Por ejemplo, el almacenamiento puede contener uno o más componentes o dispositivos tales como un disco duro, una memoria instantánea, un disco óptico regrabable, una cinta magnética regrabable, o alguna combinación de los anteriores. El almacenamiento también

puede ser fijo o removible.

Uno o más módulos de software 130 son codificados en el almacenamiento 190 y/o en la memoria 120. Los módulos de software 130 pueden comprender uno o más programas de software o aplicaciones que tienen códigos de programa de computadora o una serie de instrucciones (también referidos como la “aplicación del cliente por autenticación móvil”) ejecutadas en el procesador 110. Como se representa en la Figura 2B, preferiblemente, incluido entre los módulos de software 130 está un módulo de interfaz de usuario 170, un módulo de captura biométrica 172, un módulo de análisis 174, un módulo de registro 176, un módulo de base de datos 178, un módulo de autenticación 180 y un módulo de comunicación 182 que son ejecutados por el procesador 110. Tal código o instrucciones de programa de computadora configuran el procesador 110 para llevar a cabo operaciones de los sistemas y métodos descritos en la presente y pueden ser escritos en cualquier combinación de uno o más lenguajes de programación.

El código del programa puede ejecutarse completamente en el dispositivo móvil 101, como un paquete de software independiente, parcialmente en un dispositivo móvil, parcialmente en el servidor del sistema 105, o completamente en el servidor del sistema u otro dispositivo/computadora remota. En el último escenario, la computadora remota puede ser conectada a un dispositivo móvil 101 a través de cualquier tipo de red, que incluye una red de área local (LAN) o una amplia red de área (WAN), red de comunicaciones móviles, red celular, o la conexión puede hacerse en una computadora externa (por ejemplo, a través de la Internet usando un Proveedor de Servicios de Internet).

También se dice que el código del programa de módulos de software 130 y uno o más dispositivos de almacenamiento legibles por computadora (tales como memoria 120 y/o almacenamiento 190) forman un producto de programa que puede ser manufacturado y/o distribuido de conformidad con la presente invención, como se conoce por aquellos de habilidad ordinaria en la técnica.

Se debe entender que en algunas modalidades ilustrativas, uno o más de los módulos de software 130 pueden ser descargados sobre una red para almacenamiento 190 a partir de otro dispositivo o sistema mediante interfaz de comunicación 150 para uso dentro del sistema 100. Además, se debe notar que otra información y/o datos relevantes a la operación de los presentes sistemas y métodos (tales como base de datos 185) también pueden ser almacenados en el almacenamiento. Preferiblemente, tal información es almacenada en un almacén de

datos encriptados que está específicamente alojado para así almacenar de manera segura información recolectada o generada por el procesador que ejecuta la aplicación de autenticación segura. Preferiblemente, se usan medidas de encriptación para almacenar la información localmente en el dispositivo móvil almacenamiento y transmitir información al servidor del sistema 105. Por ejemplo, tales datos pueden ser encriptados usando un cifrado polimórfico de 1024 bits, o, dependiendo de los controles exportados, un método de encriptación AES de 256 bits. Además, la encriptación puede ser realizada usando clave remota (valores originales) o claves locales (valores originales). Los métodos de encriptación alternativos pueden ser usados como podría entenderse por aquellos expertos en la técnica, por ejemplo, SHA256.

Además, los datos almacenados en el dispositivo móvil 101a y/o servidor del sistema 105 pueden ser encriptados usando una información biométrica del usuario, información vital, o información del dispositivo móvil como una clave de encriptación. En algunas implementaciones, una combinación de lo anterior puede ser usada para crear una clave única compleja para el usuario que puede ser encriptada en el dispositivo móvil usando Criptografía de Curva Elíptica, preferiblemente al menos de 384 bits de longitud. Además, tal clave puede ser usada para asegurar los datos del usuario almacenados en el dispositivo móvil y/o el servidor del sistema.

También preferiblemente almacenada en el almacenamiento 190 está la base de datos 185. Como se describirá en mayor detalle abajo, la base de datos contiene y/o mantiene varios puntos y elementos de datos que son utilizados a través de las varias operaciones del sistema y método para autenticar a un usuario 100. La información almacenada en la base de datos puede incluir pero no se limita a plantillas biométricas del usuario e información de perfil, como se describirá en mayor detalle en la presente. Se debe notar que aunque la base de datos se representa por ser configurada localmente al dispositivo móvil 101a, en ciertas implementaciones las bases de datos y/o varios de los elementos de datos almacenados en estas pueden, además o alternativamente, ser localizados remotamente (tal como en un dispositivo remoto 102 o servidor del sistema 105 - no mostrado) y conectados al dispositivo móvil a través de una red en una manera conocida por aquellos de habilidad ordinaria en la técnica.

Una interfaz de usuario 115 es también operativamente conectada al procesador. La interfaz puede ser uno o más dispositivo(s) de entrada o salida tales como conmutador(es), botón(es), tecla(s), una pantalla de toque, micrófono, etc., como

se podría entender en la técnica de dispositivos de computación electrónicos. La interfaz de usuario puede servir para facilitar la captura de comandos a partir del usuario tal como comandos activados-desactivados o información del usuario y ajustes relacionados con la operación del sistema para autenticar a un usuario 100. Por ejemplo, la interfaz sirve para facilitar la captura de cierta información a partir del dispositivo móvil 101 tal como información personal del usuario para registrarla con el sistema para así crear un perfil de usuario.

El dispositivo de computación 101a también puede incluir una pantalla 140 la cual está también operativamente conectada con el procesador al procesador 110. La pantalla incluye una pantalla o cualquier otro dispositivo de presentación el cual permite al sistema instrucciones o de otro modo proporciona retroalimentación al usuario con respecto a la operación del sistema para autenticar a un usuario 100. Por medio del ejemplo, la pantalla puede ser una pantalla digital tal como una pantalla de matriz de puntos u otra pantalla de 2 dimensiones.

Por medio del ejemplo adicional, la interfaz y la pantalla pueden ser integradas en una pantalla sensible al tacto. Por consiguiente, la pantalla también se usa para mostrar una interfaz de usuario gráfica, la cual puede presentar varios datos y proporcionar “formas” que incluyen campos que permiten la entrada de información por el usuario. Tocar la pantalla sensible al tacto en ubicaciones correspondientes a la pantalla de una interfaz de usuario gráfica permite a la persona interactuar con el dispositivo para ingresar datos, cambiar ajustes, controlar funciones, etc. Así, cuando la pantalla sensible al tacto se toca, la interfaz de usuario comunica este cambio al procesador, y los ajustes pueden ser cambiados o la información ingresada del usuario puede ser capturada y almacenada en la memoria.

El dispositivo móvil 101a también incluye una cámara 145 capaz de capturar imágenes digitales. La cámara puede ser uno o más dispositivos de imagen configurados para capturar imágenes de al menos una porción del cuerpo del usuario que incluye los ojos y/o cara del usuario mientras utiliza el dispositivo móvil 101a. La cámara sirve para facilitar la captura de imágenes del usuario con el propósito de análisis de imagen por el procesador del dispositivo móvil 110 ejecutando la aplicación segura de autenticación de cliente la cual incluye identificar características biométricas para autenticar (biométricamente) al usuario a partir de las imágenes y determinar la vida del usuario. El dispositivo móvil 101a y/o la cámara 145 también puede incluir uno o más emisores de señal o luz (por ejemplo, LEDs, no mostrados), por ejemplo, un emisor de luz visible y/o emisor de luz infrarroja y similares. La cámara

puede ser integrada en el dispositivo móvil, tal como una cámara de cara frontal o cámara de cara trasera que incorpora un sensor, por ejemplo y sin limitación un sensor CCD o CMOS. Como podría entenderse por aquellos en la técnica, la cámara 145 también puede incluir hardware adicional tal como lentes, medidores de luz (por ejemplo, medidores lux) y otras características de hardware y software convencionales que son utilizables para ajustar la configuración de captura de imagen tal como acercamiento, enfoque, apertura, exposición, velocidad de obturación y similares. Alternativamente, la cámara puede ser externa al dispositivo móvil 101a. Las posibles variaciones de la cámara y emisores de luz podrían ser entendidas por aquellos expertos en la técnica. Además, el dispositivo móvil también puede incluir uno o más micrófonos 104 para capturar registros de audio como podría entenderse por aquellos expertos en la técnica.

La salida de audio 155 es también operativamente conectada al procesador 110. La salida de audio puede ser cualquier sistema de bocinas que es configurado para reproducir archivos electrónicos de audio como podría entenderse por aquellos expertos en la técnica. La salida de audio puede ser integrada en el dispositivo móvil 101 o externa al dispositivo móvil 101.

Varios sensores/dispositivos de hardware 160 también son operativamente conectados al procesador. Los sensores 160 pueden incluir: un reloj a bordo para realizar un seguimiento de la hora del día, etc.; un dispositivo habilitado de GPS para determinar una ubicación del dispositivo móvil; un acelerómetro para seguimiento de la orientación y aceleración del dispositivo móvil; magnetómetro de gravedad para detectar el campo magnético de la Tierra para determinar la orientación 3-dimensional del dispositivo móvil; sensores de proximidad para detectar una distancia entre el dispositivo móvil y otros objetos; sensores de radiación RF para detectar los niveles de radiación RF; y otros de tales dispositivos como podría entenderse por aquellos expertos en la técnica.

La interfaz de comunicación 150 también está operativamente conectada con el procesador 110 y puede ser cualquier interfaz que permite la comunicación entre el dispositivo móvil 101a y dispositivos externos, máquinas y/o elementos que incluyen servidor del sistema 105. Preferiblemente, la interfaz de comunicación incluye, pero no se limita a, un módem, una Tarjeta de Interfaz de Red (NIC), una interfaz de red integrada, un transmisor/receptor de frecuencia de radio (por ejemplo, Bluetooth, celular, NFC), un transmisor/receptor de comunicación satelital, un puerto infrarrojo, una conexión USB, y/o cualquiera de otras tales interfaz para conectar el dispositivo

móvil con otros dispositivos de computación y/o redes de comunicación tales como redes privadas y la Internet. Tales conexiones pueden incluir una conexión alámbrica o una conexión inalámbrica (por ejemplo, usando el estándar 802.11) aunque se debe entender que la interfaz de comunicación puede ser prácticamente cualquier interfaz que permite la comunicación a/del dispositivo móvil.

En varios puntos durante la operación del sistema para autenticar a un usuario 100, el dispositivo móvil 101a puede comunicar con uno o más dispositivos de computación, tal como el servidor del sistema 105, dispositivo de computación del usuario 101b y/o dispositivo de computación remota 102. Tales dispositivos de computación transmiten y/o reciben datos para/del dispositivo móvil 101a, de este modo preferiblemente iniciando el mantenimiento, y/o mejoramiento de la operación del sistema 100, como se describirá en mayor detalle abajo.

La Figura 2C es un diagrama de bloque que ilustra una configuración ejemplar del servidor del sistema 105. El servidor del sistema 105 puede incluir un procesador 210 el cual está conectado operativamente a varios componentes del hardware y software que sirven para permitir la operación del sistema para autenticación de un usuario 100. El procesador 210 sirve para ejecutar instrucciones para realizar varias operaciones que se refieren a procesos de transacción y autenticación del usuario como se describirá en mayor detalle abajo. El procesador 210 puede ser un número de procesadores, un núcleo de multi-procesador, o algún otro tipo de procesador, dependiendo de la implementación particular.

En ciertas implementaciones, una memoria 220 y/o un medio de almacenamiento 290 son accesibles por el procesador 210, de este modo permitiendo al procesador 210 recibir y ejecutar instrucciones almacenadas en la memoria 220 y/o en el almacenamiento 290. La memoria 220 puede ser, por ejemplo, una memoria de acceso aleatorio (RAM) o cualquier otro medio de almacenamiento legible por computadora volátil o no volátil adecuado. Además, la memoria 220 puede ser fija o removible. El almacenamiento 290 puede tomar varias formas, dependiendo de la implementación particular. Por ejemplo, el almacenamiento 290 puede contener uno o más componentes o dispositivos tales como una unidad de disco duro, una memoria instantánea, un disco óptico regrabable, una cinta magnética regrabable, o alguna combinación de los anteriores. El almacenamiento 290 también puede ser fijo o removible.

Uno o más de los módulos de software 130 son codificados en el almacenamiento 290 y/o en la memoria 220. Uno o más de los módulos de software

130 pueden comprender uno o más programas o aplicaciones de software (colectivamente referido como la “aplicación segura del servidor de autenticación”) que tienen códigos de programa de computadora o una serie de instrucciones ejecutadas en el procesador 210. Tal código de programa de computadora o instrucciones para llevar a cabo operaciones de aspectos de los sistemas y métodos descritos en la presente pueden ser escritos en cualquier combinación de uno o más lenguajes de programación, como podría entenderse por aquellos expertos en la técnica. El código del programa puede ejecutarse completamente en el servidor del sistema 105 como un paquete de software independiente, parcialmente en el servidor del sistema 105 y parcialmente en un dispositivo de computación remota, tal como un dispositivo de computación remota 102, dispositivo móvil 101a y/o dispositivo de computación del usuario 101b, o completamente en tales dispositivos de computación remota. Como se representa en la Figura 2B, preferiblemente, incluidos entre los módulos de software 130 está un módulo de análisis 274, un módulo de registro 276, un módulo de autenticación 280, un módulo de base de datos 278, y un módulo de comunicación 282, que son ejecutados por el servidor del procesador del sistema 210.

También preferiblemente almacenado en el almacenamiento 290 está una base de datos 280. Como se describirá en mayor detalle abajo, la base de datos 280 contiene y/o mantiene varios puntos de datos y elementos que son utilizados a través de las varias operaciones del sistema 100, que incluyen pero no se limitan a, perfiles de usuario como se describirá en mayor detalle en la presente. Se debe notar que aunque la base de datos 280 se representa por ser configurada localmente con el dispositivo de computación 205, en ciertas implementaciones la base de datos 280 y/o varios de los elementos de datos almacenados en esta pueden ser almacenados en una memoria legible por computadora o medio de almacenamiento que está localizado remotamente y conectado con el servidor del sistema 105 a través de una red (no mostrada), en una manera conocida por aquellos de habilidad ordinaria en la técnica.

Una interfaz de comunicación 255 está también conectada operativamente con el procesador 210. La interfaz de comunicación 255 puede ser cualquier interfaz que permite la comunicación entre el servidor del sistema 105 y dispositivos externos, máquinas y/o elementos. En ciertas implementaciones, la interfaz de comunicación 255 incluye, pero no se limita a, un módem, una Tarjeta de Interfaz de Red (NIC), una interfaz de red integrada, un receptor/transmisor de radio frecuencia (por ejemplo, Bluetooth, celular, NFC), un transmisor/receptor de comunicación satelital, un puerto infrarrojo, una conexión USB, y/o cualquier otra de tales interfaces para conectar el

dispositivo de computación 205 a otros dispositivos de computación y/o redes de comunicación, tales como redes privadas y la Internet. Tales conexiones pueden incluir una conexión alámbrica o una conexión inalámbrica (por ejemplo, usando el estándar 802.11) aunque se debe entender que la interfaz de comunicación 255 puede ser prácticamente cualquier interfaz que permite la comunicación a/del procesador 210.

La operación del sistema para autenticar a un usuario 100 y los varios elementos y componentes descritos anteriormente serán además apreciados con referencia al método para facilitar la captura de la información y autenticación biométrica como se describe posteriormente. Los procesos aquí representados son mostrados a partir de la perspectiva del dispositivo móvil 101a y/o el servidor del sistema 105, sin embargo, se debe entender que los procesos pueden ser realizados, en todo o en parte, por el dispositivo móvil 101a, el servidor del sistema 105 y/o otros dispositivos de computación (por ejemplo, dispositivo de computación remota 102 y/o dispositivo de computación del usuario 101b) o cualquier combinación de los anteriores. Se debe apreciar que más o menos operaciones pueden ser realizadas que se muestran en las figuras y se describen en la presente. Estas operaciones también pueden ser realizadas en un orden diferente que aquellas descritas en la presente. Se debe entender también que una o más de las etapas pueden ser realizadas por el dispositivo móvil 101a y/o en otros dispositivos de computación (por ejemplo, el dispositivo de computación 101b, servidor del sistema 105 y dispositivo de computación remota 102).

Cambiando ahora a la Figura 3, un diagrama de flujo ilustra una rutina 300 para detectar las características biométricas del usuario a partir de una o más imágenes de conformidad con al menos una modalidad descrita en la presente. En general, la rutina incluye capturar y analizar una o más imágenes de al menos dedos múltiples de un usuario. Preferiblemente, cuatro dedos son capturados, sin embargo menos o más dedos pueden ser capturados y analizados como se describe en la presente. Como se indica anteriormente, el proceso de captura puede ser realizado durante el registro de un usuario, así como también durante las sesiones de autenticación subsecuentes, las cuales también se describen con relación a la Figura 3.

