DOCUMENTOS INFORMATIVOS

¿Qué es la biometría?

AWARE

¿Qué es la biometría?

Los datos biométricos se refieren a las características físicas (y conductuales) más propias de cada uno, que pueden ser detectadas por dispositivos e interpretadas por computadoras de modo que puedan usarse como nuestros representantes en el ámbito digital. De este modo podemos vincular nuestros datos digitales y nuestra identidad de forma permanente, consistente y sin ambigüedad y recuperarlos rápida y automáticamente recurriendo a las computadoras.

Identidad y confianza

En cada uno de nosotros existe un sinnúmero de elementos que, tomados en conjunto, nos hace únicos, por ejemplo, los atributos físicos, el lugar donde vivimos, la fecha en que nacimos, las relaciones que mantenemos y las cosas que sabemos. La singularidad de nuestro aspecto físico y de nuestra historia personal está representada por lo que comúnmente denominamos nuestra "identidad". En el entorno actual totalmente interconectado y dominado por las computadoras, cada vez es más conveniente 1) atribuir correctamente la información digital a una persona y 2) certificar nuestra identidad de un modo que sea confiable y fácil de comunicar. Podría usarse nuestra identidad para atribuir fácil y correctamente información sobre cada uno de nosotros con el fin de ser utilizada en el futuro (p.ej., historias clínicas o registros financieros). Pero esta clase de registros también nos permite demostrar cómo nos comportamos históricamente a lo largo de nuestras vidas con el propósito de generar confianza al tiempo que nos obliga a ser más responsables personalmente. Generar confianza y demostrar responsabilidad nos permiten obtener privilegios tales como el acceso a bienes, propiedades o países. A los efectos del acceso, la identidad cumple una doble función: en primer lugar, comunicar nuestra honradez y responsabilidad y, más tarde, al intentar realizar operaciones basándonos en el "capital de confianza" que hemos acumulado, prueba que, en efecto, somos esa misma persona en la que se confió anteriormente. Contrariamente, nuestra identidad puede ser cuestionada con el fin de difundir una representación fraudulenta de nosotros o utilizada por alguien que busca sembrar desconfianza en torno a nuestra persona.

La eficacia que tienen nuestros nombres y números personales para dar cuenta de nuestra identidad es relativa. Un hecho importante es que los datos que nos identifican pueden ser interpretados no solo por personas sino también por computadoras para vincular información digital con atributos que indican si somos personas confiables o no, hecho que es de utilidad en distintas aplicaciones. Los boletines escolares, una multa por exceso de velocidad y nuestra foja de antecedentes financieros son solo algunos ejemplos de estas aplicaciones. Sin embargo, tanto nuestros nombres como nuestros números son eficaces si y solo si son 1) únicos, 2) permanentes, 3) coherentes y 4) están vinculados sin ambigüedades a nuestra persona física. Sabemos que no necesariamente son únicos (p.ej., Juan Pérez) ni permanentes (p.ej., María Pérez de González) y claramente no están vinculados sin ambigüedades a nuestra forma física (p.ej. un tatu-

aje en la frente). Es precisamente en este punto en que la biometría moderna resulta útil. Los datos biométricos se refieren a las características físicas (y conductuales) más propias de cada uno, que pueden ser detectadas por dispositivos e interpretadas por computadoras de modo que puedan usarse como nuestros representantes en el ámbito digital. De este modo podemos vincular nuestros datos digitales y nuestra identidad de forma permanente, consistente y sin ambigüedad y recuperarlos rápida y automáticamente recurriendo a las computadoras.

Modalidades Biométricas

Aunque es mucho lo que se ha avanzado en materia de modalidades biométricas, es imprescindible seguir investigando modalidades nuevas y exóticas como el oído, la marcha, el olor, etc. Por ahora las modalidades que fueron probadas en instrumentaciones de gran tamaño son las huellas dactilares, la cara, el iris y la voz. Estas son las modalidades biométricas que, hasta el día de hoy, mejor cumplen con las pruebas de singularidad, permanencia y consistencia, al tiempo que facilitan la captura a través del uso de dispositivos sensibles de un modo ergonómico, económico y sencillo. Las técnicas patentadas fn ya empleadas incluyen los patrones vasculares (vena de la palma y del dedo) y la geometría de la mano.

