

Sistema y Método para Desentrañar Características Específicas de Usuarios, Acciones y Dispositivos Registrados en los Datos del Sensor de Movimiento

5

Referencia Cruzada a Solicitudes Relacionadas

La presente solicitud se basa en la solicitud de patente provisional de EE. UU. con número de serie: 62/957,653, titulada "Sistema y Método para Desentrañar Características Específicas de Usuarios, Acciones y Dispositivos Registrados en Datos de Sensores de Movimiento", y reivindica prioridad en ella, presentada el 6 de enero de 2020, el cuyos contenidos se incorporan aquí por referencia como si se establecieran expresamente en su totalidad en este documento.

15

Campo Técnico

La presente solicitud se refiere a sistemas y métodos para extraer características de un usuario y, en particular, a sistemas y métodos para extraer características discriminatorias de un usuario de un dispositivo a partir de datos de sensores de movimiento relacionados con el usuario.

20

Antecedentes

Los sistemas de Aprendizaje Automático (ML) estándar, diseñados para la identificación y autenticación de usuarios de teléfonos inteligentes (propietarios) en función de los datos del sensor de movimiento, sufren graves caídas de rendimiento y precisión (por ejemplo, más del 10 %) cuando un atacante intenta autenticarse en el teléfono inteligente del propietario. Este problema ocurre naturalmente cuando el sistema ML no puede separar las características discriminatorias del usuario de las características discriminatorias del dispositivo de teléfono inteligente o las características discriminatorias de la acción genérica (por ejemplo, quitar el teléfono de la mesa, contestar una llamada, etc.). El problema se debe al hecho de que las señales registradas por los sensores de movimiento (por ejemplo, acelerómetro y giroscopio) durante una sesión de

autenticación contienen todas estas características (representativas del usuario, la acción y el dispositivo) juntas.

Un enfoque para resolver este problema es recolectar señales de movimiento adicionales durante el registro del usuario: (a) pidiéndole al usuario que se autentique en múltiples dispositivos mientras realiza diferentes acciones (por ejemplo, sentarse en una silla, ponerse de pie, cambiar de mano, etc.) o (b) solicitar al propietario del teléfono inteligente que permita que otra persona realice algunas autenticaciones (para simular posibles ataques). Sin embargo, ambas opciones son inconvenientes para el usuario.

Como tal, existe la necesidad de una forma más fiable y eficiente de extraer las características discriminatorias de un usuario de un dispositivo móvil.

15

Resumen

En un primer aspecto, se proporciona un método implementado por computadora para desentrañar las características discriminatorias de un usuario de un dispositivo de las señales de movimiento capturadas por un dispositivo móvil. El dispositivo móvil tiene uno o más sensores de movimiento, un medio de almacenamiento, instrucciones almacenadas en el medio de almacenamiento y un procesador configurado mediante la ejecución de las instrucciones. En el método, cada señal de movimiento capturada se divide en segmentos, con el procesador. Luego, los segmentos se convierten en segmentos traducidos con el procesador usando uno o más algoritmos de traducción entrenados. Luego, los segmentos y los segmentos traducidos se proporcionan a un sistema de aprendizaje automático con el procesador. Luego, las características discriminatorias del usuario se extraen de los segmentos y los segmentos traducidos con el procesador utilizan el sistema de aprendizaje automático que aplica uno o más algoritmos de extracción de características.

En otro aspecto, las características discriminatorias del usuario se utilizan para identificar al usuario en el futuro uso del dispositivo por parte del usuario. En otro aspecto, el uno o más sensores de movimiento comprenden al menos uno de un

giroscopio y un acelerómetro. En otro aspecto, la una o más señales de movimiento corresponden a una o más interacciones entre el usuario y el dispositivo móvil.