Se debe entender que, de conformidad con las modalidades descritas, las imágenes pueden ser capturadas y el identificador biométrico que es indicativo de las características biométricas únicas del usuario y/o vida pueden ser generadas usando dispositivos móviles (por ejemplo, dispositivo móvil 101a) que son ampliamente

disponibles y que tienen cámaras digitales 145 capaces de capturar imágenes de los dedos del usuario en al menos las bandas espectrales visibles.

El proceso comienza en la etapa 305, donde el procesador del dispositivo móvil 110 configurado ejecutando uno o más módulos de software 130, que incluye, preferiblemente, el módulo de captura 172, causa que la cámara 145 capture una o más imágenes de al menos una porción del usuario (124) capturando todos los cuatro (4) dedos de una mano. Preferiblemente la cámara captura imágenes de alta resolución, por ejemplo usando una cámara de cara trasera de un dispositivo de teléfono inteligente convencional. Si está disponible, las imágenes pueden ser capturadas con iluminación de destello para detalle incrementado.

En algunas implementaciones, durante el proceso de captura, el usuario es alentado a posicionar sus dedos enfrente de la cámara. Durante este procedimiento, al usuario se le puede dar retroalimentación visual a partir de la cámara en la pantalla del dispositivo de manera que los usuarios pueden posicionar sus dedos apropiadamente. En algunas implementaciones, las marcas presentadas en la pantalla pueden ser usadas para guiar a los usuarios para colocar sus dedos en una ubicación específica en el campo de visión de la cámara, y en una distancia separada particular. Por ejemplo, se le podría pedir a los usuarios alinear sus dedos con un contorno de cuatro (4) dedos superpuestos en la pantalla de previsualización de imagen de la cámara, por consiguiente, los usuarios podrían saber que sus dedos están en una distancia apropiada de la cámara cuando llenan el contorno de los dedos en la previsualización de la cámara. En algunas implementaciones, los usuarios podrían sujetar sus dedos índice, medio, anular y meñique en conjunto en lugar de tenerlos espaciados aparte. Entonces, en algunas implementaciones, se les podría pedir a los usuarios capturar el pulgar de cada una de las manos separadamente. En algunas implementaciones, el usuario sería un recién nacido quién será ayudado por un adulto para capturar las imágenes de los dedos. El enfoque de la cámara puede ser ajustado por el procesador configurado para enfocarse en los dedos, lo cual podría ser asumido por ser la ubicación de la posición guía del dedo sobre la pantalla. En algunas implementaciones, un clasificador será entrenado para detectar los dedos en las imágenes y este clasificador puede activar la cámara para capturar la imagen una vez que los dedos son detectados y enfocados. El clasificador que puede ser usado para detectar dedos en imágenes, en alguna implementación, puede ser clasificador en cascada Haar que ha sido entrenado usando características Haar regulares o filtros predefinidos y prediseñados que son adecuados para detectar dedos en imágenes de

la mano (así como también imágenes del pie, por ejemplo, en el caso de sistemas de identificación de recién nacidos). En algunas implementaciones, los procedimientos de mejoramiento de imagen pueden ser aplicados a la imagen antes de usar un clasificador para detectar dedos en las imágenes capturadas. En alguna implementación, los procesamientos de mejoramiento de imagen que pueden ser aplicados antes de aplicar el clasificador de dedos, pueden ser diseñados para ser filtros de paso de banda que pasan frecuencias de crestas de huellas de los dedos pero minimizan la salida de las frecuencias antecedentes de foco.

Entonces, la imagen capturada puede ser examinada, y la calidad de la muestra biométrica capturada será determinada analizando las crestas de los dedos. Esta medida de calidad puede ser una medida fusionada de las siguientes propiedades de crestas: frecuencia, orientación, nitidez, y conectividad. Si la medida de calidad está por debajo de un umbral predeterminado, el usuario podría ser aconsejado y guiado para repetir el proceso de captura nuevamente.

Después de la captura de los dedos, entonces en la etapa 310, las regiones de cada dedo serán identificadas. Entonces, en la etapa 315, las regiones son mejoradas y entonces, en la etapa 320, el espacio de la característica discriminativa de cada dedo puede ser extraído independientemente y almacenado separadamente. Más específicamente, en la etapa 310, el procesador configurado 110 puede ejecutar un algoritmo automático de detección de dedos para detectar los dedos en las imágenes. Por ejemplo un algoritmo de detección de dedos ejemplar puede incluir la aplicación de algoritmos de segmentación para distinguir los dedos del antecedente. Esto podría ser realizado, por ejemplo, dividiendo la imagen en las regiones homogéneas y después examinando cada región y clasificándola como región de dedo o no dedo. Sin embargo, esto podría ser realizado, por ejemplo, usando un clasificador para detectar y clasificar el dedo y las puntas del dedo. En alguna implementación, los clasificadores que pueden ser usados para detectar diferentes dedos, clasificarlos, y detectar las puntas del dedo, pueden ser clasificadores en Cascada Haar entrenados, clasificadores en Cascada HOG, clasificadores en Cascada LBP, o combinación de estos clasificadores. El entrenamiento de los clasificadores podría ser realizado como imágenes de ejemplo conocidas como se conoce en la técnica. Se observa que un clasificador entrenado para encontrar la mano podría primero ser usado para estrechar la región de búsqueda para los otros clasificadores que encuentran el dedo para mejorar la velocidad y precisión. Se observa también que tales clasificadores podrían ser usados en conjunto con otras técnicas de hallazgo de ubicación de la punta del

dedo para proporcionar la precisión mejorada. En algunas implementaciones, las regiones que son identificadas usando el(los) clasificador(es) pueden ser resaltadas por un margen y visualizados al usuario en la pantalla del dispositivo móvil. Por ejemplo, una región identificada como un segmento de la punta del dedo puede ser unido por un margen en la imagen que resalta la región identificada. El margen puede ser de varias configuraciones que incluyen márgenes rectangulares o elípticos y diferentes segmentos pueden ser resaltados que incluyen, puntas de los dedos, la mano, un grupo de dedos, otras regiones del dedo y similares. Los datos de registro de usuarios podrían ser usados para ayudar a entrenar el clasificador una vez que las posiciones de la punta del dedo han sido confirmadas por el usuario. Por ejemplo, en algunas implementaciones, el proceso de capturar y detectar dedos y puntas del dedo puede ser resumido en las siguientes etapas. (1) capturar imagen de la mano, después (2) invocar un clasificador en cascada que está entrenado para encontrar la primera región de la punta del dedo, después otro clasificador que está entrenado para encontrar la segunda región de la punta del dedo y así sucesivamente.

Por medio del ejemplo y sin limitación, el uso de un clasificador (tal como un clasificador LBP) puede ser implementado para encontrar las puntas del dedo en la imagen, además de esto también puede ser ventajoso usar primero un clasificador para encontrar una región mayor de la mano de tal como la mano completa o los 4 dedos de la mano, después un método secundario para localizar una región menor (tal como las puntas de los dedos o falanges intermedias) dentro de la región mayor. El método secundario podría ser otro clasificador entrenado para localizar cada una de las regiones menores. Los resultados del clasificador menor podrían además ser filtrados usando un conocimiento de las relaciones esperadas (por ejemplo, relaciones prescritas entre cada región menor (por ejemplo los cuatro (4) dedos entre la mano se mantienen planos con dedos cerrados que tienen una relación de posición conocida que puede ser usada para excluir coincidencias falsas). La filtración adicional podría ser aplicada encontrando las posiciones de otras características prominentes de la mano (tales como las uniones entre los dedos), y usar esta información para filtrar los resultados a partir del clasificador. Sin embargo, el clasificador mayor podría ser usado en tiempo real para seguir los dedos conforme el usuario los presenta a la cámara y asegurar que el enfoque y exposición sean optimizados para la mano antes de activar automáticamente la captura de imagen y/o coincidencias biométricas.

Como se indicó previamente y se describe además en la presente, el procesador puede ser configurado para detectar y seguir los dedos en tiempo real

conforme el usuario está presentando los dedos a la cámara y las imágenes están siendo capturadas usando la cámara. La posición de seguimiento de las imágenes puede ser usada para detectar cuando los dedos son suficientemente estables posicionalmente y mejorar la calidad de la imagen de verificación y la confiabilidad del reconocimiento del dedo.

En algunas implementaciones, el procesador puede ser configurado para acelerar la detección del dedo en tiempo real intercambiando dinámicamente entre un método de detección de objeto y un método de seguimiento, más rápido, tal como coincidencia de plantilla o flujo óptico. Por ejemplo, cuando una serie de cuatro puntas del dedo han sido detectadas, pueden haber sido determinadas para representar una mano, el procesador configurado puede seguir los dedos usando un algoritmo de flujo óptico. Como un resultado, las posiciones del dedo pueden ser seguidas con latencia significativamente inferior, y velocidad de marco superior, que si, por ejemplo, un Clasificador en cascada también se aplica a marcos de imagen subsecuentes. La alta velocidad se puede lograr restringiendo el espacio de búsqueda en la imagen que es buscada por el procesador a las regiones de imagen local y el procesador puede ser configurado para solamente coincidir píxeles que representan distintas características, tales como el centro de un dedo.

Si un dedo se desplaza demasiado lejos, o deja el campo de visión, el seguimiento del objeto puede fallar. Después de detectar una falla por el procesador, el procesador puede volver al método de detección de objeto inicial, es decir, un clasificador en cascada. En el caso de seguimiento de cuatro dedos, el procesador puede medir las posiciones relativas de los dedos (por ejemplo, distancia entre los centros del dedo) y si la distancia ha sido determinada por haberse alterado significativamente (por ejemplo, arriba de un valor de umbral prescrito), el sistema puede volver a la detección del objeto.

Preferiblemente, el sistema de captura es capaz de detectar cuando los dedos de un usuario son mantenidos estacionarios (dentro de una cierta tolerancia) para prevenir el movimiento de desenfoque en la imagen de verificación. Esto se puede lograr, por ejemplo, siguiendo un objeto entre marcos (por ejemplo, computando un vector de viaje) y capturando la imagen de verificación de alta resolución cuando la velocidad del objeto cae por debajo de un umbral de velocidad.

Errores menores en la localización de una posición de los objetos pueden propagarse en el cálculo de un vector de velocidad. Los métodos tales como Clasificadores en Cascada a menudo introducen fluctuaciones artificiales en la

posición de un objeto de marco a marco (el centro de los objetos “se mueve de un lado a otro”). Este ruido de posición interfiere con la determinación cuando un objeto es estacionario. El seguimiento usando flujo óptico, sin embargo, como se describe anteriormente, tiene ruido disminuido y proporciona actualizaciones más rápidas de la posición de un objeto, y puede hacer detección del objeto estacionaria significativamente más confiable.

Además, en algunas implementaciones, la información de la longitud del dedo puede ser almacenada y usada como parte del algoritmo de identificación de la punta del dedo, algún peso podría ser colocado en el hecho de que las huellas del dedo se espera en ubicaciones relativas particulares en la imagen, y esto podría mejorar la confiabilidad del algoritmo que encuentra la huella del dedo, y por ejemplo, ayuda a rechazar las coincidencias de las huellas que se hacen por error. Lo mismo es cierto para información acerca de la altura y anchura de cada uno de los dedos. Además, el color de la piel de los usuarios podría ser almacenado en el registro y usado como una identificación biométrica adicional y/o mediciones de verificación de vida. Esto tiene la ventaja de que las huellas de falsificación las cuales poseen la huella correcta pero no el tono de piel correcto pueden ser rechazadas como falsificaciones (por ejemplo, moldes de silicona rosa, o impresiones láser blanco y negro a partir de huellas dactilares latentes recuperadas).

La Figura 4 representa una rutina ejemplar 400 para detección de la punta del dedo a partir de imágenes capturadas de dedos y las imágenes correspondientes. Como se muestra, en la etapa 405 se obtienen imágenes capturadas que incluyen una pluralidad de dedos. La imagen de alta resolución ejemplar se muestra como imagen 405a. En la etapa 410, las imágenes son a escala inferior/convertidas a imágenes de escala de grises y se aplica una cascada mayor para detectar la mano dentro de la imagen. La imagen de escala de grises ejemplar y una pluralidad de márgenes representados alrededor de las regiones de la mano detectadas son representadas en la imagen 410a. En la etapa 415 la región más grande de la mano detectada es seleccionada y la región es alargada para incluir el área circundante (por ejemplo, una región expandida) además de la detección de la punta del dedo. La imagen a escala de grises ejemplar y el margen representado alrededor de la región del dedo expandida y seleccionada es representada en la imagen 415a. Entonces en la etapa 420, uno o más clasificadores en cascada de sensibilidad superior se aplican para detectar regiones menores, es decir, regiones de la punta del dedo para cada uno de los dedos. La imagen en la escala de grises ejemplar y los márgenes representados

alrededor de una pluralidad de regiones de la punta del dedo detectadas, se representa en la imagen 420a. Como se muestra, las regiones de la punta del dedo detectadas pueden exceder el número de puntas del dedo actuales en la imagen. Entonces en la etapa 425, las regiones de la punta del dedo son filtradas. La filtración se describe además en la presente con relación a la Figura 4B. La imagen en la escala de grises ejemplar y los márgenes representados alrededor de las regiones de la punta del dedo detectadas filtradas son representadas en la imagen 425a. Entonces en la etapa 430, las regiones de la punta del dedo de interés (ROI) son ajustadas (por ejemplo, redimensionadas o extendidas hacia abajo) para corregir la relación de aspecto. La imagen en la escala de grises ejemplar y los márgenes representados alrededor de las ROIs redimensionadas y detectadas son representados en la imagen 430a.

La detección del dedo es preferiblemente robusta a iluminación interior y exterior, donde las imágenes tomadas con iluminación pueden ser sustancialmente diferentes. Por ejemplo, en ambientes con poca luz, el fondo a menudo se subexpone y se vuelve oscuro, mientras que en la luz solar intensa y difusa, el brillo del fondo puede exceder aquel de los dedos y el sombreado puede ser significativamente diferente. Por consiguiente, en algunas implementaciones, el método de detección del dedo puede ser mejorado determinando, por el procesador del dispositivo móvil, la cantidad de luz ambiental y, con base en el nivel de luz detectado, cambiar a una o más trayectorias óptimas para un nivel de luz particular en tiempo real. Los niveles de luz, por ejemplo, podrían ser leídos de un medidor lux a base de hardware, tal como aquel encontrado en teléfonos móviles para ajustar el brillo de la pantalla, o estimado a partir de los ajustes de exposición de la cámara.

En tal implementación, uno o más clasificadores que son específicos a los niveles de luz respectivos pueden ser almacenados y disponibles al procesador para realizar la segmentación del dedo. Por ejemplo, un primer clasificador en cascada, que se usa para detectar una o más regiones de los dedos, puede ser entrenado con imágenes tomadas en luz ambiental alta, mientras un segundo clasificador en cascada es entrenado para tomar imágenes en baja luz ambiental. Con base en el nivel de luz medido, el procesador configurado del dispositivo móvil puede aplicar el clasificador apropiado. Más específicamente, el primer clasificador puede ser usado por el procesador para detección como una falta, a menos que los niveles de luz excedan un umbral, en tal caso el segundo clasificador puede ser usado. El cambio entre los clasificadores puede ocurrir en tiempo real, por ejemplo, si una secuencia de marcos

de imagen que tienen diferentes niveles de iluminación ambiental están siendo capturados y analizados. También se puede apreciar que el método anterior de aplicar clasificadores específicos de la luz ambiental puede ser aplicado a imágenes que son inicialmente capturadas durante el proceso (por ejemplo, imágenes de baja resolución capturadas mientras el usuario está posicionando sus dedos en la ubicación apropiada en frente de la cámara) o subsecuentes capturas de imagen de alta resolución (por ejemplo, imágenes de alta resolución capturadas después que los dedos son detectados en las capturas de imágenes iniciales y determinados por estar en foco).

Sin embargo, en algunas implementaciones, con base en el nivel de luz medido, el procesador del dispositivo móvil configurado puede implementar selectivamente etapas de preprocesamiento de imagen de destello artificial como se describe además abajo. Por ejemplo, cuando los niveles de luz son suficientemente altos, el proceso de destello artificial puede ser aplicado para así evitar utilizar la bombilla destello para iluminar el sujeto.