La biometría es de naturaleza básicamente estadística. Por lo tanto:

a) cuantos más datos tenga la muestra biométrica (o conjunto de muestras), más probabilidades hay de que ésta sea única,

b) siempre existe cierta posibilidad de que dos individuos diferentes den lugar a muestras biométricas similares o equivalentes, y

c) siempre existirá cierta posibilidad de que la comparación biométrica dé como resultado una coincidencia falsa o una no coincidencia falsa (error Tipo I y Tipo II).

Algunas modalidades biométricas son menos estables a lo largo del tiempo y algunas son más difíciles de presentar y de ser capturadas en forma confiable. Algunas son más susceptibles a plantear problemas de calidad de las muestras.

No existe una modalidad biométrica perfecta. Todas tienen ventajas y desventajas según el caso. Por ejemplo, lo que caracteriza a las huellas dactilares es que, en la escena del crimen, siempre dejan evidencia tras de sí, permanecen “latentes” (por ejemplo, las huellas dactilares que quedan en un vidrio). De todas las modalidades, la más coherente, la que otorga más información, la más parecida a un “código de barras” tal vez sea la del iris. Las imágenes faciales se destacan ya que constituyen la modalidad biométrica en la que mejor nos desempeñamos los seres humanos a la hora de establecer comparaciones. Por eso, esta modalidad permite hacer el reconocimiento integrando y complementando la capacidad humana y la de las máquinas. Además, las imágenes faciales abundan en el ámbito digital y pueden ser obtenidas a distancia y disimuladamente. La voz se destaca por ser una modalidad al mismo tiempo biológica y de comportamiento por lo cual abundan las muestras disponibles para cada individuo.

Aún cuando nuestras muestras biométricas son únicas, permanentes, coherentes y están ligadas físicamente a nosotros, los sensores y algoritmos que hemos inventado para obtenerlas y analizarlas son imperfectos.

Los sensores producen distorsiones ópticas y eléctricas. Al convertir los datos analógicos de la muestra en digitales se pierde información, lo que vuelve a ocurrir en el momento de comprimir la señal digital. Las frecuencias de muestreo (resolución espacial en el dominio digital) tienen un impacto significativo sobre la calidad de las muestras biométricas. La precisión y el desempeño de los algoritmos diseñados para extraer de una muestra “plantillas” de datos comparables varían en gran medida. Lo mismo ocurre con los algoritmos y sistemas utilizados en las computadoras para evaluar rápidamente su similitud. Las máquinas sirven para procesar señales y comparar automáticamente plantillas en forma rápida y razonablemente precisa, pero carecen de la capacidad humana para ver, analizar y caracterizar las semejanzas entre dos muestras.

No obstante, nuestros cuerpos presentan una cantidad de rasgos que resultan muy apropiados para la búsqueda y comparación biométricas. Al mismo tiempo, los avances que registran las modernas tecnologías de detección e informáticas continúan mejorando la habilidad de las máquinas para realizar la identificación biométrica de manera extremadamente rápida y precisa.