- 5 En otro aspecto, las señales de movimiento incluyen características discriminatorias del usuario, características discriminatorias de acciones realizadas por el usuario y características discriminatorias del dispositivo móvil. En otro aspecto, el paso de dividir una o más señales de movimiento capturadas en segmentos elimina las características discriminatorias de las acciones
10 realizadas por el usuario. En otro aspecto, el paso de convertir los segmentos en los segmentos traducidos elimina las características discriminatorias del dispositivo móvil.

- En otro aspecto, el uno o más algoritmos de traducción entrenados comprenden
15 una o más redes generativas antagónicas coherentes con el ciclo (Cycle-GAN) y los segmentos traducidos comprenden señales de movimiento sintéticas que simulan señales de movimiento que se originan en otro dispositivo.

- En otro aspecto, el paso de dividir una o más señales de movimiento capturadas
20 en segmentos comprende dividir cada señal de movimiento en un número fijo de segmentos, donde cada segmento tiene una longitud fija.

- En un segundo aspecto, se proporciona un método implementado por computadora para autenticar a un usuario en un dispositivo móvil a partir de
25 señales de movimiento capturadas por un dispositivo móvil. El dispositivo móvil tiene uno o más sensores de movimiento, un medio de almacenamiento, instrucciones almacenadas en el medio de almacenamiento y un procesador configurado mediante la ejecución de las instrucciones. En el método, la una o más señales de movimiento capturadas se dividen en segmentos con el
30 procesador. Los segmentos se convierten en segmentos traducidos con el procesador usando uno o más algoritmos de traducción entrenados. Los segmentos y el segmento traducido se proporcionan a un sistema de aprendizaje automático con el procesador. Los segmentos y los segmentos traducidos se clasifican luego como pertenecientes a un usuario autorizado o como

pertenecientes a un usuario no autorizado con el procesador asignando una puntuación a cada uno de los segmentos y segmentos traducidos. Luego se aplica un esquema de votación o un modelo de metaaprendizaje sobre las puntuaciones asignadas a los segmentos y los segmentos traducidos con el procesador. Luego se determina, con el procesador, si el usuario es un usuario autorizado según el esquema de votación o el modelo de metaaprendizaje.

En otro aspecto, el paso de clasificar comprende: comparar los segmentos y los segmentos traducidos con características del usuario autorizado extraídas de segmentos de muestra proporcionados por el usuario autorizado durante un proceso de inscripción, donde las características se almacenan en el medio de almacenamiento; y asignar a cada segmento una puntuación basada en un modelo de clasificación.

En otro aspecto, el uno o más sensores de movimiento comprenden al menos uno de un giroscopio y un acelerómetro. En otro aspecto, el paso de dividir una o más señales de movimiento capturadas en segmentos comprende dividir cada señal de movimiento en un número fijo de segmentos, y cada segmento tiene una longitud fija. En otro aspecto, al menos una parte de los segmentos se superponen.

En otro aspecto, uno o más algoritmos de traducción entrenados comprenden uno o más Cycle-GAN, y el paso de conversión comprende: traducir los segmentos a través de un primer generador en los segmentos traducidos, que imitan los segmentos generados en otro dispositivo; y volver a traducir los segmentos traducidos a través de un segundo generador para imitar los segmentos generados en el dispositivo móvil.

En otro aspecto, los segmentos traducidos comprenden señales de movimiento sintéticas que simulan señales de movimiento que se originan en otro dispositivo. En otro aspecto, el paso de provisión comprende: extraer, con el procesamiento usando una o más técnicas de extracción de características, características de los segmentos y segmentos traducidos para formar vectores de características; y empleando un modelo de clasificación

aprendido sobre los vectores de características que corresponden a los segmentos y los segmentos traducidos.