Ningún procedimiento único para detección de dedos es garantizado por ser 100% exitoso, sin embargo, el procesador puede ser configurado para calcular una métrica para calidad de detección, y con base en la métrica, aplicar una serie de métodos de detección hasta que se logra un resultado de calidad bastante alta. Por ejemplo, en el caso de detectar todos los cuatro dedos, el procesador configurado puede computar un registro para determinar cuál serie de cuatro detecciones representa más probablemente una mano, como se describe además en la presente. Si este registro es pobre (por ejemplo, no cubre un umbral prescrito), o los dedos se pierden, el procesador configurado puede aplicar técnicas de detección adicionales. Las técnicas de detección adicionales pueden estar en la forma de un clasificador entrenado de manera diferente, o algún otro procedimiento no relacionado. Sin embargo, en algunas implementaciones, el procesador configurado puede estimar perder ubicaciones de dedos de conformidad con las métricas de la mano conocidas de los usuarios, por ejemplo, como se determina a partir de las capturas de autenticación o registro previo. Se puede apreciar que el orden particular en el cual estos procedimientos son aplicados no tiene que ser invariable, y las técnicas de detección particulares que son implementadas y el orden de aplicación pueden ser selectivamente aplicados por el procesador como una función de las condiciones ambientales medidas, capacidades del hardware y el dispositivo móvil particular, o adaptada con el tiempo a un usuario específico (por ejemplo, con base en los algoritmos de aprendizaje de máquina y/o entrenamiento). En vista de lo anterior,

puede ser apreciado que, para mejorar la velocidad de detección, el procesador puede ser configurado para aplicar el procedimiento de segmentación en niveles en el cual los algoritmos de segmentación más rápidos (y potencialmente menos precisos) son aplicados primero y, en el caso que la calidad de los resultados no sea suficiente, la transición a algoritmos más robustos (y algunas veces procesamiento más intensivo) para detectar más precisamente los segmentos de la punta del dedo.

Como se indica anteriormente y además como se describe en la presente, los algoritmos de reconocimiento a base de dedos ejemplares implementados por el procesador del dispositivo móvil pueden incluir una o más etapas de mejoramiento de imagen para mejorar la detección del dedo y extracción de la característica. Debido a que los métodos de detección tales como Clasificadores en Cascada a menudo funcionan en imágenes en escala de grises, por lo tanto, la información de color se pierde, por ejemplo, si solamente se usa brillo como una entrada. Por consiguiente, los métodos para detectar objetos con características de color conocidas, tales como la mano humana, pueden ser benéficamente mejorados potenciando las regiones que representan el color esperado previo a la conversión a escala de grises.

En una implementación ejemplar, un método de pre-procesamiento de imagen aplicable a detección del dedo implementado por el procesador incluye Modelos de Piel Adaptivos. Más específicamente, el procesador puede ser configurado para analizar una o más de las imágenes capturadas y localizar una región de tono de piel conocido, por ejemplo detectando una mano dentro de una imagen, y después se computa un modelo de color. La imagen es entonces convertida en espacio de color HSV y una función de densidad de probabilidad (PDF) se fija a tanto la distribución del matiz como a los valores de saturación de píxeles dentro de la región de piel pre-determinada. Los píxeles restantes en la imagen están localizados dentro del PDF y se extrae una probabilidad (valor-p) que representa la probabilidad de que un píxel representa la piel. Preferiblemente, el proceso es iterativo en que todos los píxeles que exceden un valor-p umbral son usados para refinar el modelo previo, y el modelo actualizado es entonces aplicado, usando el procesador, a todos los píxeles. En algunas implementaciones, asumiendo que las regiones de la piel son continuas, los píxeles con bajos valores-p, pero los cuales son rodeados por píxeles con altos valores-p, también pueden ser incluidos en el modelo. El proceso puede ser detenido después de un número fijo de iteraciones o cuando el número de píxeles de la piel no se incremente más significativamente (es decir, sin más incrementos de una cantidad prescrita, convergencia). Los valores-p que han convergido pueden entonces ser

usados ya sea directamente (convertidos a imagen de escala de grises) como entrada para algoritmos de detección adicional o, además alternativamente, pueden ser usados para aclarar las regiones de la piel en la imagen con relación al fondo, regiones que no son piel (por ejemplo, actuando como un “destello artificial”).

En el caso de dedos que son presentados a la cámara del dispositivo móvil en una ubicación relativamente predeterminada (por ejemplo, como guiado usando una guía en pantalla), el procesador puede ser configurado para asumir que una región particular es altamente probable que represente el tono de piel (por ejemplo, una región centralizada de la mano en la guía). Por consiguiente, esta región asumida puede actuar como la región inicial para construir un modelo de piel. Además o alternativamente, el tono de piel puede ser registrado cuando un usuario se registra con el sistema (por ejemplo, completado sin el uso de un modelo de piel).

La Figura 4B representa una rutina ejemplar 450 para filtración de segmentos/regiones de la punta del dedo detectadas (es decir, etapa 425 de la Figura 4A). La filtración en general se refiere a la selección de una mejor serie de segmentos de punta del dedo (es decir, seleccionar un segmento de la punta del dedo para cada uno de los dedos que son más probable que correspondan al segmento de la punta del dedo actual).

El proceso comienza en la etapa 455 en la cual las detecciones de la punta del dedo son clasificadas en la dirección horizontal (“X”) (por ejemplo, arregladas en una dirección que es perpendicular a la orientación de los dedos de conformidad con el orden de los dedos). Entonces en la etapa 460, las combinaciones de las cuatro regiones de la punta del dedo son generadas usando la pluralidad de regiones de la punta del dedo detectadas. La imagen en la escala de grises ejemplar y los márgenes representados alrededor de una combinación de cuatro regiones de la punta del dedo detectadas son representados en la imagen 460a.

Entonces en la etapas 465-480, cada una de las series combinadas de cuatro regiones de la punta del dedo son clasificadas. La clasificación incluye analizar las regiones de la punta del dedo para determinar las características físicas de las regiones de la punta del dedo individuales y/o regiones de la punta del dedo múltiples y comparar las características medidas con las características esperadas. Como se describe además en la presente, la clasificación se puede basar en un análisis comparativo de las características físicas de uno o más segmentos de la punta del dedo con relación u otros segmentos de la punta del dedo y, además o alternativamente, con relación a las características físicas de la pluralidad de dedos

tales como la anchura total de la región de la mano previamente detectada (por ejemplo, “anchura de mano” como se detecta en la etapa 415).

Más específicamente, en algunas implementaciones, la anchura combinada de las detecciones en una serie puede ser comparada con la anchura de la mano y clasificada con base en la comparación. Además o alternativamente la distribución de las anchuras de las detecciones (por ejemplo, la distancia de centro a centro entre segmentos adyacentes del dedo) también puede ser clasificada con relación a una distribución de anchura esperada de los segmentos del dedo en vista de la anchura de la mano. La distribución de la anchura esperada puede ser determinada como un promedio a partir de una serie de entrenamiento de dedos previamente identificados. Las series de entrenamiento y la serie pueden ser normalizadas de conformidad con la anchura de la mano para comparación precisa. Por ejemplo, la imagen 470a, una imagen a escala de grises ejemplar de cuatro dedos, los márgenes representados alrededor de una combinación de cuatro regiones/segmentos de la punta del dedo detectados y la distancia media a media medida entre los segmentos adyacentes $d1$, $d2$, y $d3$.

En algunas implementaciones, cada comparación particular puede ser asignada a un peso, de manera que la clasificación calculada es una función de los pesos. Por ejemplo, las medidas importantes/menos conclusivas (por ejemplo, mediciones con inferior precisión o exactitud o que tienen menos confiabilidad) pueden ser discontinuadas por ser asignadas a un peso inferior para así no desviar los resultados totales de la clasificación. Por ejemplo y sin limitación, como la longitud relativa del dedo meñique tiene varianza superior entre individuos, la influencia de la distancia medida en Y determinada con relación al dedo meñique puede ser “ponderada baja” por consiguiente. La Tabla 470b en la Figura 4B representa anchuras ejemplares, pesos y anchuras esperadas usadas para clasificar las características de distancia relativas. Como se muestra en la tabla 470b, una distancia relativa esperada ejemplar entre los dedos adyacentes es $1/4$ de la anchura total de los cuatro dedos y cada uno es asignado con un peso de 1.

En la etapa 475, las anchuras de los segmentos de la punta del dedo. La comparación de las anchuras del dedo se puede basar en las anchuras relativas esperadas de dedos particulares. Por ejemplo, los dedos índice se espera sean más largos con relación a los dedos finales, por consiguiente, la anchura relativa de las regiones/segmentos de la punta del dedo pueden ser clasificados de conformidad con tales comparaciones de segmento de dedo individual. La imagen en la escala de

grises ejemplar de los dedos y cuatro regiones de la punta del dedo detectadas posibles que corresponden a los dos dedos de en medio (dedo índice y medio) son representados en la imagen 475a.

De manera similar, en la etapa 480, la posición relativa de las regiones de la punta del dedo en la dirección Y puede ser clasificada de conformidad con la longitud esperada del segmento de la punta de los dedos respectivos. Por ejemplo, los dos dedos de en medio en general se espera que sean superiores en la dirección Y con relación a los dedos finales y los segmentos de la punta del dedo pueden ser clasificados de conformidad con tales características de posición relativa esperados. Por consiguiente, la distribución de altura de los segmentos de la punta del dedo en la dirección Y (es decir, la dirección que es paralela a la orientación de los dedos) puede ser analizada. Más específicamente, analizar la distribución de Y incluye analizar el “patrón de longitud” de los dedos como se representa en 480a. Es decir, el dedo índice se espera sea más corto que el dedo medio, el dedo medio más largo que el dedo anular, y el dedo anular más largo que el dedo meñique. Por lo tanto, las regiones de interés para el sujeto deben tener posiciones que siguen un patrón “arriba, abajo, abajo” en Y, desde el dedo índice al dedo meñique. El patrón esperado preciso puede ser determinado como un promedio de una serie de entrenamiento de dedos previamente identificados. Se puede apreciar que la serie de entrenamiento y la serie de segmentos de la punta del dedo pueden ser normalizados de conformidad con las dimensiones de la mano y/o dedo respectivos para comparación precisa de longitudes y/o posiciones relativas en Y. Por consiguiente, el procesador puede ser configurado para computar la distancia en Y entre los límites superiores de las varias regiones/segmentos de interés, de este modo proporcionando tres distancias; índice a medio, medio a anular, anular a meñique. El procesador puede entonces usar la anchura de la mano para normalizar las distancias, haciéndolos comparables a través de diferentes escalas de la mano. Posteriormente, las distancias pueden ser comparadas con el patrón esperado y la combinación de dedos puede ser clasificada como una función de la comparación. La imagen en la escala de grises ejemplar de los dedos y cuatro posibles regiones de la punta del dedo detectadas siendo comparadas en la dirección Y son representados en la imagen 480a. También se puede apreciar que la altura relativa, anchura, posición-Y y posición-X de las regiones de la punta del dedo también pueden ser ponderados de conformidad con la importancia y/o confiabilidad.

Además de las medidas anteriores, el procesador configurado también puede

clasificar las combinaciones de los segmentos de la punta de dedo de conformidad con las características de iluminación de los segmentos de la punta del dedo representados. Más específicamente, se puede esperar que los dedos aparezcan con iluminación aproximadamente igual en la imagen. Por consiguiente, el procesador configurado puede, para cada combinación de segmentos de la punta del dedo, medir la iluminación a través de la combinación de segmentos de la punta del dedo y clasificar la varianza en la iluminación. Para velocidad y precisión, solamente los valores de píxel en el centro de cada segmento de la punta del dedo (por ejemplo, dentro de un rectángulo de 10 por 16), puede ser sumado y la varianza de las 4 sumas determinada. La alta varianza implica que uno o más segmentos de la punta del dedo son correctamente posicionados y una peor clasificación puede ser asignada.

Entonces en la etapa 485, las clasificaciones cumulativas de las combinaciones de las regiones de la punta del dedo son ponderadas, sumadas y la mejor combinación de segmentos se define de conformidad con la clasificación calculada. La imagen en la escala de grises ejemplar de los dedos y los márgenes representados alrededor de la menor combinación de clasificación de cuatro regiones de la punta del dedo detectadas son representadas en la imagen 485a.

Además, en algunas implementaciones, la examinación puede ser realizada analizando las frecuencias y orientaciones de los bordes dentro de cada región. Además o alternativamente, el segmento de la imagen que contiene los dedos puede ser identificado como el(los) segmento(s) que principalmente llenan la ubicación de la guía de posicionamiento del dedo en pantalla.

En alguna implementación, en el caso de usar por ejemplo solamente cuatro (4) dedos para identificación, Un procedimiento robusto para registrar y verificar las cuatro huellas de los dedos (4) podría correr como sigue: a). Guiar al usuario a posicionar cuatro dedos de la mano (4) en frente de la cámara y capturar una imagen de destello, b). Opcionalmente usar un algoritmo de procesamiento de imagen (como se explica previamente) para identificar la ubicación de las cuatro huellas (y otras regiones de interés), c). Resaltar estas regiones al usuario mediante por ejemplo, súper imponiendo elipses sobre las regiones de la huella, y pedir que el usuario ya sea acepta el reconocimiento de la huella del dedo como precisa, o ajuste las elipses de huellas del dedo mal localizadas arrastrando las elipses a la posición correcta. De esta forma se aseguran huellas registradas precisas, d). Usar las huellas registradas precisas para procedimientos de verificación futura. Esto puede incluir el proceso de usar las huellas registradas para encontrar las huellas de verificación en la imagen de

verificación.

Sin embargo, en algunas implementaciones, en el caso de capturar cuatro (4) huellas, la imagen detectada de los cuatro dedos puede entonces ser dividida en cuatro dedos individuales definiendo uniones entre cada uno de los dedos adyacentes, por ejemplo, localizando puntos donde existe perturbación en las orientaciones de las crestas. Estos puntos son referidos como puntos singulares. Entonces, un algoritmo de agrupamiento de media-K puede ser utilizado para agrupar los puntos determinados en cuatro (4) grupos que representan los cuatro dedos. En alguna implementación, la media-K puede usar una función de distancia especial para capturar la matriz de distancia que será usada en el algoritmo de agrupación. Esta función especial resultará en medidas de menos distancia a puntos que se localizan en el mismo dedo aún si están lejos con respecto a la distancia Euclidiana tradicional. Entonces, los algoritmos de segmentación que crecen en la región pueden ser utilizados para segmentar individualmente cada dedo.

Entonces, para cada dedo, al menos una región de la falange distal de cada dedo puede ser identificada dentro de las imágenes. Preferiblemente, la región del dedo la cual está localizada entre la punta del segmento del dedo y las líneas más gruesas entre las falanges intermedia y distal, se identifica por contener las características más discriminativas las cuales son minuciosas.

Tanto los dedos como las manos tienen un espacio relativamente restringido de formas posibles, por consiguiente, en algunas implementaciones, los Modelos de Forma Activa y Modelos de Apariencia Activa pueden ser procedimientos útiles para implementar el reconocimiento dactilar de huella sin contacto. Por ejemplo, para localizar y segmentar una mano de una imagen objetivo, un Modelo de Distribución de Punto es computado primero colocando series de puntos sobre futuras manos, tales como márgenes de la punta del dedo, dentro de los imágenes de ejemplo. El modelo es entonces inicializado dentro de la imagen objetivo formando una estimación inicial en cuanto a la posición de las manos usando una guía para la colocación de la mano del usuario, u otra técnica de procesamiento de imagen. Por ejemplo, un Clasificador en Cascada puede ser usado para proporcionar un estimado inicial a la ubicación de las manos. El mejor ajuste para el modelo se encuentra entonces comparándolo iterativamente con los datos de la imagen y actualizando las posiciones del punto.

Los puntos del modelo ajustado son usados para extraer regiones de interés para reconocimiento. Por ejemplo, puntos que describen márgenes de la punta del dedo son usados para extraer huellas dactilares.

De manera similar, un Modelo de Forma Activa que describe la forma de un dedo puede ser usado para segmentar puntas del dedo individuales. Por ejemplo, las regiones de imagen que contienen las puntas del dedo son primero encontradas usando un Clasificador en Cascada y después segmentadas usando el modelo para remover tanto los dedos del fondo como cercanos. Además, los Modelos de Forma Activa pueden ser ajustados a usuarios individuales. Por ejemplo, dado un ajuste de modelo correcto, confirmado por el usuario durante el registro del sistema, el modelo se ajusta para describir mejor tales formas de mano y dedos de los individuos. Esto incrementa la velocidad y confiabilidad del reconocimiento, y desviaciones a partir del modelo pueden ser usadas para identificar las falsificaciones.