Procesos biométricos

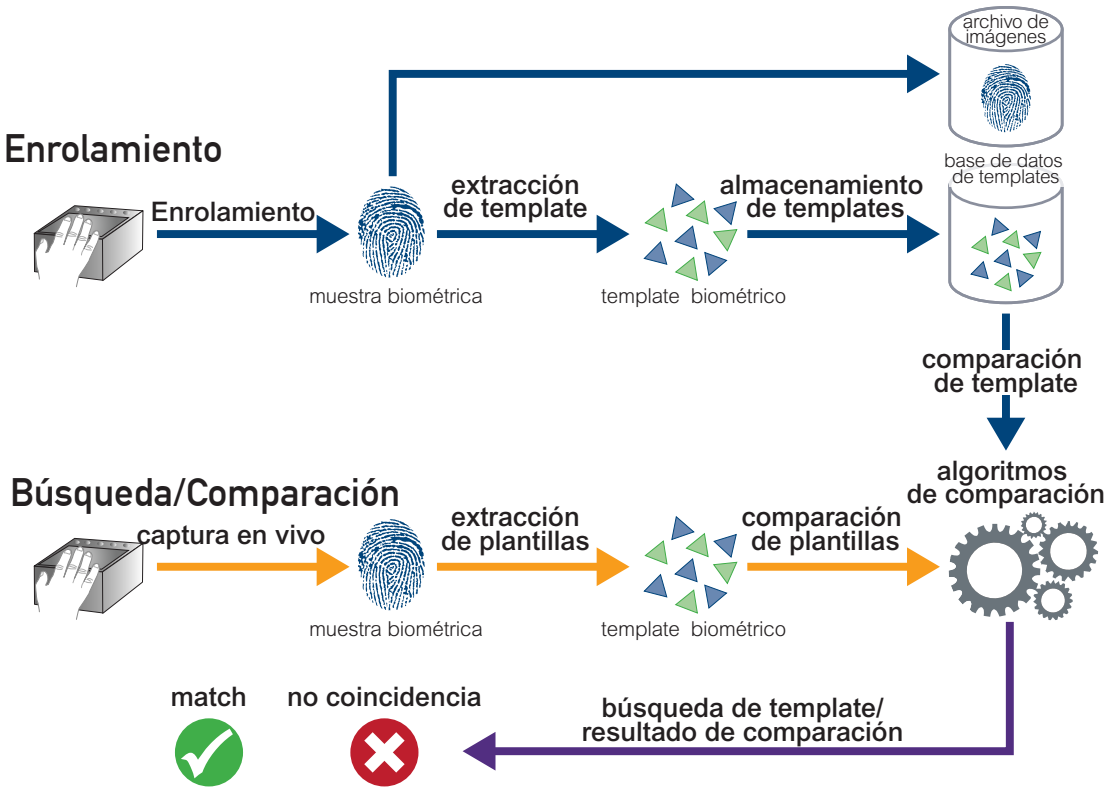
Los sistemas biométricos se basan en distintos procesos discretos: registro, captura en vivo y la extracción y com-

paración de plantillas. El propósito del registro consiste en recoger y archivar las muestras biométricas y generar plantillas numéricas para futuras comparaciones. Al archivar las muestras sin procesar es posible generar, en el caso de que se introduzca en el sistema un algoritmo de comparación nuevo o actualizado, nuevas plantillas sustitutas. Las prácticas que facilitan el registro de muestras de alta calidad son esenciales para garantizar la coherencia de la muestra y mejorar el rendimiento general de la comparación. Esto, a su vez, es especialmente importante para la identificación biométrica en la búsqueda de "uno-a-muchos".

Podemos diferenciar la "captura en vivo" del registro, ya que la primera es el proceso de recolección en vivo de muestras biométricas de tipo "sondeo" luego de acceder o intentar la identificación para compararla con una "galería" de plantillas registradas previamente.

Para generar una plantilla numérica, la extracción de plantillas requiere que se procesen las señales de las muestras biométricas sin procesar (por ejemplo, muestras de imágenes o de audio). A fin de agilizar el procesamiento en las futuras comparaciones, las plantillas se generan y almacenan en el momento del registro. Para evaluar las similitudes entre dos plantillas, la comparación aplica cálculos algorítmicos. Una vez hecha la comparación, se asigna un puntaje de coincidencia. Si dicho puntaje está por encima de un umbral especificado, se considera que las plantillas son coincidentes.

Típicamente, la extracción de plantillas biométricas y la comparación de algoritmos son técnicas patentadas (diferentes y secretas) y no pueden ser usadas en el mismo sistema con técnicas de otros proveedores (por ejemplo, no es posible comparar plantillas generadas por distintos productos, o usar un algoritmo de comparación de una compañía para realizar una comparación con plantillas generadas con algoritmos de otra compañía). La única excepción son las plantillas de huellas dactilares basadas en minucias y los algoritmos de comparación con certificación MINEX. Este tipo de plantillas y dispositivos de comparación fueron específicamente diseñados, probados y certificados de forma independiente por NIST para ser interoperables en la verificación uno-a-uno, de modo que resultan ideales para el almacenamiento compacto en tarjetas inteligentes o documentos de viaje.