En un tercer aspecto, se proporciona un sistema para desentrañar las
5 características discriminatorias de un usuario de un dispositivo de las señales de movimiento capturadas en un dispositivo móvil y autenticar a un usuario en el dispositivo móvil, donde el dispositivo móvil tiene al menos un sensor de movimiento. El sistema incluye una interfaz de comunicación de red, un medio de almacenamiento legible por computadora y un procesador configurado para
10 interactuar con la interfaz de comunicación de red y el medio de almacenamiento legible por computadora y ejecutar uno o más módulos de software almacenados en el medio de almacenamiento. Los módulos de software incluyen:

un módulo de segmentación que, cuando se ejecuta, configura el procesador
15 para dividir cada señal de movimiento capturada en segmentos;
un módulo de conversión que, cuando se ejecuta, configura el procesador para convertir los segmentos en segmentos traducidos utilizando una o más redes adversas generativas coherentes con el ciclo (Cycle-GAN) entrenadas;
un módulo de extracción de características que, cuando se ejecuta, configura el
20 procesador para extraer características discriminatorias del usuario de los segmentos y segmentos traducidos, utilizando el procesador un sistema de aprendizaje automático;
un módulo de clasificación que cuando se ejecuta configura el procesador para asignar puntajes a los segmentos y segmentos traducidos y determinar si los
25 segmentos y segmentos traducidos pertenecen a un usuario autorizado o a un usuario no autorizado en base a sus puntajes respectivos; y
un módulo de metaaprendizaje que cuando se ejecuta configura el procesador para aplicar un esquema de votación o un modelo de metaaprendizaje sobre las puntuaciones asignadas a los segmentos y segmentos traducidos en función de
30 los segmentos almacenados correspondientes al usuario.

En otro aspecto, el al menos un sensor de movimiento comprende al menos un giroscopio y un acelerómetro.

En otro aspecto, el módulo de conversión configura el procesador para traducir los segmentos a través de un primer generador en los segmentos traducidos, que imitan los segmentos generados en otro dispositivo y vuelven a traducir los segmentos traducidos a través de un segundo generador para imitar los segmentos generados en el dispositivo móvil.

En otro aspecto, el módulo de extracción de características está además configurado para emplear un modelo de clasificación aprendido en las características extraídas que corresponden a los segmentos y los segmentos traducidos.

Breve descripción de los dibujos

La figura 1A describe un diagrama de alto nivel de un sistema para desentrañar las características discriminatorias de un usuario de un dispositivo de los datos del sensor de movimiento y autenticar a un usuario de los datos del sensor de movimiento, de acuerdo con al menos una realización descrita aquí;

La figura 1B es un diagrama de bloques de un sistema informático para desentrañar las características discriminatorias de un usuario de un dispositivo de los datos del sensor de movimiento y autenticar a un usuario de los datos del sensor de movimiento, de acuerdo con al menos una realización descrita aquí;

La figura 1C es un diagrama de bloques de módulos de software para desentrañar las características discriminatorias de un usuario de un dispositivo de los datos del sensor de movimiento y autenticar a un usuario de los datos del sensor de movimiento, de acuerdo con al menos una realización descrita aquí;

La figura 1D es un diagrama de bloques de un sistema informático para desentrañar las características discriminatorias de un usuario de un dispositivo de los datos del sensor de movimiento y autenticar a un usuario de los datos del sensor de movimiento, de acuerdo con al menos una realización descrita aquí;

5

La figura 2 es un diagrama que muestra un sistema de identificación de usuario de teléfono inteligente estándar ejemplar y un diagrama de flujo basado en aprendizaje automático, de acuerdo con una o más realizaciones;

10 La figura 3 es un diagrama que muestra un sistema de dispositivo móvil ejemplar y un diagrama de flujo para la identificación del usuario mediante la eliminación de características discriminatorias de la acción basada en el aprendizaje automático, de acuerdo con una o más realizaciones;

15 La figura 4 es un diagrama de una Red adversa generativa coherente con el ciclo (Cycle-GAN) a modo de ejemplo para la traducción de señal a señal, de acuerdo con una o más realizaciones;