Para máxima calidad de extracción de huella del dedo un usuario puede ser alentado a colocar su mano y dedos en una ubicación óptima con relación a la posición de tanto la fuente de luz de iluminación como la cámara, por ejemplo, proporcionando una guía visual o contorno de la colocación del dedo óptima en la pantalla del dispositivo. Esto podría ser para posicionar las huellas dactilares cerca del centro del campo de vista de la cámara, con huellas que subtendiendo un ángulo máximo a la cámara de aproximadamente ± 20 grados. Por ejemplo, los dedos pueden ser colocados bastante cerca de la fuente de luz para minimizar el ángulo de incidencia con rayos de iluminación, previniendo la pérdida del detalle en las superficies anguladas, mientras esta bastante cerca para iluminación suficientemente intensa. Concurrentemente, los dedos están orientados para reflejar máximamente la iluminación hacia la cámara y posicionarse bastante cerca a la cámara para asegurar suficiente densidad de píxel para el reconocimiento.

La calidad de la huella capturada puede ser además mejorada agregando fuentes de iluminación adicionales, o fuentes extendidas al sistema de cámara del teléfono inteligente para dispersar la extensión espacial de la fuente de iluminación. Por ejemplo, agregando 4 LEDs en las esquinas del teléfono inteligente o tableta la luz se reflejará favorablemente por más regiones de la huella del dedo que conduce a una calidad superior de captura de la huella.

Una vez que las regiones relevantes de los dedos son identificadas, en la etapa 315, las regiones relevantes pueden ser mejoradas. Más específicamente, el procesador del dispositivo móvil 110, el cual es configurado ejecutando los módulos de software 130, que incluye, preferiblemente, el módulo de análisis 172, puede procesar las porciones de las imágenes para mejorar el detalle de las imágenes, por ejemplo, usando una serie de filtros Gabor, sintonizando a los mapas de orientación de cresta

suavizados. En alguna implementación, el objetivo principal de este mejoramiento de imagen es generar imágenes de huellas dactilares que son similares a las imágenes de la impresión de las huellas dactilares las cuales se capturan usando sensor de escáner de vida y usualmente almacenan en bases de datos legales como el IAFIS. Esta similitud significa que la imagen capturada usando dispositivos móviles están imitando la misma calidad y atributos como las imágenes capturadas de sensores de escáner de vida. Esta similitud es deseable para garantizar la posibilidad de coincidir las imágenes capturadas por los dispositivos móviles contra las imágenes de la impresión de huellas dactilares almacenadas en bases de datos legales tales como el IAFIS.

Para mejorar la extracción de las características discriminatorias de las puntas del dedo puede ser ventajoso usar filtros de mejoramiento para reforzar el contraste entre crestas y surcos. En algunas implementaciones, el procesador del dispositivo móvil puede aplicar Ecualización de Histograma para reforzar el contraste de imagen local distribuyendo uniformemente intensidades sobre el intervalo de valores posibles (típicamente $[0,255]$ en imágenes en escala de grises). Esto se puede lograr computando un histograma acumulativo de intensidades de píxel, normalizando al valor máximo en el intervalo permitido, y remapeando píxeles de fuente de conformidad con su ubicación en esta distribución.

El mejoramiento de contraste tiene la desventaja de ser no discriminante y así mejorar el ruido de fondo así como también la señal de interés. Como tal, puede ser benéfico aislar solamente aquellas señales de interés por filtración previo al mejoramiento del contraste. Por ejemplo, el procesador puede aplicar un Filtro de Paso de Banda para remover las señales con frecuencias que no corresponden a la frecuencia esperada de las crestas de la huella dactilar. Una de tal implementación remueve las altas frecuencias sustrayendo una imagen de fuente filtrada de desenfoque Gaussiano a partir de la imagen de fuente sin procesar. El resultado puede entonces ser filtrado nuevamente para remover las bajas frecuencias aplicando otro filtro de desenfoque Gaussiano con aproximadamente radio más pequeño. Una ecualización de histograma puede entonces ser aplicada al resultado del paso de banda para lograr una imagen óptima para extracción de características.

En la etapa 320, los detalles minuciosos de cada uno de los dedos se extrae y se genera un identificador biométrico. Como podría entenderse por aquellos en la técnica, los detalles minuciosos se refieren a los puntos donde las crestas de una huella dactilar terminan, y textura se refiere al patrón definido por las crestas. Más

específicamente, el procesador del dispositivo móvil 110, el cual es configurado ejecutando los módulos de software 130, que incluyen, preferiblemente, el módulo de análisis 172, analiza las imágenes mejoradas para extraer características a partir de al menos la región distal de cada dedo usando un algoritmo tal como el algoritmo de extracción de detalles minuciosos.

La mayoría de los sistemas automáticos para comparación de huellas dactilares se basan en la coincidencia de detalles minuciosos; por lo tanto, la extracción confiable de detalles minuciosos es una tarea importante. Muchos de tales métodos requieren la imagen a escala de grises de la huella dactilar para ser convertidos en una imagen de esqueleto. Entonces, un escáner de imagen simple permite la detección de píxeles que corresponden a los detalles minuciosos donde las crestas de la huella dactilar terminan y se bifurcan. Los detalles minuciosos extraídos pueden ser almacenados como series de puntos en el plano de dos dimensiones.

Finalmente, un algoritmo de coincidencia a base de detalles minuciosos puede ser realizado por el procesador configurado para generar la clasificación de similitud entre las huellas dactilares. Estos algoritmos de coincidencia calculan la clasificación de similitud entre las huellas dactilares encontrando la alineación entre la plantilla y las series de detalles minuciosos de entrada que resultan en el número máximo de apareamientos de detalles minuciosos.

Las características extraídas a partir de la región distal pueden ser almacenadas junto con otras características que son extraídas de manera similar a partir de las restantes regiones identificadas de los dedos y/o la mano. Tales características pueden ser distinguidas en uno o más identificadores biométricos los cuales incluyen uno o más vectores de características.

Durante el registro, en la etapa 325, tales vectores de características son almacenados en la memoria como un identificador biométrico (por ejemplo, plantilla) para uso para asegurar las etapas de verificación del usuario. Alternativamente, durante la verificación del usuario (etapa 330), el identificador biométrico se compara con la versión almacenada durante el registro.

Más específicamente, durante el proceso de verificación, los dedos del usuario son capturados y el identificador biométrico es generado como se describe con relación a las etapas 305-320. Sin embargo, en la etapa 330, los vectores de característica de consulta son entonces comparados con los vectores de características de registro y almacenados. Con base en la comparación, se genera una clasificación de coincidencia por el procesador configurado 110 con relación a la

similitud de la coincidencia. Si la clasificación de coincidencia representa una coincidencia suficientemente cercana, el usuario puede ser determinado por pasar el procedimiento de verificación.

En una o más implementaciones, la clasificación de coincidencia puede ser una clasificación de coincidencia combinada con base en las huellas dactilares de consulta que coinciden (por ejemplo, vectores de característica de consulta) a huellas dactilares registradas individualmente y determinando una clasificación de coincidencia combinada. Más específicamente, a partir de una base de datos de imágenes de manos, las imágenes pueden ser apareadas, hasta con dos distintas clases de pares: pares de imágenes de la misma mano, y pares de imágenes de diferentes manos. Para cada par de dedos en estas manos (Por ejemplo, índice con índice), una clasificación de coincidencia puede ser calculada la cual mide la cercanía de estas imágenes de la mano, con clasificaciones superiores que representan una coincidencia más cercana.

Estas clasificaciones pueden ser trazadas para formar distribuciones de clasificación. Para cada tipo de dedo (por ejemplo, dedo anular), existen dos distribuciones, estas clasificaciones a partir de imágenes coincidentes del mismo dedo de la misma mano, y el mismo dedo a partir de diferente mano (es decir, un impostor).

Estas distribuciones de clasificación pueden ser consideradas como distribuciones de probabilidad, lo cual proporciona la probabilidad de que una clasificación de coincidencia dada pertenece a una de las distribuciones. Estas distribuciones empíricamente derivadas pueden ser suavizadas de ruido y caracterizadas compactamente ajustándolas a una distribución conocida, por ejemplo, la distribución gamma.

Dado un par no caracterizante de imágenes de dedos, el sistema de identificación ejemplar puede ser configurado para determinar una clasificación de coincidencia. Estas distribuciones de probabilidad ajustadas pueden entonces ser usadas para determinar la relación de probabilidad (índice de probabilidad) que el par de imágenes del dedo pertenecen al mismo dedo o a un dedo diferente.

Cuando se hace una coincidencia completa de los cuatro dedos, el sistema configurado puede probar una imagen desconocida (la imagen de "prueba") contra imágenes previamente registradas de un sujeto conocido (las imágenes de "galería"). Para cada par de dedos de prueba contra los dedos de galería, el sistema puede determinar un índice de probabilidad. Estas relaciones pueden entonces ser multiplicadas en conjunto, y el resultado final proporciona una medida total de la

oportunidad de que la imagen de prueba pertenece al sujeto quién proporciona la imagen de galería.

Este método tiene la ventaja de no ser degradado por dedos específicos que tienen pobre capacidad predictiva; en particular el dedo meñique es menos probable que proporcione una coincidencia claramente predictiva que los otros dedos. También permite alguna tolerancia contra las imágenes malas; si un dedo hace una pobre coincidencia, puede ser compensado si el otro dedo hace una coincidencia particularmente buena.

Mientras la combinación de clasificación a través de dedos múltiples proporciona tolerancia contra imágenes malas, es teóricamente posible para una clasificación de coincidencia de galería/prueba única será bastante grande para provocar un paso total. Esto podría ser más fácil producir falsificaciones, por ejemplo, si un atacante es capaz de producir un facsímil de muy alta calidad de uno de los dedos del usuario autorizado. Un método ejemplar para mitigar este problema puede incluir requerir, por el procesador durante el proceso de coincidencia y clasificación, un número mínimo de los dedos de prueba para producir individualmente clasificaciones de coincidencias que cruzan un umbral secundario, así como también requerir que la combinación de clasificaciones de coincidencias pasen el umbral de coincidencia primaria con el fin de determinar una coincidencia positiva. Por consiguiente, esta medida podría requerir que cualquier éxito de falsificación duplique exitosamente tal número mínimo de dedos, lo cual es una tarea más difícil que duplicar un dedo único exitosamente. Se puede apreciar que el número mínimo de clasificación de dedos arriba del umbral secundario requeridos por el proceso de autenticación y el valor del umbral secundario, puede ser ajustado para cambiar el riesgo de falsificación contra la resiliencia a la calidad de imagen degradada, como conviene a las necesidades de seguridad de la implementación.

Típicamente cuando se comparan los datos del dedo de consulta con los datos del dedo registrados es importante asegurar que las escalas de las imágenes respectivas sean similares. Por consiguiente, durante el análisis de las imágenes de la huella dactilar en la etapa 320, el procesador configurado 110 puede determinar la frecuencia fundamental de las crestas de la huella dactilar. Durante el registro (por ejemplo, etapa 325), el procesador configurado puede almacenar la frecuencia fundamental. Durante la verificación (por ejemplo, etapa 330), el procesador configurado puede escalar la frecuencia fundamental del punto de verificación para coincidir con la frecuencia fundamental de la huella registrada antes de la

comparación. Además o alternativamente, el procesador puede normalizar la frecuencia de la huella a una frecuencia de referencia prescrita por ejemplo, una (1), de manera que la frecuencia actual no tiene que ser almacenada. Por consiguiente, durante el reconocimiento, la huella de consulta puede ser normalizada al valor de referencia prescrito.

Se debe entender que una o más operaciones de pre-procesamiento pueden ser realizadas en los marcos de imagen previo a generar los vectores de características o previo a comparar los vectores de característica durante la autenticación. Por ejemplo y sin limitación, el pre-procesamiento de los datos de imagen previo al análisis puede incluir orientar los marcos de imagen en espacios coordinados y similares como podría entenderse por aquellos expertos en la técnica.

Las tecnologías existentes que se refieren a la identificación de huellas dactilares a base de imagen implementando algoritmos de escalación existentes en general pierden la escala aproximadamente al 2% de las huellas dactilares resultando en rechazos falsos durante la autenticación. Esto es debido en parte a aquellos algoritmos que usan un número insuficiente de puntos de referencia en una imagen (es decir, usando solamente dos puntos, el punto de la punta/partida de la huella dactilar y el punto de la base/final de la huella) para deducir el tamaño y escala por consiguiente. Para mejorar las operaciones de escalación, de conformidad con uno o más de las modalidades descritas, el procesador puede implementar un algoritmo que analiza la frecuencia promedio de una huella del dedo (por ejemplo, número típico de líneas por pulgada) y normaliza la escala de la(s) huella(s) por consiguiente. Puesto que esta técnica juzga la escalación con base en una serie más grande de los píxeles de las huellas, tomados en muchos puntos a través del área de la huella, se puede lograr confiabilidad considerablemente superior durante el proceso de escalación.

Antes y/o después de las etapas de registro y verificación, el método también puede incluir una etapa de detectar la vida. La detección de vida se representa como etapa 355 en la Figura 3. Un método de detección de vida puede ser implementado para verificar que la imagen de cuatro (4) dedos capturada es de dedos reales en lugar de, por ejemplo, una huella de falsificación o molde de los dedos. Más específicamente, en algunas implementaciones, el procesador del dispositivo móvil 110, el cual es configurado ejecutando los módulos de software 130, que incluye, preferiblemente, el módulo de análisis 172, puede analizar la calidad de imagen de los dedos y determinar si son consistentes con las imágenes de los dedos vivos y/o dedos falsos, los cuales típicamente tienen artefactos notables tales como resolución y

nitidez reducida.

Por ejemplo, como se describe además en la presente, una técnica de detección de vida puede ser alentar al usuario a girar la mano durante la formación de la imagen y el procesador configurado puede determinar que la mano de imagen es apropiadamente tridimensional usando, por ejemplo, técnicas de profundidad de movimiento y técnicas de profundidad de enfoque. Alternativamente, el sistema puede implementar técnicas para detección de vida pasiva, por ejemplo, para analizar la calidad de imagen para comprobar que es suficientemente nítida y no una baja resolución (por ejemplo, a partir de una huella falsificada de la mano). El procesador configurado también puede analizar el color de los dedos para determinar si la coloración es consistente con una imagen de mano viva y/o el color conocido de la mano del usuario. Por lo tanto, en algunas implementaciones, la consistencia de color, en otras palabras, la uniformidad de color de la mano puede ser realizada detectando las puntas de los dedos y la mano simultáneamente. Entonces, separando el área de la mano que no contiene la punta de los dedos la cual consiste de la palma y las falanges inferiores (es decir, la próxima e intermedia) y después determinar el histograma de color de esta área y el histograma de color de las 4 áreas de las puntas de los dedos detectadas. Finalmente, en alguna implementación, comparar estos dos histogramas se puede utilizado como una prueba para la uniformidad de color de la mano y los dedos para determinar la medida de vida, especialmente, si el agresor está usando moldes (es decir, dedos falsos) al sistema de falsificación. Además, el procesador configurado también puede pedir que el usuario haga uno o más posturas con sus dedos, por ejemplo, separe y cierre los dedos o mueva ciertos dedos en una manera particular.

No obstante, en algunas implementaciones, un clasificador puede ser entrenado para distinguir vida de falsificación. El clasificador puede ser entrenado de manera que aprende la diferencia entre las imágenes del dedo real y varias imágenes falsificadas. El procesador que implementa el clasificador puede entonces ser configurado para proporcionar un resultado de falla de paso con base en su entrenamiento.

Además, en algunas implementaciones, como un factor extra de vida de biométricas, las posiciones de las huellas del dedo en la imagen podrían ser tomadas en cuenta, es decir, el usuario genuino tendrá primero, segundo, tercero y cuarto dedos de longitudes particulares. De manera que cuando el usuario mantiene su mano con los dedos extendidos y cerrados, las posiciones de las cuatro (4) huellas del dedo

deben tener un posicionamiento relativo que es consistente con tal usuario particular. Esta información podría ser usada como una comprobación de seguridad adicional para ayudar a prevenir el ataque de falsificación. Por ejemplo un hacker quien encuentra huellas latentes en una pantalla de teléfono es improbable que sea capaz de deducir las longitudes de los dedos del usuario, y así podría ser improbable que los presente correctamente.

Además de los sistemas ejemplares y métodos descritos con relación a la Figura 3, varias alternativas y variaciones están contempladas. En algunas implementaciones, las imágenes registradas de los dedos del usuario no son necesariamente capturadas por la cámara del dispositivo móvil. Preferiblemente, los vectores de características de los dedos podrían ser adquiridos a partir de una fuente alternativa tal como una base de datos pregrabada de las imágenes de los dedos.

En algunas implementaciones, durante el proceso de registro, para captura de los dedos (por ejemplo y sin limitación, cuatro o diez dedos con resolución mejorada, la imagen de cada dedo puede ser capturada secuencialmente en imágenes individuales. En este caso, durante el procedimiento de registro, que despliega en una pantalla la guía del dedo puede alentar al usuario a colocar un dedo en la pantalla en un tiempo y el algoritmo de segmentación puede ser usado para identificar la falange distal y la región de la huella dactilar de los dedos individualmente.