Figurua 1 - Sistema biométrico

Prueba de precisión del sistema biométrico

Por lo general, la precisión de un sistema biométrico se cuantifica a través del gráfico de la "característica de funcionamiento del receptor" o "Curva de ROC" que compara las tasas de coincidencias y de no coincidencias falsas con una galería de muestras biométricas. La tasa de coincidencias falsas representa la frecuencia con que se asigna erróneamente a una misma fuente muestras biométricas de distintas fuentes. La tasa de no coincidencias falsas representa la frecuencia con que se asignan erróneamente muestras provenientes de una misma fuente a fuentes diferentes. Un sistema biométrico eficiente se caracteriza por ofrecer resultados inmediatos y por tasas bajas de coincidencias falsas y de no coincidencias falsas. La precisión de un sistema se ubica en un punto de la curva ROC cuya posición es función del "umbral" de coincidencias aplicado. Un umbral alto reduce la tasa de coincidencias falsas al tiempo que incrementa la tasa de no coincidencias falsas (más seguridad, menos practicidad). Un umbral más bajo reduce la tasa de de no coincidencias falsas pero incrementa las coincidencias falsas (más practicidad, menos seguridad; ver la Figura 3). En comparación con los datos que exigen la verificación uno-a-uno, los procesos de búsqueda uno-a-muchos exigen una cantidad mayor de datos (por ejemplo, más huellas dactilares) y muestras de gran calidad (altamente coherentes).

Es importante tener en cuenta que la precisión de un sistema biométrico depende en gran medida de la naturaleza de los datos biométricos incluidos en el sistema. Cada galería de datos biométricos con la que se realiza la búsqueda de un conjunto de sondeo dará como resultado una curva de ROC de distinta precisión. Existen galerías biométricas de acceso público que ofrecen puntos de referencias comunes contra los cuales cotejar los distintos algoritmos de comparación. Es posible mejorar el desempeño de los algoritmos con bases de datos conocidas "instruyéndolos o entrenándolos", algo similar a cuando conocemos de antemano las preguntas de un examen. La instrucción o entrenamiento mejora la precisión de la capacidad de comparar cuando se trabaja con bases de datos conocidas pero no necesariamente ocurre lo mismo cuando los datos son desconocidos, tal como acontece en el mundo real. De manera que para predecir cómo habrá de comportarse un sistema biométrico en un contexto real lo mejor es probar su desempeño con datos para los que no fue instruido de manera explícita.

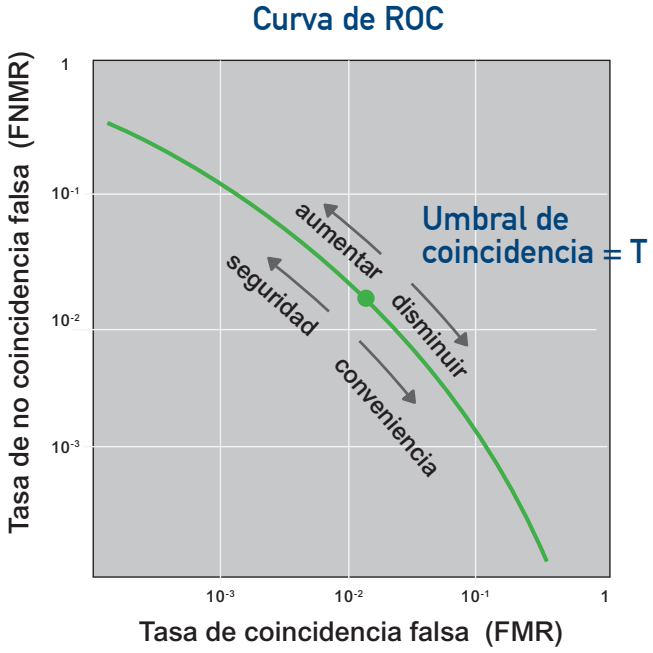


Figura 2 - Uma curva ROC para um determinado sistema de correspondência biométrico e conjunto de dados