Las figuras 5A-5D muestran un sistema y un diagrama de flujo para desentrañar
20 las características discriminatorias de un usuario de un dispositivo móvil de los datos del sensor de movimiento y autenticar a un usuario de los datos del sensor de movimiento, de acuerdo con una o más realizaciones;

La figura 6A describe un diagrama de bloques de alto nivel que muestra un flujo
25 de cálculo para desentrañar las características discriminatorias de un usuario de un dispositivo de los datos del sensor de movimiento, de acuerdo con al menos una realización descrita en este documento; y

La figura 6B revela un diagrama de bloques de alto nivel que muestra un flujo de
30 cálculo para autenticar a un usuario en un dispositivo móvil a partir de datos de sensores de movimiento, de acuerdo con al menos una realización revelada en este documento.

Descripción detallada de ciertas realizaciones

A modo de descripción general e introducción, aquí se describen sistemas y métodos ejemplares para extraer o separar las características discriminatorias de un usuario de teléfono inteligente de las señales de movimiento y separarlas de las características que son útiles para discriminar la acción y discriminar el dispositivo, sin requerir que el usuario realice cualquier autenticación adicional durante el registro. De acuerdo con una o más realizaciones del método, en una primera etapa, las características que discriminan las acciones se eliminan cortando la señal en fragmentos más pequeños y aplicando un sistema de aprendizaje automático en cada uno de estos fragmentos, de forma independiente. Debe entenderse que el término "eliminar" no significa necesariamente que las características de la señal relacionadas con la acción (o el dispositivo) se eliminen de la(s) señal(es) de datos de movimiento resultante. Más bien, el proceso elimina efectivamente la característica discriminatoria de la acción ofuscando esas características discriminatorias a través del procesamiento independiente de los fragmentos de señal. Dicho de otra manera, dado que el sistema no puede reconstruir toda la señal a partir de pequeños fragmentos, la acción del usuario que corresponde a la señal de movimiento (p. ej., deslizar el dedo, gesto) ya no se puede recuperar e identificar y, por lo tanto, se elimina efectivamente. En una segunda etapa, las características que discriminan el dispositivo se eliminan efectivamente empleando un modelo generativo, p. redes adversarias generativas, para simular sesiones de autenticación en un conjunto predefinido de dispositivos. El modelo generativo está entrenado para tomar como entrada fragmentos de señales de un dispositivo y proporcionar como salida fragmentos de señales similares que reemplazan las características del dispositivo de entrada con características discriminatorias para otros dispositivos en un conjunto predefinido. Después de infundir características de diferentes dispositivos en las señales de un determinado usuario, el sistema de aprendizaje automático puede aprender de los fragmentos de señal originales y los fragmentos de señal simulados qué características no cambian entre dispositivos. Estas son las características que son útiles para discriminar al usuario en cuestión.

Los métodos y sistemas descritos en este documento se pueden conectar a cualquier sistema de aprendizaje automático diseñado para la identificación y

autenticación de usuarios (propietarios) de teléfonos inteligentes, por ejemplo. Los métodos y sistemas descritos se centran en las características discriminatorias del usuario, al tiempo que eliminan las características que discriminan dispositivos y acciones. Los métodos y sistemas se validan en un conjunto de experimentos y los beneficios se demuestran empíricamente.

La figura 1A describe un diagrama de alto nivel del presente sistema 100 para desentrañar las características discriminatorias de un usuario de un dispositivo de los datos del sensor de movimiento y autenticar a un usuario de los datos del sensor de movimiento de acuerdo con al menos una realización. Los presentes métodos pueden implementarse usando uno o más aspectos del presente sistema 100, como se describe con más detalle a continuación. En algunas implementaciones, el sistema 100 incluye una plataforma de servidor de sistema basada en la nube que se comunica con PC, servidores y dispositivos fijos como teléfonos inteligentes, tabletas y computadoras portátiles operados por los usuarios.