En algunas implementaciones, en lugar de limitar el proceso de coincidencia (por ejemplo, etapa 330) a la comparación de las regiones de la punta del dedo (por ejemplo, falange distal), la comparación podría incluir otras partes de la mano además de las huellas dactilares o en lugar de las huellas dactilares. Por ejemplo la región de interés puede incluir cualquiera de las partes de la mano con patrones detectables, o las falanges distal e intermedia, o los metacarpales. Algunas de estas regiones tienen la ventaja agregada que son más resistentes al ataque de falsificación de este modo proporcionando un nivel superior de seguridad. Por ejemplo, las huellas de la punta del dedo del usuario pueden a menudo encontrarse en el estuche de un teléfono inteligente u otras superficies que el usuario ha tocado. Estas huellas del dedo latentes pueden ser copiadas por un impostor, y un molde creado que podría pasar la verificación. Sin embargo, las huellas en los metacarpales no mucho más difíciles de encontrar puesto que son menos comunes para estas regiones de la mano para tocar superficies para dejar huellas latentes.

En algunas implementaciones, en lugar de usar puntos singulares para separar los cuatro grupos de dedos en dedos separados, el usuario podría ser alentado a

separar sus dedos durante la captura. Estos dedos podrían entonces ser aislados usando un algoritmo de segmentación, y un método de deformación de contorno podría ser usado para identificar las posiciones de cada una de las puntas del dedo.

En algunas implementaciones, la segmentación de las regiones del dedo pertinentes podría ser realizada usando color de piel, frecuencia y orientación. Por ejemplo, un operador de Sobel podría ser implementado por el procesador configurado para enfatizar regiones que están en enfoque (es decir, los dedos en lugar del fondo), para ayudar al proceso de segmentación. Además o alternativamente, la segmentación podría también hacerse extrayendo simplemente regiones fijas a partir de la imagen capturada con relación a regiones que el usuario fue guiado para colocar sus dedos durante el proceso de captura.

En algunas implementaciones, durante el proceso de autenticación, la segmentación puede ser realizada durante la información de huella registrada. Segmentar e identificar y/o coincidir las características de la huella dactilar con base en una plantilla de huella generada durante el registro puede proporcionar mejoramientos sobre las técnicas existentes. Por ejemplo las técnicas de identificación de huella dactilar a base de imagen existentes aíslan una huella dactilar en la misma manera durante el registro y autenticación y, como un resultado, aísla una huella dactilar única a partir de imágenes con éxito no satisfactorio para uso confiable. En algunos casos, el aislamiento exitoso usando los métodos existentes ocurre solamente 96% del tiempo resultando en 4% de rechazos falsos durante la autenticación. Usando tal técnica separadamente en dedos múltiples, este problema se complica.

Sin embargo, de conformidad con una o más de las modalidades descritas, un algoritmo diferente para aislamiento de huella dactilar se realiza por el procesador configurado, es decir, una que usa la huella registrada para encontrar el(los) dedo(s) y aislar/coincidir las huellas durante la autenticación. Esto proporciona desempeño significativamente más robusto. En algunas implementaciones, el procesador configurado puede implementar el proceso de segmentación, por ejemplo, extrayendo características del dedo (tales como detalles minuciosos) a partir de la imagen de los cuatro dedos, y localizar la región de los dedos comparando exhaustivamente todas las ubicaciones de la imagen con las características del dedo a partir de las huellas registradas. La región del dedo se conocerá por estar localizada donde el dedo registrado se encuentra por coincidir las características del dedo en la imagen. Además de minimizar la posibilidad de una coincidencia falsa por características aleatorias en la imagen, la validez de las regiones coincidentes podría ser

comprobada, por ejemplo, en el caso del procedimiento de captura de cuatro (4) dedos, asegurando que los 1ro, 2do, 3er, y 4to dedos se encuentran aproximadamente como se esperaba a partir de la imagen de superposición de guía de usuario, el color de piel es como se esperaba, y similares (por ejemplo, coincidencia de plantilla usando la plantilla registrada para guiar la comparación). No obstante, en lugar de usar este proceso para buscar la imagen completa para ubicaciones del dedo, el intervalo de búsqueda podría ser restringido a las áreas que los dedos se anticipan de la imagen de superposición de guía de usuario.

Además o alternativamente basando la escala de los dedos en frecuencia de crestas fundamentales, el procesador 110 puede ser configurado para escalar la huella con base en uno o más de: la anchura del grupo de cuatro dedos segmentados, la anchura o longitud de cada uno de los dedos de la región de interés, o en puntos específicos en el dedo tal como puntos singulares y las líneas más gruesas en la unión de la falange.

Así como también (o en lugar de) coincidir los dedos con base en detalles minuciosos, el procesador 110 puede también ser configurado para coincidir huellas con base en la textura.

No obstante, en algunas implementaciones, en lugar de usar una imagen de los dedos, varias imágenes podrían ser usadas para registrar o autenticar a un usuario. Las imágenes múltiples pueden ser capturadas por el procesador configurado 110 usando la cámara 145 en varias exposiciones y/o distancias focales para crear una imagen con profundidad de campo y/o intervalo dinámico mejorados. Capturar las imágenes con tales exposiciones variantes y/o distancias focales puede ayudar a asegurar que el enfoque de las huellas en varias ubicaciones a través de las manos es óptimo. Por consiguiente, el procesador configurado puede seleccionar y analizar la(s) imagen(es) o porciones de la imagen que tienen enfoque óptimo en la porción del dedo de interés.

Además o alternativamente, la detección de vida puede ser implementada comprobando que otras métricas son consistentes con aquellas de un dedo real en lugar de una falsificación de dedo moldeado o video o huella. Estas métricas podrían incluir análisis de reflexiones especulares del destello capturado en las imágenes, análisis de las reflexiones especulares a partir del destello en comparación con una imagen tomada sin el destello, color, métricas coloridas (como para rechazar falsificaciones blanco y negro y monocromáticas).

En algunas implementaciones, la vida puede ser detectada por el análisis de

reflexiones especulares o profundidad de la información de enfoque obtenida a partir de las imágenes de los dedos. Por medio de ejemplo no limitante, los sistemas y métodos ejemplares para determinación de vida con base en reflexiones especulares e información de profundidad de enfoque se describen en la presente y en la Solicitud de Patente Estadounidense copendiente y comúnmente asignada Serie No. 62/066,957 titulada SISTEMAS Y MÉTODOS PARA REALIZAR LA IDENTIFICACIÓN Y VERIFICACIÓN DEL IRIS USANDO DISPOSITIVOS MÓVILES QUE UTILIZAN ILUMINACIÓN DE ESPECTRO VISIBLE, presentada el 15 de Octubre de 2014. La vida también puede ser detectada por el análisis de movimiento dinámico de los dedos (por ejemplo, posturas de los dedos) tal como inclinando los dedos, o estirando/estrechando los dedos como se representa a través de una secuencia de imágenes capturadas por la cámara. Por medio del ejemplo no limitante, los sistemas y métodos ejemplares para la determinación de vida con base en el movimiento dinámico de características y posturas biométricas se describen en la presente y en la Solicitud de Patente Estadounidense co-pendiente y comúnmente asignada Serie No. No. 62/041,803, titulada “SISTEMA Y MÉTODO PARA DETERMINACIÓN DE VIDA” presentada el 26 de Agosto de 2014.

En algunas implementaciones, la vida puede ser detectada realizando un análisis de reflectividad de luz emitida sobre las crestas de los dedos durante la captura de imágenes de los dedos. Las crestas de los dedos vivos reflejan el destello no uniformemente, mientras los dedos impresos reflejan el destello uniformemente. Por consiguiente, las propiedades de reflexividad de creta capturadas en las imágenes de los dedos pueden ser analizadas para determinar la vida. Un proceso ejemplar para determinar la vida con base en la reflectividad se describe además en la presente con relación al diagrama de flujo de la Figura 5, e imágenes correspondientes en las Figuras 5B-5C. En la etapa 505, se obtienen entradas al algoritmo de detección de vida. Las entradas incluyen imagen(es) de alta resolución de uno o más de los dedos capturados con el destello encendido, así como también imágenes de alta resolución de los dedos capturados con el destello apagado. Imágenes de destello encendido 505A y destello apagado 505B ejemplares del(los) dedo(s) se muestran en la Figura 5B. En la etapas 510, la(s) imagen(es) de destello encendido son redimensionadas de manera que la huella dactilar dentro de la imagen es aislada. En la etapa 515, las regiones en la(s) imagen(es) de destello apagado que incluyen el dedo correspondiente son segmentadas (por ejemplo de conformidad con los algoritmos de segmentación de huella dactilar ejemplares descritos anteriormente). Por consiguiente,

la huella dactilar representada en la imagen de destello encendido y la huella dactilar correspondiente en las imágenes de destello apagado son aisladas para procesamiento adicional. Las imágenes de destello encendido y destello apagado aisladas ejemplares de la punta de los dedos se muestran como imagen 510A y 515B, respectivamente, en la Figura 5B. Entonces en la etapa 520 se aplica un filtro de alto paso para retener la porción de las imágenes que representan las crestas. Las imágenes de destello encendido y destello apagado filtradas ejemplares de las puntas de los dedos se muestran como imágenes 520A y 520B en la Figura 5B. Entonces en la etapa 525, se calcula la clasificación de vida. En un arreglo ejemplar, la clasificación de vida se calcula como una función de la desviación estándar (a) del histograma generado a partir de la imagen de destello apagado filtrada y la desviación estándar correspondiente (b) del histograma generado a partir de la imagen de destello encendido filtrada (es decir, clasificación de vida = a/b). Por medio del ejemplo, imágenes similares obtenidas durante la aplicación del proceso 500 en imágenes falsificadas de las huellas dactilares son representadas en la Figura 5C. En otra implementación, otras medidas pueden ser computadas a partir de los histogramas de las imágenes de destello encendido y destello apagado filtradas para calcular la clasificación de vida. Lo siguiente son algunos ejemplos de las medidas que pueden ser usadas: (1) la diferencia entre los medios de los histogramas, (2) la diferencia entre los medios de las frecuencias del histograma, (3) la relación de la desviación estándar de las frecuencias del histograma, (4) la diferencia entre la curtosis de los histogramas, y/o (5) el número de los puntos clave correspondientes en las imágenes de destello encendido y destello apagado filtradas. En alguna implementación, la diferencia en las intensidades de píxel del fondo de las imágenes de destello encendido y destello apagado pueden ser usadas como una medida de vida.

Las Figuras 6A-6F representan imágenes de cresta ejemplares de dedos capturados en varias posiciones con relación al campo de visualización de la cámara. En particular, la Figura 6A representa una imagen capturada e imágenes de cresta correspondientes para dedos que están también muy lejos de la cámara y tienen baja resolución de la huella. La Figura 6B representa una imagen capturada e imágenes de cresta correspondientes para dedos que están también muy lejos de la cámara y tienen baja resolución de la huella. La Figura 6C representa una imagen capturada e imágenes de cresta correspondientes que muestran buena resolución debido a que la colocación del dedo es central en el campo de visualización y suficientemente cercano a la cámara. La Figura 6D representa una imagen capturada e imágenes de cresta

correspondientes que muestran una pérdida de reflexiones en los bordes del dedo índice y meñique debido a reflexiones LED de ángulo alto. La Figura 6E representa una imagen capturada e imágenes de cresta correspondientes que muestran una pérdida de reflexiones en las puntas de los dedos debido a reflexiones LED de ángulo alto conforme los dedos son colocados cerca del borde del campo de visualización de la cámara. La Figura 6F representa una imagen capturada e imágenes de cresta correspondientes que muestran una pérdida de reflexiones en las puntas de los dedos debido a reflexiones LED de alto ángulo conforme los dedos son colocados cerca del borde del campo de visualización de la cámara.

En algunas implementaciones, la autenticación a base de huella dactilar puede además ser combinada con identificación facial para proporcionar la seguridad/confiabilidad mejorada de biométricas multimodales. Por ejemplo, en el caso de un teléfono inteligente, los cuatro dedos del usuario podrían ser capturados usando una cámara de cara trasera de teléfonos inteligentes simultáneamente o secuencialmente conforme la captura de rostro y/o iris se hace usando la cámara de cara frontal. Por medio del ejemplo no limitante, sistemas y métodos ejemplares para generar identificadores biométricos híbridos y realizar identificación/autenticación usando identificadores biométricos híbridos se describen en la Solicitud de Patente Estadounidense co-pendiente y comúnmente asignada Serie No. 62/156,645, titulada SISTEMA Y MÉTODO PARA GENERAR IDENTIFICADORES BIOMÉTRICOS HÍBRIDOS, presentada el 04 de Mayo de 2015.

Por medio del ejemplo adicional, además de caracterizar a un usuario generando vectores de característica de un dedo de conformidad con la rutina 300, como se describe anteriormente, las características biométricas adicionales pueden ser extraídas a partir de la(s) imagen(es) capturadas en la etapa 305, o información biométrica capturada separadamente. Tales características biométricas adicionales pueden incluir por medio del ejemplo y sin limitación, rasgos biométricos suaves y rasgos biométricos duros. Los rasgos “biométricos suaves” son características humanas físicas, de conducta o adheridas mientras las biométricas duras tales como, características de huella dactilar, iris, perioculares, y similares, son en general no variantes. Por medio del ejemplo adicional, rasgos biométricos suaves pueden incluir rasgos físicos tales como texturas de la piel, o colores de la piel. Las biométricas suaves pueden incluir también movimiento como se detecta por el giroscopio/acelerómetro del teléfono inteligente, características de movimiento del ojo como se detecta por algoritmos de seguimiento del ojo y características de movimiento

de la cabeza como se detecta por el seguimiento del movimiento de un rostro y/o cabeza. Tales características biométricas pueden ser extraídas y caracterizadas de conformidad con el método anterior así como también con algoritmos de análisis biométricos existentes. Además, las caracterizaciones adicionales de las características biométricas del usuario pueden ser codificadas como parte del identificador biométrico generado en la etapa 320, o de otro modo incluido en un identificador biométrico compuesto el cual incluye el identificador biométrico de huella dactilar, por ejemplo, fusionando identificadores biométricos múltiples.

En una o más modalidades ejemplares, la captura de imagen los dedos puede ser realizada a una distancia mayor que la típicamente realizada por un usuario usando dispositivo portátil tal como un teléfono inteligente. Las modalidades ejemplares pueden ser de maneras similar implementadas usando sistemas configurados para capturar las imágenes usando modalidades de adquisición de imagen de rango corto a rango largo posibles. La adquisición de imagen a una distancia puede ser realizada con modalidades ópticas tales como con sistemas de base óptica de varios tipos, por ejemplo, usando telefoto-lentes, así como también sistemas a base de enfoque láser, y sistemas a base de sonar. Las aplicaciones de estos tipos de modalidades de captura de imagen de rango más amplio pueden ser críticas en la aplicación de la ley, militar e inteligencia, y pueden finalmente ser desplegados en ambientes comerciales.

No obstante, la captura de imagen puede ser realizada mientras el sujeto no está estacionario, tales implementaciones son referidas en la presente como huella dactilar en los sistemas de movimiento (FOM). Este tipo de captura oportunística puede ocurrir concurrentemente con el tiempo conforme las huellas dactilares de la persona se vuelven visibles para operadores especiales encargados con este trabajo en convertir los modos de operación y/o supervivencia.

Para captura a una distancia pueden ser implementadas técnicas de súper resolución para incrementar la calidad de la huella usando datos a partir de marcos múltiples, y a regiones de paso parciales de la huella a partir de diferentes marcos en conjunto en una imagen de huella más grande. Por medio del ejemplo no limitante, los sistemas y métodos ejemplares para realizar técnicas de súper resolución para generar identificadores con base en capturas de imagen múltiple y realizar identificación/autenticación usando los mismos se describen en la presente y en la Solicitud de Patente Estadounidense co-pendiente y comúnmente asignada Serie No. 62/066,957 titulada SISTEMAS Y MÉTODOS PARA REALIZAR LA IDENTIFICACIÓN

Y VERIFICACIÓN DEL IRIS USANDO DISPOSITIVOS MÓVILES QUE UTILIZAN ILUMINACIÓN DE ESPECTRO VISIBLE, presentada el 15 de Octubre de 2014.

Además, se puede apreciar que los procedimientos anteriores para realizar adquisición de huella dactilar e identificación pueden realizar de manera similar usando imágenes capturadas en el espectro de luz NIR y luz RI, y usando dispositivos equipados con emisores de luz NIR y/o IR. Esta implementación puede ser especialmente útil para incorporar identificación de patrón de vena como un factor biométrico adicional. Por medio del ejemplo no limitante, los sistemas y métodos ejemplares para capturar imágenes biométricas en las bandas espectrales NIR e IR usando emisores de luz NIR e IR y realizando identificación/autenticación se describen en la presente y en la Solicitud de Patente Estadounidense co-pendiente y comúnmente asignada Serie No. 62/129,277, titulada "SISTEMAS Y MÉTODOS PARA REALIZAR LA IDENTIFICACIÓN Y VERIFICACIÓN DEL IRIS USANDO DISPOSITIVOS MÓVILES" presentada el 6 de Marzo de 2015.