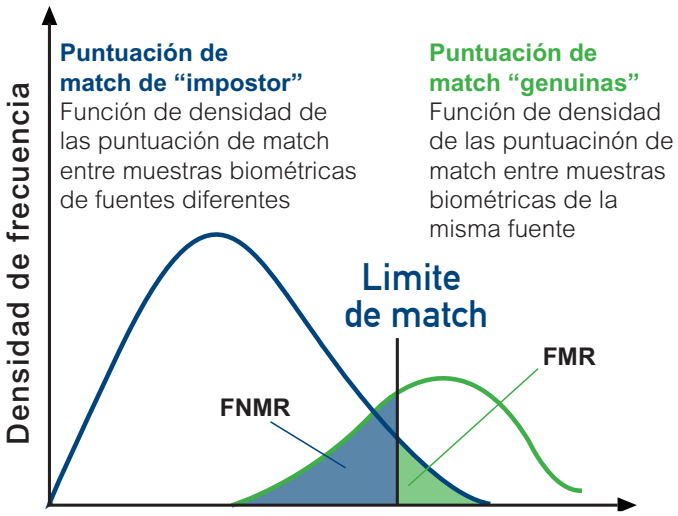


Figura 3 - Funções de densidade de pontuações de comparação entre a) amostras de fontes diferentes e b) amostras das mesmas fontes, ilustrando FMR e FNMR.

Aplicaciones biométricas

La primera modalidad biométrica utilizada fueron las huellas dactilares usadas para identificar a un sospechoso en una investigación criminal. Con el auxilio de las nuevas tecnologías de captura de imágenes y el poder de las computadoras, ese proceso que usaba el papel y era trabajoso se hizo mayormente digital (aunque no totalmente) y automatizado. Nuevas tecnologías permiten emplear la identificación biométrica en otras aplicaciones, a saber, en el proceso de "autenticación" física y lógica de las personas en los controles de acceso, así como en el reconocimiento casi en tiempo real de sospechosos en un control fronterizo, y en otras aplicaciones en las cuales es necesario acceder a los datos muy rápidamente.

Las aplicaciones biométricas pueden agruparse según tres objetivos: 1) verificación, 2) identificación y 3) control de duplicados:

La verificación requiere que se realice una comparación biométrica "uno-a-uno" a fin de asegurar el acceso ya sea a un activo físico o digital, tal como una aplicación informática o base de datos. En este tipo de aplicación, los datos biométricos se usan como contraseña o PIN para reforzar el control de acceso al comparar la muestra biométrica de un individuo con una muestra única confiable almacenada. La muestra almacenada puede estar en una base de datos central, un teléfono inteligente, o ser una clave contenida en una credencial, tal como un documento de identidad inteligente. De esta manera podemos "autenticar" la declaración de identidad de una persona mediante la pregunta siguiente: "¿Es usted la persona a la que se le adjudicó esta clave?" y utilizar el resultado de la comparación para franquear o impedir su acceso. El empleo de datos biométricos para controlar el acceso es especialmente interesante en las aplicaciones destinadas a la seguridad comercial y personal. La verificación biométrica puede utilizarse como una alternativa muy conveniente o como un refuerzo del PIN o contraseña, en cuyo caso, el usuario puede optar por usar el PIN o la contraseña si le resulta más conveniente. Por ejemplo, el iPhone 5S de Apple ofrece esta alternativa.

La identificación es un proceso distinto y más exigente (en términos de algoritmos biométricos y desempeño informático), que sirve para confirmar si los datos biométricos de un individuo se hallan presentes en una base de datos o "galería". Una galería puede contener miles de millones de plantillas e incluso más. En el proceso de identificación, se capturan los datos biométricos vitales de un individuo y se los envía a un sistema de búsqueda biométrico para una comparación de "uno-a-muchos". El sistema compara matemáticamente la plantilla de la muestra biométrica de sondeo con todas las plantillas existentes en la galería. Al hacerlo, los datos biométricos ayudan a identificar a un individuo aun cuando mienta acerca de su identidad. En general, las aplicaciones para la identificación se utilizan en el sector público donde es vital confiar en la identidad por un problema de seguridad pública, por ejemplo en la investigación criminal y en la aplicación de la ley, la emisión de visas y la gestión de fronteras, la verificación de antecedentes antes de contratar nuevos empleados en áreas como defensa e inteligencia.

El control de duplicados es el proceso biométrico que permite determinar si un individuo figura más de una vez en una base de datos. Este recurso posibilita detectar fraudes tales como cuando un individuo se inscribe varias veces en un programa de beneficios sociales. El proceso implica comparar la plantilla biométrica de cada registro presente en la base de datos con cada uno de los otros en un proceso denominado "desduplicación biométrica".