En una disposición, el sistema 100 comprende un servidor de sistema (servidor back-end) 105 y uno o más dispositivos de usuario que incluyen uno o más dispositivos móviles 101. Mientras que los presentes sistemas y métodos generalmente se describen como realizados, en parte, con un dispositivo móvil (por ejemplo, un teléfono inteligente), en al menos una realización, los presentes sistemas y métodos pueden implementarse en otros tipos de dispositivos informáticos, como estaciones de trabajo, una computadora personal, una computadora portátil, dispositivos de control de acceso u otras computadoras digitales apropiadas. Por ejemplo, mientras que los dispositivos orientados al usuario, como el dispositivo móvil 101, normalmente capturan las señales de movimiento, el sistema puede realizar una o más de las operaciones de procesamiento ejemplares dirigidas a desentrañar las características discriminatorias del usuario de la señal de movimiento, y la autenticación/identificación. servidor 105. El sistema 100 también puede incluir uno o más dispositivos informáticos remotos 102.

El servidor del sistema 105 puede ser prácticamente cualquier dispositivo informático o aparato de procesamiento de datos capaz de comunicarse con los dispositivos de usuario y los dispositivos informáticos remotos y recibir, transmitir y almacenar información electrónica y procesar solicitudes como se describe más adelante en este documento. De manera similar, el dispositivo informático remoto 102 puede ser prácticamente cualquier dispositivo informático o aparato de procesamiento de datos capaz de comunicarse con el servidor del sistema o los dispositivos de usuario y recibir, transmitir y almacenar información electrónica y procesar solicitudes como se describe más adelante en este documento. También debe entenderse que el servidor del sistema o dispositivo informático remoto puede ser cualquier número de dispositivos informáticos en red o basados en la nube.

En una o más realizaciones, el o los dispositivos de usuario, el o los dispositivos móviles 101 pueden configurarse para comunicarse entre sí, el servidor del sistema 105 o el dispositivo informático remoto 102, transmitiéndoles información electrónica y recibiendo información electrónica de ellos. Los dispositivos de usuario pueden configurarse para capturar y procesar señales de movimiento del usuario, por ejemplo, correspondientes a uno o más gestos (interacciones) de un usuario 124.

El (los) dispositivo (s) móvil (es) 101 puede(n) ser cualquier dispositivo informático móvil o aparato de procesamiento de datos capaz de incorporar los sistemas y métodos descritos en este documento, incluidos, entre otros, una computadora personal, tableta, asistente digital personal, dispositivo electrónico móvil, teléfono celular o dispositivo de teléfono inteligente y similares.

Cabe señalar que, si bien la figura 1A representa el sistema 100 para desentrañar las características discriminatorias de un usuario y la autenticación del usuario con respecto a los dispositivos móviles 101 y un dispositivo informático remoto 102, cualquier número de dichos dispositivos puede interactuar con el sistema en la forma aquí descrita. También se debe tener en cuenta que mientras que la figura 1A representa un sistema 100 para desentrañar las características discriminatorias de un usuario y la autenticación con respecto al usuario 124,

cualquier número de usuarios puede interactuar con el sistema de la manera descrita en este documento.

Debe entenderse además que si bien los diversos dispositivos y máquinas informáticos a los que se hace referencia en el presente, incluidos, entre otros, los dispositivos móviles 101, el servidor del sistema 105 y el dispositivo informático remoto 102, se denominan en el presente dispositivos y máquinas individuales o individuales, en determinadas implementaciones los dispositivos y máquinas a los que se hace referencia, y sus operaciones, características y funcionalidades asociadas o que los acompañan pueden combinarse u organizarse o emplearse de otro modo a través de una serie de dichos dispositivos o máquinas, como a través de una conexión de red o una conexión por cable, como es sabido por aquellos de destreza en el arte.