La siguiente discusión describe procedimientos ejemplares para mejorar el desempeño de los sistemas de captura óptica de huella dactilar, de conformidad con una o más modalidades descritas de la invención, se describe en la presente en el contexto de dispositivos móviles con cámaras, y métodos para coincidir la salida de un sistema óptico sin contacto a huellas capturadas usando otros tipos de sensores, por ejemplo, aquellos capturados usando escáneres de contacto. Las imágenes capturadas usando un sistema óptico sin contacto (por ejemplo, una cámara) son referidas en la presente como "4F" o "imágenes 4F." Debido a que tales imágenes son capturadas usando un sistema óptico y sin contacto entre el dedo y el sensor/detector, son imágenes de un objeto tridimensional. Las imágenes capturadas usando escáneres de contacto tradicionales son referidas en la presente como "Plano" o "imágenes Planas". Debido a que tales "imágenes planas" son típicamente capturadas con el dedo contactando el escáner/sensor, las imágenes representan una superficie de dos dimensiones de un objeto.

Para mejorar el desempeño, se proporcionan en la presente métodos para optimizar la selección de detalles minuciosos de alta calidad, combinar clasificaciones de coincidencia a través de dedos múltiples y plantillas mientras se tiene en cuenta la variación en el desempeño de coincidencia de dedo individual (referido como fusión de clasificación), evitando los problemas de estimación de escala de huella dactilar/escala desconocida, y detalles de esquemas mejorados para el registro del usuario.

Para coincidir huellas capturadas con diferentes dispositivos, los sistemas y

métodos ejemplares resuelven los problemas de distorsión de huella. Cada técnica de captura introduce sus propios tipos de distorsión y por lo tanto degradan los desempeños de coincidencias. También se describen en la presente métodos para aplicar Redes Neurales Convolucionales en el dominio de coincidencia de huella dactilar el cual puede ser elaborado robusto para distorsión a través del proceso de entrenamiento y por lo tanto superan los emparejadores de huella dactilar tradicionales.

Además, descritos adicionalmente en la presente están métodos para detectar falsificaciones de presentación para captura óptica de huella con una cámara única por reconstrucción digital de la conformación 3D de los dedos a partir de imágenes múltiples. Esto es particularmente aplicable para captura en dispositivos móviles debido al hardware limitado disponible.

Fuente de Información de Selección de Detalles Minuciosos Ejemplares

Se extrajeron detalles minuciosos a partir de huellas ópticamente capturadas en ambientes no controlados y con hardware variante; iluminación, fondo y lentes. Como tal, las imágenes pueden contener características que son detectadas como puntos de detalles minuciosos los cuales son en efecto, artefactos de captura de huella óptica. Aunque los escáneres de cama plana sufren de problemas similares (suciedad, manchas, etc.), artefactos adicionales pueden ser causados por objetos de fondo, regiones de mal enfoque, marcas en los lentes, así como también otras características de la mano no capturadas normalmente en una captura escaneada. Por ejemplo, los márgenes de los dedos, claramente visibles en las fotografías, no están presentes en huellas escaneadas en cama plana, y pueden causar que detalles minuciosos falsos aparezcan donde terminan las crestas en los márgenes del dedo.

Los sistemas y métodos ejemplares emplean una serie de operaciones para seleccionar óptimamente contra los detalles minuciosos artificiales y/o de pobre calidad, mientras previenen la falla en ambientes imprevistos; para todavía seleccionar los mejores detalles minuciosos en casos donde un gran porcentaje puede ser considerado incorrectamente artificial/de pobre calidad.

Los detalles minuciosos detectados son clasificaciones de calidad que son impactadas por varios algoritmos de filtración. Los detalles minuciosos no son suprimidos, solamente ordenados en una lista de selección de conformidad con su calidad, a partir del cual los detalles minuciosos superiores, dado algún umbral, son seleccionados. Esto proporciona robustez en casos donde muchos detalles minuciosos pueden haber sido erróneamente descargados, mientras mantienen la

selección confiable de detalles minuciosos en casos típicos.

Clasificaciones de Calidad Inicial

Los algoritmos de extracción de detalles minuciosos, tales como aquellos que se incluyen en el emparejador Bozorth NIST, proporcionan típicamente una clasificación de calidad determinada por algoritmos que son diseñados para evaluar la calidad de una huella de contacto. Por ejemplo, determinando regiones donde la huella se ha manchado. Los mismos algoritmos aplican igualmente también a huellas ópticamente capturadas ya que regiones borrosas o lentes sucios pueden tener efectos similares en el contraste de la cresta. Como tal, los sistemas y métodos ejemplares usan la clasificación de calidad producida por los extractores de detalles minuciosos disponibles en el mercado como los sistemas de clasificación de calidad inicial para detalles minuciosos.

Filtración de Cadena de Detalles Minuciosos

La Figura 7A ilustra una imagen capturada 700 de dedos y puntos de detalles minuciosos correspondientes detectados sobre y entre los dedos de conformidad con al menos una modalidad descrita en la presente. Como se ilustra en la Figura 7A, numerosos puntos de detalles minuciosos pueden ser detectados sobre y alrededor de las puntas de los dedos. Los puntos de detalles minuciosos son ilustrados por un punto (por ejemplo, 702) que muestra la ubicación del detalle minucioso y una cola (por ejemplo, 704) orientada en la dirección de la característica del detalle minucioso. Como se muestra, por ejemplo, el detalle minucioso puede ser representado usando varios puntos que significan una clasificación de calidad correspondiente (es decir, un punto redondo 702 simboliza un punto de detalle minucioso de calidad superior, un punto cuadrado (no mostrado) simboliza la calidad mediocre y un punto de triángulo 706 simboliza el detalle minucioso de calidad más baja). La Figura 7A ilustra el detalle minucioso que es falsamente detectado entre los dedos 710 (falsamente detectado/puntos de detalle minucioso pobres ilustrados como un punto de triángulo). Usando el algoritmo detallado abajo, los sistemas pueden encontrar cadenas conectadas de puntos de detalle minucioso (por ejemplo, 712, 714) con base en las restricciones y suprimir sustancialmente los efectos de tales puntos de detalles minuciosos falsamente detectados, mayormente mejorando el desempeño y velocidad de los procesos de coincidencias. La alta confiabilidad de este método permite que todos los detalles minuciosos o inválidos sean movidos al fondo de la lista de selección ordenada por calidad multiplicando sus clasificaciones de calidad por cero.

El algoritmo para encontrar cadenas de detalles minuciosos falsos funciona

creando cadenas más largas dado ciertas restricciones. Específicamente, el sistema puede usar una técnica de extracción en forma de nivel donde inicialmente en un nivel, el sistema construye una subserie de cadenas de detalles minuciosos obteniendo todos los pares de puntos de detalles minuciosos y después removiendo pares de esta subserie si (i) el par tiene una distancia más grande de un umbral d y (ii) si la diferencia de ángulo entre las orientaciones de detalles minuciosos es más grande que el umbral θ . En el segundo nivel, y de manera similar para niveles futuros, el sistema construye cadenas más grandes fusionando cadenas más pequeñas. Es decir, si dos cadenas cada una tiene una longitud N puntos de detalles minuciosos y comparten $N - 1$ detalles minuciosos en sus cadenas, las dos cadenas son combinadas y fusionadas en una cadena $N + 1$ única. En niveles futuros, las cadenas de longitud $N + 1$ serán fusionadas para crear cadenas de longitud $N + 2$ y así sucesivamente. Las pruebas han mostrado que, en algunas implementaciones, correr el algoritmo hasta que se obtienen 5 cadenas de longitud puede ser suficiente y correr el algoritmo hasta para obtener cadenas más largas puede ser redundante. Sin embargo, en algunas implementaciones correr el algoritmo para obtener cadenas más largas puede ser benéfico.

Aumento de Detalles Minuciosos de Fondo

Los píxeles de imagen de fondo pueden a menudo, ser interpretados como detalles minuciosos de huellas dactilares, aunque típicamente el fondo no está en enfoque y los detalles minuciosos parecen ser de baja calidad. Sin embargo, tales detalles minuciosos pueden ser identificados segmentando el antecedente a partir del dedo en primer plano y disminuyendo la clasificación de calidad de los detalles minuciosos. Por ejemplo, una segmentación de umbral en el canal de luminancia de la imagen puede ser realizada, asumiendo que el dedo es altamente iluminado por la fuente de luz.

Un procedimiento más confiable, por ejemplo, es usar Modelos de Detección de Piel (previamente descritos). En particular, la implementación de un Modelo de Detección de Piel puede ser empleado para iluminar artificialmente los tonos de piel de la mano. El mismo modelo puede ser aplicado al segmento del dedo de primer plano.

En una de tal aplicación, el resultado del sistema de detección del dedo (por ejemplo, clasificadores en cascada) proporciona un ROI para cada dedo (regiones de interés/cuadros delimitadores). Una imagen de la punta del dedo se crea recortando la imagen original con el ROI apropiado. Una región cuadrada, central que cubre 20% de la imagen puede entonces ser seleccionada y un modelo computado. Esto genera el

modelo de piel inicial el cual se aplica en la primera iteración del algoritmo de detección. Esto funciona en la presunción que el sistema de detección del dedo identifica correctamente la ubicación del dedo, y el centro de la imagen casi ciertamente contiene solamente píxeles que representan la piel. El algoritmo de detección de piel entonces procede como se describe previamente, aplicando el modelo y actualizando el modelo en cada iteración.

En algunas implementaciones, el resultado es un mapa de probabilidad (mapa-p), donde los píxeles que representan la piel son evaluados cercanos a 1, mientras los píxeles del fondo son evaluados cercanos a cero. El mapa-p puede además requerir de umbral, por ejemplo, a 0,5 para crear un mapa binario.

Los detalles minuciosos que caen en regiones de fondo tienen sus valores de calidad multiplicados por un valor menor (por ejemplo, 0,01). Este procedimiento mantiene el orden de los detalles minuciosos en términos de calidad y también su posición arriba de aquellos determinados por ser parte de las cadenas (los cuales tienen valor de cero). En casos donde ocurren errores (por ejemplo, la imagen completa es erróneamente determinada por ser el fondo) la selección de detalles minuciosos no es afectada.

Finalmente, debido a que el umbral fijo puede ser no confiable, el sistema puede aplicar, por ejemplo, el método de umbral de Otus (como podría entenderse por aquellos en la técnica) para determinar dinámicamente el umbral dentro del histograma bimodal producido por el antecedente y la piel. Este algoritmo es robusto a casos donde, por ejemplo, solamente la piel está presente en la imagen.

Fuente de Información de Detalles Minuciosos

La Figura 7B representa una imagen capturada de los dedos y datos de imagen procesada a través de las etapas de una fuente de información ejemplar para selección de detalles minuciosos de conformidad con al menos una modalidad descrita en la presente. Una fuente de información ejemplar para selección de detalles minuciosos puede ser como sigue y se representa en la Figura 7B:

1. Un dedo recortado sufre mejoramiento de cresta y todos los detalles minuciosos posibles se extraen (los resultados se ilustran por la imagen 722).
2. Segmentación binaria usando una Modelo de Detección de Piel (resultados ilustrados por la imagen 724).
3. Los valores de calidad de detalles minuciosos en las regiones de fondo son reducidos (multiplicación por 0,01) (los resultados se ilustran por la imagen 726).
4. Filtración de cadena aplicada a todos los detalles minuciosos, las

clasificaciones de calidad se ajustan a cero (los resultados se ilustran por la imagen 728).

5. Parte superior 40%, en términos de clasificación de calidad, los detalles minuciosos son seleccionados para la plantilla (los resultados se ilustran por la imagen 724).

Método de Escalación Ejemplar

Como imágenes capturadas a partir del sistema de reconocimiento de huella dactilar 4F o el dispositivo de escaneo pueden estar a diferentes escalas, para incrementar el desempeño de coincidencia de las imágenes se llevan preferiblemente a una escala similar. Además se presentan aquí diferentes procedimientos para superar este problema.

Escalación de Costo Mínimo

Este procedimiento se dirige a minimizar la distancia entre los detalles minuciosos correspondientes correctos aplicando diferentes escalas y de este modo, minimizar los efectos de huellas de escala perdida. Encontrando la mejor escala con la clasificación de coincidencia más alto el sistema puede reducir los efectos de escala de huella en el proceso de coincidencias.

Por ejemplo la huella de prueba puede ser probada usando el sistema sobre un intervalo de escala de 80% hasta 120% en 10% de etapas, con la mejor clasificación de coincidencia tomada. Estos parámetros pueden ser ajustados dependiendo de factores tales como la tolerancia de escala del emparejador. También puede ser ventajoso escalar los ejes X y Y independientemente, especialmente cuando la coincidencia contra las huellas se toman con un escáner de contacto que puede haber sido estirada predominantemente en una dirección.

Escalación de Cresta

Alternativamente, la escalación de la imagen mejorada del dedo recortado se puede hacer utilizando las frecuencias de crestas locales de las imágenes de galería y prueba siendo coincidadas/comparadas (aplicables en escenarios: 4F contra 4F, o 4F contra Plano).

Las frecuencias de cresta local son la inversa de la distancia promedio entre crestas en el área local en una dirección perpendicular a la orientación local. Como podría entenderse por una persona de habilidad ordinaria en la técnica, existen varios métodos para determinar la frecuencia de la cresta. Por ejemplo, en algunas configuraciones, como un procedimiento descrito por Hong et al., (L. Hong, Y. Wan, y A. Jain. Fingerprint image enhancement: algorithm and performance evaluation. IEEE

Transactions on Pattern Analysis and Machine Intelligence, 20(8):777-789, Agosto 1998), se puede usar para encontrar las frecuencias de la cresta local de una imagen de la huella dactilar. Sin embargo, la frecuencia de cresta local puede variar a través de diferentes dedos, y también puede variar notablemente a través de diferentes regiones de la misma huella dactilar. Por lo tanto, puede ser preferible usar las frecuencias de cresta mediana a local de una imagen de dedo como la métrica a las imágenes a escala.

Asumiendo que la frecuencia mediana de la imagen de dedo de prueba es f_1 y la frecuencia mediana de la imagen del dedo de la galería es f_2 . Por ejemplo, para escalar la prueba con base en la información de la frecuencia, el factor de escala $S = f_2/f_1$. Usando este factor de escalación para escalar la anchura y altura de la imagen de prueba, la resolución de las crestas de la huella dactilar será mucho más cercana a la resolución de la imagen de la galería.

Este procedimiento puede ser extendido para normalizar la imagen del dedo de prueba sin la necesidad de la imagen de galería o calcular la frecuencia mediana si es la imagen de galería. En la literatura, se ha recomendado que una resolución de imagen de 500 puntos por pulgada (ppi), donde un punto es un píxel o un punto, son necesarios para para el procesamiento y coincidencia exitosa en la aplicación biométrica. En esta resolución, por ejemplo, la distancia entre las crestas adyacentes es aproximadamente 9 píxeles. Considerando 9 píxeles como la longitud de onda para adquirir una imagen de huella dactilar que tiene resolución de 500 ppi, el sistema puede escalar la imagen de huella dactilar de prueba con base en su frecuencia mediana. Por lo tanto, la normalización se puede hacer escalando la imagen de prueba con el factor de escalación de normalización, $NS = f_2 \cdot 9$. Con base en los resultados empíricos, se ha encontrado que algún tipo de huella dactilar (medio, anular, meñique) dará mejores resultados de coincidencia si la longitud de onda que se usa para normalización es 8 píxeles en lugar de 9 píxeles.

Proceso de Fusión de Clasificación Ejemplar

Después de obtener varias clasificaciones de coincidencia para cada huella dactilar, puede ser importante combinar estas clasificaciones para una mejor clasificación total para la mano como un todo. La siguiente discusión presenta varios procedimientos para combinar clasificaciones, sean entre dedos en una mano única o casos múltiples de la misma mano.

Clasificación de Fusión mediante Huellas Digitales Múltiples

Un procedimiento para determinar si un dedo único se iguala a otro es

determinar un umbral de corte, con base en las clasificaciones computadas a partir de los datos probados, lo cual proporciona una velocidad de aceptación falsa particular. Sin embargo, las investigaciones muestran que las distribuciones de coincidencias de impostor y genuinas difieren entre dedos, por lo tanto, para combinar los resultados de todos los cuatro dedos usando un umbral único pueden conducir a resultados disminuidos (por ejemplo, resultado de un ángulo de cámara, ángulo para iluminación, enfoque a través del ccd, etc.). Consecuentemente, combinar las clasificaciones a través de las huellas dactilares agregando clasificaciones en conjunto, puede en algunos casos, proporcionar resultados pobres.