Dispositivos y sensores

Los dispositivos y sensores son cualquier sistema mecánico o electrónico utilizado para registrar y capturar muestras biométricas sin procesar de manera que puedan ser digitalizadas y convertidas en una plantilla biométrica. Para las huellas dactilares, la cara, el iris y la voz, éstos son respectivamente, el sensor de huellas dactilares, las cámaras digitales, las cámaras para iris y los micrófonos. La mayoría de los sensores de huellas dactilares se basan en técnicas ópticas o capacitivas aunque cada vez se usan más los sensores emisores de luz y los sistemas multiespectrales. Los sensores capacitivos pueden ser del tipo imagen de dedo completo o de deslizamiento. Para comparar exitosamente las imágenes de huellas dactilares es imprescindible que dichas imágenes tengan suficiente contraste y resolución (500ppi), hayan sido comprimidas correctamente con WSQ y no presenten distorsiones. Para capturar las imágenes de las huellas dactilares, los sensores ópticos usan un prisma, una fuente de luz y un sensor de luz. Los sensores capacitivos se basan en un chip de silicio que detecta las corrientes

eléctricas en el momento en que las crestas dactilares hacen contacto. Los sensores por deslizamiento generan imágenes que no tienen la calidad de imagen suficiente como para someterlas a una identificación de uno-a-muchos. En términos generales, la cantidad y coherencia de las muestras biométricas requeridas dependen del tamaño de la base de datos en la que debe hacerse la búsqueda.

La captura de las imágenes faciales se realiza con cámaras réflex digitales de uso habitual, cámaras de bolsillo y cámaras web. En los últimos tiempos la tecnología de los sensores de bajo costo evolucionó en forma notable haciendo posible capturar imágenes faciales biométricas con un teléfono inteligente. Actualmente, para la comparación de uno-a-uno, las imágenes faciales digitales necesitan una resolución interocular de aproximadamente 60 pixeles y de 90 pixeles para una comparación de uno-a-muchos. El aspecto más crítico y que plantea el mayor desafío en relación con los resultados de la comparación facial es la coherencia; por un lado, lograr poses, ángulos de la cabeza y expresiones del sujeto similares; por el otro, el brillo, contraste y resolución de la imagen total.

También mejoraron mucho los sensores para los datos biométricos del iris. La comparación del iris se distingue de la de la cara por el hecho de que la primera requiere una imagen infrarroja del iris a fin de optimizar el contraste de la imagen y así facilitar el análisis realizado por la máquina. Cuanto mayor sea el grado de captura de una imagen infrarroja pura (con un mínimo de "contaminación" proveniente de la luz), mejor será el rendimiento de la comparación. Por eso, para capturar la imagen del iris no sirven las cámaras comerciales y todavía se necesita una cámara especial. El sistema debe iluminar el iris con luz infrarroja y filtrar luego las otras longitudes de onda.

La ubicuidad y capacidad para captar audio de los teléfonos inteligentes los hace especialmente viables para desplegar datos biométricos de voz a gran escala y para la verificación uno-a-uno. Los datos biométricos de voz enfrentan los mismos desafíos que los faciales en el sentido de que, en ambos casos, el entorno de captura puede ser muchas veces impredecible e inconsistente. Tal como acontece con las imágenes faciales, el ruido del entorno puede afectar a la captura y al proceso de comparación.

Modos de uso y arquitectura del sistema

Una aplicación biométrica "privada" es aquella que utiliza una única persona para efectuar la verificación biométrica uno-a-uno y asegurar el acceso a sus propios equipos, por ejemplo, su teléfono inteligente. Un sistema "basado en permisos" exige que el controlador de un activo autorice el acceso al mismo (por ejemplo, una compañía que emplea datos biométricos para conferirles a los empleados el ingreso a sus datos). Las aplicaciones "basadas en operador" necesitan un operador autorizado y entrenado en el uso del dispositivo para recopilar datos biométricos de la persona que proporciona la muestra, por ejemplo, una aplicación de una autoridad de aplicación de la ley. Las aplicaciones "basadas en quioscos" admiten que la persona que realiza la captura no tenga entrenamiento ni experiencia previa y cuente con una instrucción mínima. Es lo que ocurre en un control automatizado de puesto fronterizo.