También debe entenderse que los sistemas y métodos ejemplares descritos en este documento en el contexto de los dispositivos móviles 101 (también denominados teléfonos inteligentes) no se limitan específicamente al dispositivo móvil y pueden implementarse utilizando otros dispositivos informáticos habilitados.

Con referencia ahora a la figura 1B, el dispositivo móvil 101 del sistema 100 incluye varios componentes de hardware y software que sirven para permitir el funcionamiento del sistema, incluidos 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 de cliente en forma de instrucciones de software que se pueden cargar en la memoria 120. El procesador 110 puede ser cualquier número de procesadores, una unidad de procesamiento central CPU, una unidad de procesamiento de gráficos GPU, un núcleo multiprocesador o cualquier otro tipo de procesador, dependiendo de la implementación.

Preferiblemente, el procesador 110 puede acceder a la memoria 120 y/o al almacenamiento 190, lo que permite que el procesador reciba y ejecute instrucciones codificadas en la memoria y/o en el almacenamiento para hacer que

el dispositivo móvil y sus diversos componentes de hardware lleven a cabo operaciones para aspectos de los sistemas y métodos como se describirá con mayor detalle a continuación. La memoria puede ser, por ejemplo, una memoria de acceso aleatorio (RAM) o cualquier otro medio de almacenamiento legible por ordenador volátil o no volátil adecuado. Además, la memoria puede ser fija o extraíble. El almacenamiento 190 puede tomar varias formas, dependiendo de la implementación. Por ejemplo, el almacenamiento puede contener uno o más componentes o dispositivos, como un disco duro, una memoria flash, 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 pueden codificarse 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 un código de programa de computadora, o un conjunto de instrucciones ejecutadas en el procesador 110. En una realización ejemplar, como se representa en la figura 1C, preferiblemente, incluido entre los módulos de software 130 hay un módulo de interfaz de usuario 170, un módulo de extracción de características 172, un módulo de segmentación 173, un módulo de clasificación 174, un módulo de metaaprendizaje 175, un módulo de base de datos 176, un módulo de comunicación 177, y un módulo de conversión 178 que son ejecutados por el procesador 110. Tal código de programa informático o instrucciones configuran el procesador 110 para llevar a cabo operaciones de los sistemas y métodos descritos en este documento y pueden escribirse en cualquier combinación de uno o más lenguajes de programación.

Específicamente, el módulo de interfaz de usuario 170 puede comprender uno o más algoritmos para realizar pasos relacionados con la captura de señales de movimiento de un usuario y la autenticación de la identidad del usuario. El módulo de extracción de características 172 puede comprender uno o más algoritmos de extracción de características (por ejemplo, algoritmos de aprendizaje automático) para realizar pasos relacionados con la extracción de características discriminatorias de los usuarios de segmentos y segmentos traducidos de las señales de movimiento del usuario. El módulo de segmentación 173 puede

comprender uno más algoritmos para realizar pasos relacionados con la división de las señales de movimiento capturadas en segmentos. El módulo de conversión 178 comprende uno o más algoritmos de traducción para realizar pasos relacionados con la conversión de segmentos de señales de movimiento en segmentos traducidos. El módulo de clasificación 174 comprende uno o más algoritmos para realizar pasos relacionados con la puntuación (por ejemplo, asignar probabilidades de clase a) los segmentos y los segmentos traducidos. El módulo de metaaprendizaje 175 comprende uno o más algoritmos (por ejemplo, un esquema de votación o un modelo de metaaprendizaje) para realizar pasos relacionados con la integración de las puntuaciones asignadas a los segmentos y segmentos traducidos para identificar o rechazar al usuario que intenta autenticarse. El módulo de base de datos 176 comprende uno o más algoritmos para almacenar o guardar datos relacionados con las señales de movimiento, segmentos o segmentos traducidos a la base de datos 185 o al almacenamiento 190. El módulo de comunicación 177 comprende uno o más algoritmos para transmitir y recibir señales entre la computadora dispositivos 101, 102 y/o 105 del sistema 100.