Un método ejemplar para resolver este problema es deducir los modelos de probabilidad para cada dedo independientemente, y después combinar de manera probable estas clasificaciones en una probabilidad de una coincidencia de mano única. Por lo tanto, usando las probabilidades, el sistema puede combinar teóricamente de manera precisa los resultados de coincidencia a partir de dedos individuales que representan diferentes distribuciones.

Por ejemplo, esto se puede hacer ajustando las distribuciones de probabilidad (por ejemplo, distribuciones gamma), para cada dedo, para tanto distribuciones de clasificación impostoras como genuinas. Este procedimiento se basa en la prueba del índice de probabilidad y requiere estimación explícita de densidades de clasificación coincidentes genuinas e impostoras. El procedimiento a base de densidad tiene la ventaja de que logra directamente desempeño óptimo en cualquier punto de operación deseado (FAR), siempre que las densidades de clasificación sean precisamente estimadas.

La probabilidad de una clasificación dada de que un usuario es genuino ($P(S | G)$) puede ser determinada usando la curva ajustada como una probabilidad de función de densidad, ya que puede estar la probabilidad de la clasificación dada de que el usuario es un impostor ($P(S | I)$). En el caso simple, la probabilidad de que un dedo único es genuino dada la clasificación de coincidencia ($P(G | S)$) puede ser computada usando el Teorema de Bayes como:

$$P(G | S) = \frac{P(S | G) \cdot P(G)}{P(S)}$$

donde $P(G)$ es la probabilidad del usuario de ser genuino, estimado a 0,5 (esto podría ser determinado a partir de datos si están disponibles), $P(S)$ es la probabilidad de la clasificación con respecto de ser genuino o un impostor:

$$P(S) = P(S|G=0) \cdot P(G=0) + P(S|G=1) \cdot P(G=1).$$

Para computar la probabilidad de la mano completa de ser genuina el sistema puede aplicar el producto a través de los cuatro dedos:

$$P(G|S) = \frac{\prod_{i=1}^4 P(S_i|G) \cdot P(G)}{\prod_{i=1}^4 P(S_i)},$$

Se observa que cuando se computa en un procesador, es necesario salvaguardar contra la inestabilidad numérica cuando las probabilidades son muy pequeñas. Esto se puede hacer, por ejemplo, por computación en espacios logarítmicos.

Fusión de Clasificación mediante Plantillas Múltiples

En este procedimiento, se usaron plantillas múltiples para el registro y/o la verificación. Coincidiendo todas (o una subserie de) las combinaciones de registro y plantillas de verificación, se mejoró la capacidad del sistema para discernir al genuino del impostor. El uso de múltiples plantillas minimiza tanto el impacto de regiones de calidad pobre que pueden residir dentro de una plantilla múltiple y cubre mejor las fuentes de variación (por ejemplo, ángulo de captura) que puede resultar en mejor/peor captura de regiones dentro de un dedo.

Como un ejemplo, el sistema puede capturar tres plantillas de registro; es decir, tres imágenes de la mano de un usuario, extrayendo cuatro plantillas de dedo por mano, totalizando 12 plantillas por dedo. Para autenticar, una plantilla de verificación única puede ser usada (4 plantillas de dedo). Para cada dedo, el sistema realiza tres coincidencias, las clasificaciones las cuales pueden ser combinadas. La combinación de clasificaciones podría tomar cualquier forma, por ejemplo, sumación, mediana, o mediante procedimientos de probabilidad (Fusión de Clasificación mediante Huellas Dactilares Múltiples).

Esquema de Plantillas Múltiples - Captura en Registro

Capturar plantillas múltiples en el registro incrementa el tiempo requerido por el usuario para completar el registro pero proporciona dos beneficios importantes. En primer lugar, se requiere la verificación del usuario para capturar solamente una plantilla única, lo cual es rápido. En segundo lugar, el sistema puede procesar las plantillas de registro para evaluar la adecuabilidad del usuario por cruza de coincidencia de las plantillas. Esto permite rechazo temprano de aquellas personas con huellas degradadas o intentos para registrar los objetos arbitrarios. Esto ayuda a

mitigar los huecos de seguridad durante la verificación debido a registros de pobre calidad.

Método Ejemplar de Detección de Vida a Base de Dedos

Un método para determinar la diferencia entre la mano real y de falsificación es para comprobar que la forma tri-dimensional (3D) de la mano o dedos es como se esperaba, y/o noes como podría esperarse para una falsificación.

En una modalidad ejemplar, dos imágenes del(los) dedo(s) del usuario pueden tomarse a partir de diferentes ángulos, la forma de los dedos se deduce y se hace una métrica con relación a la cercanía de ajuste a un dedo real. Si la forma es bastante cercana a la forma esperada a partir de un dedo real entonces se pasa la prueba de vida.

Dos imágenes podrían ser recolectadas a partir del usuario desplegando primero una guía de mano en la pantalla en una ubicación. Después que el usuario ha posicionado su mano en la guía se toma una imagen, la guía es entonces movida a otra ubicación fomentan animando al usuario a mover su mano a una nueva ubicación. Cuando el usuario ha movido su mano a la nueva ubicación se captura la segunda imagen. Más de dos (2) imágenes podrían ser usadas para construir un modelo 3D más robusto de la mano. Un método computacionalmente eficiente para generar un modelo 3D de la mano es recolectar dos (2) imágenes del dedo a partir de ubicaciones horizontalmente desplazadas, después realizar coincidencias de correspondencia para crear un mapa profundo como es bien sabido en la técnica previa.

La Figura 8A representa (a) Dos imágenes de dedos recolectadas a partir del usuario en diferentes ubicaciones (cambio a lo largo del dedo); (b) y (c) Mapas de borde vertical y horizontal son generados para alinear dedos correspondientes; (d) Recortar y mejorar los dedos medios a partir de las dos imágenes.

Las coincidencias de correspondencia se pueden hacer más eficientes si estas dos imágenes de dedos son rotacionalmente y verticalmente alineadas, y son idénticamente escaladas. Esta alineación puede llevarse a cabo localizando las líneas sombreadas entre los dedos, y rotándolas hasta que son horizontales. La alineación vertical se puede llevar a cabo localizando y alineando las puntas de los dedos. La escalación podría llevarse a cabo normalizando la distancia entre las líneas sombreadas entre cada dedo. Después de la alineación apropiada, las imágenes del dedo son recortadas y mejoradas usando algoritmo de ecualización de histograma.

El mapa de disparidad entre dos imágenes de dedo puede ser computado de píxel por píxel usando técnicas de mapeado de bloque. Solamente las disparidades a

lo largo de la detección del dedo son usadas para la detección de vida. El mapa es entonces ajustado usando modelo de superficie polinomial de segundo orden para reducir los ruidos. La Figura 8B muestra los mapas de disparidad de un dedo real (800a) y una fotografía 2D (800b). Debido a la propiedad 3D del dedo, una superficie curvada puede verse en la dirección perpendicular al dedo en el mapa de disparidad 800a. Por el contrario, el mapa de disparidad 800b a partir de la fotografía de falsificación es mucho más plano puesto que todos los puntos son de superficie 2D. Las curvaturas de cada una de las líneas verticales son entonces calculadas y usadas para determinar la vida y la decisión final de vida se hace comprobando la vida de cada dedo. La Figura 8C ilustra los datos de mapa de disparidad (puntos, 810) y una superficie matemáticamente ajustada 815 para un dedo real (800c) y la Figura 8D ilustra los datos de mapa de disparidad (puntos, 820) y una superficie matemáticamente ajustada 835 para una fotografía de falsificación 2D (800d).

Método Ejemplar de Corrección de Distorsión

Varios procedimientos han sido aplicados para resolver el desafío de coincidencias de huellas dactilares en imágenes distorsionadas. Esta distorsión cambia las relaciones espaciales entre los detalles minuciosos de las huellas dactilares y previene a los emparejadores de huellas dactilares encontrar una coincidencia correcta. Mientras procedimientos previos han sido algo exitosos, se han enfocado principalmente en la coincidencia de huellas dactilares obtenidas a partir del mismo sensor. No obstante las distorsiones con las que se enfrentan se originan principalmente de los artefactos en la imagen.

Los sistemas y métodos ejemplares descritos en la presente se dirigen a resolver este problema en un nivel más desafiante. En primer lugar, además de un dispositivo de captura único, el sistema está configurado para hacer intentos adicionales para coincidir huellas dactilares obtenidas a partir de dos diferentes técnicas de captación de imagen. Específicamente, por ejemplo, la primera técnica captura imágenes de los dedos usando una cámara en un dispositivo de teléfono móvil para verificación mientras la segunda también puede usar un dispositivo de escaneo de huella dactilar en lugar de la cámara para registro. En segundo lugar, los tipos de distorsión introducidos por estos dispositivos varían significativamente e introducen nuevos problemas en las coincidencias.

Mientras ambas técnicas de captura de imagen mencionadas anteriormente incluyen distorsiones, cada técnica también introduce sus propios tipos de distorsión, de este modo introduciendo nuevos desafíos.

En una imagen capturada con un teléfono móvil usando tecnología de reconocimiento de dedo sin contacto ejemplar descrita en la presente, el centro de la imagen puede ser menos distorsionada mientras la región más externa del dedo puede ser más altamente distorsionada. Esto surge debido a la curvatura de los dedos donde la distorsión más alta viene de la región entre la curvatura más alta, es decir, el margen de los dedos.

En una imagen obtenida a partir del escáner de cama plana, en adelante referida como Plana, mientras todavía existe poca o ninguna distorsión de curvatura, existen sin embargo, distorsiones locales en diferentes partes de la huella dactilar. Esto es debido a diferentes puntos de presión siendo aplicados por el dedo en la superficie del escáner. No obstante, estas distorsiones locales pueden variar significativamente a través de la huella dactilar.

En el caso de coincidencias usando un tipo de sensor único tanto el registro como verificación de huellas dactilares son del mismo tipo de distorsión. Sin embargo, en el caso de diferentes dispositivos de captura, las imágenes registradas pueden ser de, es decir, un escáner y las imágenes de verificación pueden ser de una cámara móvil (por ejemplo, “4F” o “Imágenes 4F”). Por lo tanto el proceso de coincidencia es configurado para intentar encontrar coincidencias correctas entre diferentes tipos de distorsiones.

Mientras las técnicas mencionadas anteriormente descritas pueden ser usadas para ayudar a abordar la imagen del dedo para un problema de coincidencia Planta, la siguiente discusión se dirige a, entre otros, resolver este problema y puede mejorar el desempeño del sistema de reconocimiento de dedo significativamente.

Modelación de Distorsión Usando Ranuras de Placa Delgada

Como podría entenderse por una persona de habilidad ordinaria en la técnica, existen varios métodos para modelación de distorsión. Por ejemplo, en algunas configuraciones, un procedimiento descrito por Ross y Nadgir (Ross A. y Nadgir R., “A thin-plate spline calibration model For fingerprint sensor interoperability,” IEEE Transaction Data and Knowledge Engineering, vol. 20, no. 8, pp. 1097-1110, 2008.), un mapeo entre los dos tipos de distorsión usando una ranura de placa delgada puede ser moldeado. Aplicando este modelo sobre los detalles minuciosos obtenidos a partir de una imagen de teléfono móvil, el sistema puede ser configurado para mapearlo sobre sus detalles minuciosos correspondientes correctos sobre la imagen de la superficie y usarlas para verificación. Esto permite al emparejador encontrar coincidencias más correspondientes entre los dos tipos de imagen.

Emparejador Robusto de Distorsión

Los procedimientos previos son típicamente aplicados ya sea antes o después del proceso de coincidencia. Aplicando este procedimiento emparejador robusto de distorsión, sin embargo, los parámetros en el emparejador pueden ser ajustados para permitir niveles de distorsión superior. Esto permite las coincidencias correctas que sufren grados de distorsión superior que serán coincidentes, resultando en coincidencias más correctas.

Corrección de Distorsión Usando Dispositivo de Escaneo:

En este procedimiento los sistemas y métodos ejemplares son configurados de manera que el problema de distorsión se resuelve en la etapa de captura de imagen. Usando un escáner, simultáneamente mientras captura una huella dactilar, el sistema almacena la presión aplicada por el dedo de la persona en términos de su dirección y magnitud. Esto resulta en vectores a través del dedo y aplicándolo sobre la imagen y sus detalles minuciosos, el sistema puede de este modo difundirse y remapear cualquier distorsión causada como un resultado de la presión.

Método Ejemplar de Coincidencia de Huella Digital usando CNNs

Como una alternativa a usar extractores y emparejadores a base de detalles minuciosos, las Redes Neurales Convolucionales (CNNs) también pueden ser aplicadas usando el sistema para coincidir una huella digital de verificación con una imagen registrada. Varias redes tales como “GoogleNet” o “AlexNet” existentes pueden ser usadas para el proceso de entrenamiento. Cada serie de datos con las cuales el sistema se entrena o puede consistir de imágenes de los siguientes tipos:

1) Imágenes RGB: Estos tipos de imágenes son las huellas dactilares recortadas de los 4 dedos o imágenes de la palma

2) Escala de grises: Imágenes de RGB convertidas a escala de grises.

3) Imágenes de cresta mejoradas: Se usó la imagen a escala de grises y se realizaron mejoramientos usando la técnica de mejoramiento de huella dactilar resumida en la patente previa.

4) Imágenes de cresta: Se realizó creación de cresta en imágenes mejoradas donde se buscó para, y se crearon crestas a partir de una imagen de huella dactilar. Esto produce una imagen binaria de las crestas de huellas dactilares.

5) Imágenes de cresta mejoradas combinadas: Se combinaron las imágenes de cresta mejoradas para maximizar la información útil a partir de las imágenes mejoradas.

Las siguientes Modalidades describen diferentes procedimientos usando CNNs

para realizar coincidencias de huellas dactilares en la imagen de dedo(s) (4F) a 4F o 4F a aplicaciones Planas.

Modalidad A

Las CNNs pueden ser usadas como parte de un proceso de coincidencia de huella dactilar. Este procedimiento involucra entrenar una CNN donde cada dedo de la persona es una clase. El entrenamiento puede incluir varios casos de las huellas dactilares de la persona y las pruebas/coincidencias se realizarán en un caso no visto de una persona vista previamente. Por lo tanto, usando este procedimiento una huella dactilar de prueba será clasificada para una persona previamente vista.

Modalidad B

El sistema también puede usar el modelo previo para identificar y verificar una persona previamente no vista. En este procedimiento una nueva persona obtendrá un vector de probabilidades donde cada valor en este vector representa que tan similar es una persona a una persona particular. Este vector puede ser usado para representar la persona en identificación y verificación.

Modalidad C

En el caso previo, el modelo ha sido entrenado para un número fijo de personas. Mientras este proporciona alto desempeño de clasificación para personas previamente vistas, si una nueva persona necesita ser autenticada, la CNN puede no ser capaz de representarla completamente. Para cambiar las características de la CNN a partir de las características específicas de la persona para características de huellas dactilares genéricas, un proceso de entrenamiento de dos etapas puede ser usado. El primero involucra entrenar una CNN similar a la clasificación de un caso a muchos. Sin embargo, una segunda fase de entrenamiento se realiza con base en el aprendizaje de similitud el cual continúa el entrenamiento del modelo de clasificación. Este nuevo modelo puede ser usado en personas no vistas previamente que no estuvieron presentes en la etapa de clasificación.

Por ejemplo, aplicando la CNN con el modelo de aprendizaje de similitud entrenada, se puede obtener un vector de característica para tanto una huella dactilar de verificación previamente no vista y una huella dactilar registrada. Comparando las dos huellas dactilares se puede realizar verificación donde las más similares son las más probables que sean una coincidencia correcta. Por lo tanto, este procedimiento puede ser usado para cualquier persona nueva donde gustaría registrar y autenticar.

Modalidad D

Las CNNs también pueden ser usadas para el propósito de identificación a

gran escala. Por ejemplo, el procedimiento previo puede ser aplicado para realizar identificación en uno a muchos casos. Aquí, se obtienen los vectores para todas las personas que se desean identificar. Dada una nueva serie de huellas dactilares, se puede obtener un vector para representar las huellas dactilares de una nueva persona. Comparando este vector contra todos los vectores de otras personas y obtener una medida de similitud (tal como distancia euclidiana) para cada comparación, el par con la similitud más alta puede ser identificado. En este caso, la persona será identificada conforme la persona obtiene la similitud más alta.

Modalidad E

Para aplicar las CNNs al escenario 4F a Plano, además de los procedimientos previos, se pueden colocar imágenes de tanto ejemplos de 4F a Plano en conjunto dentro de los datos de entrenamiento, dado que son el mismo tipo de imágenes, por ejemplo, imágenes de cresta mejorada combinadas. Esto permitirá a la CNN aprender características comunes entre ambos tipos de huellas dactilares.