Las plantillas biométricas previamente registradas o las plantillas con las cuales se compara la plantilla de una muestra capturada en vivo pueden estar en cualquier ubicación, por ejemplo, en un teléfono inteligente, una credencial, tal como el chip de una tarjeta de identificación o en un código de barras impreso, en un dispositivo de captura biométrico móvil o en un servidor central. La ubicación de las plantillas registradas y la del lugar en el que se realizan las comparaciones dependen del uso, el funcionamiento y la seguridad de la aplicación. La comparación biométrica uno-a-uno puede incluso realizarse totalmente en el chip de una tarjeta inteligente.

Privacidade

Os governos coletam informações pessoais sobre seus cidadãos, normalmente, com interesse em promover melhoria social, médica e de segurança física de algum tipo. Nem todos concordam sobre o quanto dessas informações pessoais é excessiva e a biometria tende a resumir informações pessoais consideradas como sendo excessivas. O uso histórico da biometria por órgãos governamentais de policiamento como uma ferramenta para registro criminal e investigação perpetua, acaba por perpetuar sua associação com a privação de direitos pessoais. Em algumas partes do mundo, existe um histórico de abuso de informações pessoais que gerou uma forte aversão a sua posse

pelos governos. Embora, atualmente, as corporações privadas possuam, usem e transfiram quantidades de dados pessoais significativamente maiores, temos a tendência de considerá-las mais inócuas e que estamos obtendo algo em troca, como o uso de seus produtos.

Mais recentemente, com a proliferação da Internet, das câmeras digitais, smartphones e mídia social foi introduzida a era do "Big Data" e com ela veio um aumento exponencial na disponibilidade de dados pessoais e o potencial para seu abuso. Estamos aprendendo que nessa nova era, a privacidade é uma escolha muito pessoal; alguns indivíduos optam por minimizar a quantidade de informações pessoais que compartilham, enquanto outros, entusiasticamente, "as compartilham em excesso". Nos dois casos, a biometria tem o potencial de fornecer meios mais práticos e seguros para aumentar a privacidade por meio de um melhor controle de acesso a uma crescente e vasta abundância de informações pessoais, especialmente quando usadas em conjunto com outros mecanismos tradicionais de segurança como números PIN e senhas.

A abundância das imagens faciais na Internet oferece a oportunidade que sejam abusadas como biometria. É concebível que por meio de um processo de "resolução de identidade", as imagens faciais e seus dados associados (por ex., nome, escola, associações, etc.) possam ser associados por meio de identificação facial biométrica com informações de diferentes sites e bancos de dados onde as imagens faciais estão armazenadas. A resolução da identidade é um processo, bem diferente, os dados "em silos" são agregados em uma "identidade digital" que compreende uma visão mais abrangente de uma pessoa que existe a partir de qualquer fonte de dados individual. Quando quantidades pequenas e dispersas de informações pessoais foram disponibilizadas — cada uma com um uso específico e um público em mente — a agregação desses dados pessoais a partir de várias fontes disponibilizadas com uma pesquisa facial biométrica pode constituir uma ameaça à privacidade. Deve-se notar que não está claro se isso realmente já foi feito de forma que afetou a privacidade de alguém. Além disso, esse processo é mais tradicionalmente (e talvez mais efetivamente) executado usando os dados em texto e, portanto, existe uma ameaça potencial com ou sem a presença de imagens faciais. Vale a pena notar que outras modalidades biométricas não apresentam o mesmo risco que as imagens faciais para este tipo de processo, porque não existem abundantemente em domínio público. Ao avaliar o impacto da biometria na privacidade, é essencial considerá-la em um contexto mais amplo de todos os dados de identidade baseados em sinal e em texto; isso inclui os dados que são mantidos pelos órgãos governamentais e por entidades privadas, disponíveis na Internet e a partir de outros códigos abertos.

Privacidad

Existem pouquissimos relatos de sistemas biométricos fraudados, seja para evitar identificação ou seja obter acesso não autorizado. Ocasionalmente, os jornalistas simulam tentativas de violação e as publicam largamente, portanto, a ameaça de furos de segurança contidos na biometria tende a ser uma percepção aumentada.