El código del programa puede ejecutarse completamente en el dispositivo móvil 101, como un paquete de software independiente, en parte en el dispositivo móvil, en parte en el servidor del sistema 105 o completamente en el servidor del sistema u otra computadora o dispositivo remoto. En el último escenario, la computadora remota se puede conectar al dispositivo móvil 101 a través de cualquier tipo de red, incluida una red de área local (LAN) o una red de área amplia (WAN), una red de comunicaciones móviles, una red celular, o la conexión puede ser hecho a una computadora externa (por ejemplo, a través de Internet utilizando un proveedor de servicios de Internet).

En una o más realizaciones, el código de programa de los módulos de software 130 y uno o más dispositivos de almacenamiento legibles por computadora (como la memoria 120 y/o el almacenamiento 190) forman un producto de programa de computadora que se puede fabricar y/o distribuir de acuerdo con la presente invención, como es conocido por los expertos en la materia.

En algunas realizaciones ilustrativas, uno o más de los módulos de software 130 se pueden descargar a través de una red al almacenamiento 190 desde otro dispositivo o sistema a través de la interfaz de comunicación 150 para usar dentro del sistema 100. Además, cabe señalar que otra información y/o datos relevantes para el funcionamiento de los presentes sistemas y métodos (como la base de datos 185) también se pueden almacenar en el almacenamiento. Preferiblemente, dicha información se almacena en un almacén de datos cifrados que se asigna específicamente para almacenar de forma segura la información recopilada o generada por el procesador que ejecuta la aplicación de autenticación segura. Preferiblemente, las medidas de cifrado se utilizan para almacenar la información localmente en el almacenamiento del dispositivo móvil y transmitir información al servidor del sistema 105. Por ejemplo, dichos datos se pueden cifrar utilizando un cifrado polimórfico de 1024 bits o, dependiendo de los controles de exportación, un método de cifrado de 256 bits AES. Además, el cifrado se puede realizar utilizando claves remotas (iniciales) o claves locales (iniciales). Se pueden usar métodos de encriptación alternativos como entenderán los expertos en la técnica, por ejemplo, SHA256.

Además, los datos almacenados en el(los) dispositivo(s) móvil(es) 101 y/o el servidor del sistema 105 se pueden cifrar usando los datos del sensor de movimiento de un usuario o la información del dispositivo móvil como clave de cifrado. En algunas implementaciones, se puede usar una combinación de lo anterior para crear una clave única compleja para el usuario que se puede cifrar en el dispositivo móvil usando criptografía de curva elíptica, preferiblemente de al menos 384 bits de longitud. Además, esa clave se puede utilizar para proteger los datos del usuario almacenados en el dispositivo móvil o en el servidor del sistema.

Además, en una o más realizaciones, una base de datos 185 se almacena en el almacenamiento 190. Como se describirá con mayor detalle a continuación, la base de datos 185 contiene o mantiene varios elementos y elementos de datos que se utilizan a lo largo de las diversas operaciones del sistema 100 y métodos para desentrañar las características discriminatorias de un usuario y la autenticación del usuario. La información almacenada en la base de datos puede

incluir, entre otros, plantillas de datos de sensores de movimiento del usuario e información de perfil, como se describirá con mayor detalle en este documento. Cabe señalar que, aunque la base de datos se representa como configurada localmente para el dispositivo móvil 101, en ciertas implementaciones, la base de datos o varios de los elementos de datos almacenados en ella pueden, además o
 5 alternativamente, ubicarse de forma remota (como en un dispositivo remoto 102 o servidor del sistema 105 - no mostrado) y conectado al dispositivo móvil a través de una red de una manera conocida por los expertos en la materia.