Modalidad F

Otro procedimiento al escenario 4F a Plano es para entrenar modelos individuales para imágenes 4F a Planas, volviendo a entrenar cada modelo usando aprendizaje de similitud y después encontrando un mapeo entre los vectores 4F a Plano. Este mapeo puede entonces ser usado para predecir vectores genuinos o impostores en las coincidencias.

Huellas Digitales 4F a Convertidor Plano

Para mejorar el desempeño de coincidencia de una verificación de imagen 4F contra una imagen Plana registrada, una CNN puede ser usada para convertir la imagen de verificación 4F a una imagen de verificación Plana. Esto permitirá al sistema coincidir una imagen Plana de verificación convertida contra una imagen Plana registrada. Por ejemplo, los métodos propuestos por Gatys et al. (Leon A. Gatys, Alexander S. Ecker, Matthias Bethge; The IEEE Conference on Computer Vision and Pattern Recognition (CVPR), 2016, pp. 2414-2423) pueden ser usados para transformar una imagen a otro estilo. En este caso el sistema puede hacer una transformación de imagen 4F y parecer como una imagen Plana.

Extracción de Detalles Minuciosos de CNN y Filtración

Las CNNs también pueden ser usadas para detectar ciertos patrones dentro de las huellas dactilares. Entrenando una CNN, el sistema puede detectar y extraer detalles minuciosos. Esto puede involucrar entrenamiento en parches de imágenes de huella dactilar que contienen una variedad de tipos de detalles minuciosos, sus

diferentes rotaciones, escalas, y ubicaciones de centro de traslación. Adicionalmente, se puede usar un procedimiento similar para filtrar parches de detalles minuciosos que obtienen una baja clasificación como un resultado de aplicar el modelo entrenado.

Clasificador de Tipo Huella Dactilar de CNN

Usando este procedimiento el sistema puede clasificar el tipo de huella dactilar (espiral, arco, etc.) y usar esta información para evitar huellas dactilares incompatibles coincidentes. El sistema puede realizar esto creando una base de datos donde cada pliego representará una clase de un tipo de huella dactilar. Entrenando la CNN, el sistema puede aprender que cada huella dactilar se parece y aplicando el modelo en una huella dactilar de prueba el sistema puede predecir su clase de tipo de huella dactilar.

Clasificación Borrosa a Base de CNN

Las CNNs también pueden ser entrenadas y utilizadas para determinar si una imagen no está dentro de los estándares de calidad requeridos por un sistema. Un ejemplo es detectar automáticamente imágenes borrosas y no utilizables que pueden ser capturadas usando el sistema 4F. La CNN se clasificará con base en dos clases es decir, Nítida y Borrosa. Si una imagen es clasificada como Borrosa y considerada no utilizable, el sistema 4F requerirá otra captura de imagen a partir del usuario. Esto podría requerir entrenar una CNN en una serie de datos que consisten de dos pliegues cada uno que representa clases Borrosas y Nítidas, donde en cada pliegue las imágenes que representan cada clase estarán presentes.

Detección de vida por CNN

Una red de CNN puede ser entrenada para detectar y distinguir entre imágenes falsificadas y genuinas. En este procedimiento, una red es entrenada en una serie de datos que consisten de dos tipos de imágenes (i) genuina, la cual puede ser capturada usando cualquier técnica y (ii) falsificada, la cual puede consistir de imágenes tomadas a partir de una variedad de ataques de presentación. Esto puede requerir entrenar una CNN en una serie de datos que consisten de dos pliegues cada uno que representa clases genuinas y falsificadas, donde en cada pliegue las imágenes que representan cada clase, estarán presentes.

Encontrar Umbral Óptimo

Usando las CNNs el sistema puede separar clasificaciones genuinas e impostoras usando un hiperplano en lugar de un umbral fijo. En el caso de CNN en lugar de tomar la suma de distancias euclidianas, el sistema puede realizar una sustracción en forma de elemento y después alimentar los vectores genuinos e

impostores a un algoritmo de aprendizaje de máquina (por ejemplo, SVM) para ajustar un hiperplano en lugar de uno fijo a un umbral de una dimensión. En esta forma, cada característica en el vector de características es preservado, distinto antes donde fueron combinadas todas en una clasificación única. Adicionalmente, como es posible para algunas características ser menos discriminativas, el algoritmo de aprendizaje de máquina puede dar más atención a las características más discriminantes.

Expansión de Serie de Datos de CNN

Las CNNs dependen de series de datos grandes para obtener modelos confiables. Las series de datos pueden ser expandidas modificando casos existentes en las series de datos para generar las nuevas. Estas modificaciones pueden incluir, rotar, trasladar, escalar, recortar, cambiar la relación de aspecto o el espacio de color de las imágenes. En un procedimiento ejemplar, como se ilustra en la Figura 9, numerosos casos de solamente una huella dactilar única se pueden obtener rotando, escalando y cambiando la relación de aspecto. La Figura 9 ilustra tales series de datos expandidos con base en las modificaciones de la huella dactilar.

Clasificadores de Rostro Individual a Base de CNN

Para el propósito de reconocimiento facial, mientras tradicionalmente las CNNs son entrenadas en imágenes de rostro completo, el sistema también puede entrenar CNNs individuales en regiones particulares del rostro, y después combinar todas las clasificaciones a partir de cada modelo. Por ejemplo, diferentes CNNs pueden ser entrenadas para párpados, ojos, boca, nariz, etc. Cuando se realiza reconocimiento, el sistema puede correr cada modelo separadamente en una imagen de prueba donde obtiene clasificaciones y/o vectores de cada modelo. El sistema puede entonces combinar las clasificaciones y vectores para obtener la clasificación de reconocimiento final.

Proceso de Registro Óptimo Ejemplar

Tener una buena etapa de registro es de alta importancia para el desempeño de autenticación. La siguiente discusión describe procedimientos para asegurar que los datos reunidos durante el registro son óptimos.

Maximizar Variación de Plantilla

Un método para mejorar la calidad del registro es capturar plantillas múltiples. Los mejoramientos de usar plantillas múltiples se originan a partir de las plantillas que contienen variación. Si todas las plantillas son idénticas, aún si son de alta calidad, el desempeño podría no incrementar. Por lo tanto, maximizar la variación conduce a desempeño mejorado ya que existe una mayor probabilidad de que tanto el registro

como representaciones de verificación ambas contengan las mismas características.

Existen tres fuentes prominentes de variación cuando se capturan imágenes usando cámaras de dispositivo móvil; iluminación/ambiente, ángulo/posición de la mano durante la captura, cómo el usuario mantiene juntos sus dedos (esto oscurece ciertas regiones de la huella cuando se hace). Como un ejemplo, un esquema de registro que alienta al usuario a remover su mano de la visión de la cámara entre capturas, capturará más de la variación descrita previamente que tomar simplemente imágenes consecutivas, rápidas.

Un procedimiento más sofisticado que puede ser implementado por el sistema en combinación con el anterior, es usar plantillas a partir de intentos de autenticación exitosos, con la presunción de que el usuario es autenticado en muchos ambientes diferentes. Por ejemplo, un procedimiento básico podría ser capturar dos plantillas en el registro y agregar una tercera plantilla cuando el primer usuario se autentifica (preferiblemente se toma cuidado para parametrizar el sistema correctamente para coincidir 1, 2 o 3 plantillas). Sin embargo, este procedimiento puede ser además extendido, para actualizar continuamente las plantillas registradas con mayor variación con el beneficio agregado de adaptarlo a las huellas que cambian de un usuario sobre periodos de tiempo prolongados.

Como se describe previamente el ángulo de incidencia de la fuente de iluminación (típicamente el destello LED de la fuente del punto) y las crestas de las huellas, tienen un efecto significativo en el contraste de la cresta. Notablemente, por ejemplo, el dedo meñique es típicamente menos iluminado que los dedos medios o índice, pero posicionando la mano superior puede remediar esto. Como tal, es benéfico para el usuario colocar su mano en varias posiciones con relación a la iluminación.

Uno de tal esquema de registro implementado usando el sistema podría ser como sigue: El usuario es requerido para capturar dos imágenes de su mano. Para la primera imagen en la guía de mano de la pantalla es posicionada fuera del centro hacia la parte superior de la pantalla, y la retroalimentación en tiempo real a partir del seguimiento del dedo dirige al usuario a colocar su mano en esta posición ligeramente elevada. El usuario remueve su mano y es este consultado para verificar la primera imagen de registro. Para esta segunda captura la guía de mano es posicionada fuera del centro hacia el fondo de la pantalla. Esto ayuda a la variación de posición requerida al registro. Para desempeño adicional, un modelo de probabilidades puede ser independientemente computado para estas diferentes posiciones, cada una

codificando la forma óptima para combinar las clasificaciones de coincidencias a partir de diferentes dedos cuando la mano del usuario está en ubicaciones no específicas. Esto es, por supuesto, no limitado a dos posiciones y puede extenderse en un arreglo completo de 2D de posiciones de las manos.

Captura de Datos de Vistas múltiples

Cuando se captura una imagen 4F de una mano colocada en el centro de la imagen, ciertas áreas de los dedos pueden no proporcionar tanta información de detalles minuciosos debido a la borrosidad del enfoque y la carencia de luz que golpea ciertas regiones. Este es particularmente el caso para el dedo meñique. Para evitar estos problemas el sistema puede implementar una técnica de “vista múltiple” donde, en lugar de capturar tres imágenes de las manos registradas todas en la posición central, el sistema es configurado para capturar la mano en diferentes ubicaciones es decir, centro, izquierda y derecha como se ilustra en la Figura 10, lo cual representa imágenes del “centro”, “izquierda”, y “derecha” capturadas en la etapa de registro para maximizar los datos de detalles minuciosos a partir de cada huella digital.

Este procedimiento ayuda a asegurar que cada dedo ha sido visto limpiamente en al menos una imagen y ha sido capturado en la calidad más alta para extracción de detalles minuciosos. Haciendo coincidir una imagen de verificación contra cada una de las tres imágenes de vista múltiple, se pueden obtener tres series de clasificaciones de huellas dactilares y cuando el valor máximo para cada dedo (o cualquier otra técnica de fusión de clasificación) se usa, una clasificación más confiable para cada dedo se puede obtener puesto que el sistema posee una representación mucho mejor de cada dedo a partir de imágenes de múltiples vistas.

Si el sistema es configurado para usar un registro estándar o vista múltiple, este procedimiento combina información de detalles minuciosos para cada dedo a través de las tres imágenes de registro para encontrar una plantilla óptima. Esto se puede hacer mediante:

1. Ordenar las diferentes plantillas con base en su calidad o coincidiéndolas entre sí y determinando la proporcionada a la clasificación de coincidencia más alta con otras plantillas.
2. Alinear la segunda mejor plantilla (plantilla de registro) con la primera (plantilla de referencia) utilizando punto más cercano iterativo para encontrar los detalles minuciosos correspondientes y después usar ranura tardía delgada para registrarlos.
3. Fusionar las dos plantillas usando un cuadro limítrofe para encontrar detalles

minuciosos que son muy cercanos entre sí y elegir una de las mejores plantillas (la plantilla de referencia) para ser mantenidos y la calidad de medición de los detalles minuciosos mantenidos puede ser actualizada para reflejar su consistencia.

4. La etapa 2 y 3 puede ser repetida hasta que todas las plantillas son fusionadas.

En esta coyuntura, se debe notar que aunque mucha de la descripción anterior se ha dirigido a sistemas y métodos para autenticar a un usuario de conformidad con las características biométricas del usuario que son capturadas usando dispositivos de teléfonos inteligentes convencionales, los sistemas y métodos descritos en la presente pueden ser de manera similar desplegados y/o implementados en escenarios, situaciones, y ajustes más allá de los escenarios referenciados.

Mientras esta especificación contiene muchos detalles de implementación específicos, estos no deben ser construidos como limitaciones en el alcance de cualquier implementación o de lo que puede ser reivindicado, sino preferiblemente como descripciones de características que pueden ser específicas a modalidades particulares de implementaciones particulares. Ciertas características que son descritas en esta especificación en el contexto de modalidades separadas también pueden ser implementadas en combinación en una modalidad única. Contrariamente, varias características que son descritas en el contexto de una modalidad única también pueden ser implementadas en modalidades múltiples separadamente o en cualquier subcombinación adecuada. No obstante, aunque las características pueden ser descritas anteriormente como actuando en ciertas combinaciones y aún inicialmente reivindicadas como tales, una o más características a partir de una combinación reivindicada pueden en algunos casos, ser escindidas de la combinación, y la combinación reivindicada puede ser dirigida a una subcombinación o variación de una subcombinación.

De manera similar, mientras las operaciones son representadas en los dibujos en un orden particular, este no debe ser entendido como que requiere que tales operaciones sean realizadas en el orden particular mostrado en orden secuencial, o que todas las operaciones sean realizadas, para lograr resultados deseables. En ciertas circunstancias, las multitareas y procesamiento paralelo pueden ser ventajosos. No obstante, la separación de varios componentes del sistema en las modalidades descritas anteriormente no debe ser entendido como que requiere tal separación en todas las modalidades, y se debe entender que los componentes y sistemas del programa descrito pueden en general, ser integrados en conjunto en un producto de

software único o empacado en productos de software múltiples.

La terminología usada en la presente es para el propósito de describir modalidades particulares solamente y no se pretende ser limitante de la invención. Como se usa en la presente, las formas singulares “un”, “uno”, y “el”, están propuestos para incluir las formas plurales así también, a menos que el contexto lo dicte claramente de otro modo. Se entenderá además, que los términos “comprende” y/o “que comprende”, cuando se usa en esta especificación, especifica la presencia de características declaradas, enteros, etapas, operaciones, elementos, y/o componentes, pero no evita la presencia o adición de una o más de otras características, enteros, etapas, operaciones, elementos, componentes, y/o grupos de los mismos. Se debe notar que el uso de términos ordinales tales como “primero”, “segundo”, “tercera”, etc., en las reivindicaciones para modificar un elemento reivindicado no por sí mismo connota cualquier prioridad, precedencia, o se realizan en el orden de un elemento reivindicado sobre otro o en el orden temporal en el cual actúa de un método, pero son usados solamente como etiquetas para distinguir un elemento de reivindicación que tiene un cierto nombre a partir de otro elemento que tiene un mismo nombre (pero para uso del término ordinal) para distinguir los elementos reivindicados. También, la fraseología y terminología usadas en la presente son para el propósito de descripción y no deben ser considerados como limitantes. El uso de “que incluye”, “que comprende”, o “que tiene”, “que contiene”, “que involucra”, y variaciones de los mismos, está significando abarcar los puntos listados posteriormente y equivalentes de los mismos así como también puntos adicionales. Se entiende que números similares en los dibujos representan elementos similares a través de las varias figuras, y que no todos los componentes y/o etapas descritas e ilustradas con referencia a las figuras son requeridos para todas las modalidades o arreglos.

De este modo, modalidades y arreglos ilustrativos de los presentes sistemas y métodos proporcionan un método implementado por computadora, sistema de computadora, y producto de programa de computadora para autenticar a un usuario de conformidad con las biométricas del usuario. Los diagramas de bloque y diagramas de flujo en las figuras ilustran la arquitectura, funcionalidad, y operación de implementaciones posibles de sistemas, métodos y productos de programa de computadora de conformidad con varias modalidades y arreglos. En este sentido, cada bloque en el diagrama de bloque o diagrama de flujo puede representar un módulo, segmento, o porción de código, el cual comprende una o más instrucciones

ejecutables para implementar la(s) función(es) lógica(s) especificadas. Se debe notar también que, en algunas implementaciones alternativas, las funciones indicadas en el bloque pueden ocurrir fuera del orden indicado en las figuras. Por ejemplo, dos bloques mostrados en sucesión pueden, en efecto, ser ejecutados substancialmente concurrentemente, o los bloques pueden algunas veces ser ejecutados en el orden inverso, dependiendo de la funcionalidad involucrada. También se notará que cada bloque de los diagramas de bloque y/o ilustración de diagrama de flujo, y combinaciones de bloques en los diagramas de bloque y/o ilustraciones de diagrama de flujo, pueden ser implementados por sistemas a base de hardware con propósito especial que realiza las funciones o actos especificados, o combinaciones de hardware de propósito especial e instrucciones por computadora.

La materia objeto descrita anteriormente se proporciona por medio de ilustración solamente y no debe ser construida como limitante. Varias modificaciones y cambios pueden hacerse para la materia objeto descrita en la presente sin seguir las modalidades ejemplares y aplicaciones ilustradas y descritas, y sin apartarse a partir del espíritu verdadero y alcance de la presente invención, el cual se expone en las siguientes reivindicaciones.