Los gobiernos recogen información personal acerca de sus ciudadanos, en general con el fin de mejorar su seguridad social, médica y física. No existe acuerdo respecto a cuánta información personal se considera adecuada. En cuanto a los datos biométricos, éstos tienden a ser vistos como el tipo de información que algunos consideran excesiva. El uso que siempre han hecho los gobiernos de los datos biométricos, a través de las autoridades judiciales y policiales, a fin de llevar un registro de criminales y realizar investigaciones, a menudo se asocia con la pérdida de los derechos individuales. En algunas regiones del mundo existe un historial de abusos de la información personal que ha contribuido a que surja una fuerte aversión a que los gobiernos dispongan de la misma. Aun cuando hoy en día las corporaciones poseen, utilizan y comercian grandes cantidades de datos personales, tendemos a ver este fenómeno como si fuera inocuo y algo a cambio de lo cual recibimos alguna ventaja tal como el uso de sus productos.

En los últimos tiempos, la proliferación de Internet, cámaras digitales, teléfonos inteligentes y redes sociales dio nacimiento a la era "Big Data" en la que se produce un incremento exponencial de los datos personales disponibles y del potencial para el abuso de los mismos. Estamos aprendiendo que, en esta nueva era, la privacidad es una elección muy personal. Algunas personas tienden a compartir la menor cantidad de

información personal posible mientras que otras dan a conocer sus datos con gran entusiasmo. Cualquiera sea el caso, la biometría brinda la posibilidad de disponer de formas seguras y convenientes que aumentan la privacidad, al asegurar un mayor control del acceso a la información personal, cada vez más abundante, en especial cuando se la utiliza con otros mecanismos tradicionales de seguridad tales como los PIN y las contraseñas.

La enorme cantidad de imágenes faciales que proliferan en Internet hace posible que se abuse de ellas. Es posible pensar que a través de un proceso de "resolución de identidad", se puedan asociar, vía la comparación biométrica, las imágenes faciales y los datos asociados a ellas (por ejemplo, el nombre, la escuela, las personas vinculadas, etc.) con información proveniente de sitios web y bases de datos que contengan esas mismas imágenes. La resolución de identidad es un proceso por el cual la información, antes dispersa y "aislada", se combina en una "identidad digital" que ofrece una visión más completa de una persona que la que existe en cualquier fuente de datos individual. Ahora que están disponibles cantidades pequeñas y dispersas de información personal - cada una de ellas para un uso determinado y una audiencia específica - la reunión de estos datos personales provenientes de múltiples fuentes, que hizo posible la búsqueda por datos biométricos faciales, plantea una amenaza a la privacidad. Cabe destacar que, hasta el día de hoy, no existe información de que haya ocurrido algún incidente que haya impactado en la privacidad de nadie. Más aun, esta amenaza existe desde antes (y tal vez con mayor efectividad) mediante la utilización de datos provenientes de fuentes escritas, de modo que la amenaza potencial existe en presencia y en ausencia de imágenes faciales. Vale la pena notar que, en relación con este peligro, las otras modalidades biométricas no plantean el mismo riesgo simplemente porque su presencia en el dominio público no es tan frecuente. Al estimar el impacto de los datos biométricos en la privacidad es muy importante considerarlos dentro del contexto más amplio de todos los datos de identidad basados en textos y señales, lo que incluye la información que manejan los organismos gubernamentales, entidades privadas, disponibles en Internet y otras fuentes abiertas.

About Aware, Inc.

Aware es un proveedor líder en productos de software biométrico y desarrollo de servicios para organismos de gobierno, integradores de sistemas y proveedores de soluciones de todo el mundo. Nuestros productos incluyen múltiples SDK, componentes de software, aplicaciones para estaciones de trabajo y una plataforma modular y centralizada orientada al servicio. Desempeñan una gran variedad de funciones críticas para la autenticación biométrica y de búsqueda utilizando huellas dactilares, el rostro y el iris, que incluyen la captura automática de muestras, el aseguramiento de la calidad de la imagen, la abstracción de los dispositivos periféricos de hardware de captura, el procesamiento de datos y flujos de trabajo centralizados, la conectividad de subsistemas y algoritmos de correlación de datos biométricos. Los productos se usan para habilitar soluciones de seguridad centradas en la identidad con datos biométricos para aplicaciones, entre ellas, organismos de aplicación de la ley, gestión de fronteras, acreditación y control de acceso y defensa e inteligencia. Aware es una empresa que cotiza en bolsa (NASDAQ: AWRE) con sede en Bedford, Massachusetts.

AWARE

Para maiores informações:

sales@aware.com
www.aware.com