10 Una interfaz de usuario 115 también está operativamente conectada al procesador. La interfaz puede ser uno o más dispositivos de entrada o salida, como interruptores, botones, teclas, una pantalla táctil, micrófono, etc., como se entendería en el arte de la informática electrónica. dispositivos. La interfaz de usuario 115 sirve para facilitar la captura de comandos del usuario, como
 15 comandos de encendido y apagado o información del usuario y configuraciones relacionadas con el funcionamiento del sistema 100 para el reconocimiento del usuario. Por ejemplo, en al menos una realización, la interfaz 115 puede servir para facilitar la captura de cierta información desde el (los) dispositivo(s) móvil(es) 101, como información personal del usuario para inscribirse en el sistema para
 20 crear un perfil de usuario.

El dispositivo móvil 101 también puede incluir una pantalla 140 que también está operativamente conectada al procesador 110. La pantalla incluye una pantalla o cualquier otro dispositivo de presentación que permita al sistema instruir o
 25 proporcionar información al usuario sobre las operaciones del sistema 100. para desentrañar las características discriminatorias de un usuario y la autenticación del usuario. A modo de ejemplo, la pantalla puede ser una pantalla digital tal como una pantalla de matriz de puntos u otra pantalla bidimensional.

30 A modo de ejemplo adicional, como es común en los teléfonos inteligentes como el dispositivo móvil 101, la interfaz y la pantalla pueden integrarse en una pantalla táctil. En consecuencia, la pantalla también se usa para mostrar una interfaz gráfica de usuario, que puede mostrar varios datos y proporcionar "formularios" que incluyen campos que permiten la entrada de información por parte del

usuario. Tocar la pantalla táctil en lugares correspondientes a la visualización de una interfaz gráfica de usuario permite que la persona interactúe con el dispositivo para ingresar datos, cambiar configuraciones, controlar funciones, etc. Entonces, cuando se toca la pantalla táctil, la interfaz de usuario comunica este cambio a procesador, y la configuración se puede cambiar, o la información ingresada por el usuario se puede capturar y almacenar en la memoria.

El dispositivo móvil 101 también puede incluir una cámara 145 capaz de capturar imágenes digitales. El dispositivo móvil 101 o la cámara 145 también pueden incluir uno o más emisores de luz o señal (por ejemplo, LED, no mostrados), por ejemplo, un emisor de luz visible o un emisor de luz infrarroja y similares. La cámara se puede integrar en el dispositivo móvil, como una cámara frontal o una cámara trasera que incorpore un sensor, por ejemplo, y sin limitación, un sensor CCD o CMOS. Como entenderán los expertos en la materia, la cámara 145 también puede incluir hardware adicional, como lentes, medidores de luz (por ejemplo, medidores de lux) y otras funciones de hardware y software convencionales que se pueden usar para ajustar la configuración de captura de imágenes, como zoom, enfoque, apertura, exposición, velocidad de obturación y similares. Alternativamente, la cámara puede ser externa al dispositivo móvil 101. Los expertos en la técnica comprenderán las posibles variaciones de la cámara y los emisores de luz. Además, el dispositivo móvil también puede incluir uno o más micrófonos 125 para capturar grabaciones de audio como entenderán los expertos en la materia.

La salida de audio 155 también está operativamente conectada al procesador 110. La salida de audio puede ser cualquier tipo de sistema de altavoces que esté configurado para reproducir archivos de audio electrónicos, como entenderán los expertos en la materia. La salida de audio puede estar integrada en el dispositivo móvil 101 o externa al dispositivo móvil 101.

Varios dispositivos de hardware o sensores 160 también se pueden conectar operativamente al procesador. Por ejemplo, los sensores 160 pueden incluir: un reloj integrado para realizar un seguimiento de la hora del día, etc.; un dispositivo con GPS para determinar la ubicación del dispositivo móvil; Magnetómetro de

gravedad para detectar el campo magnético de la Tierra para determinar la orientación tridimensional del dispositivo móvil; sensores de proximidad para detectar la distancia entre el dispositivo móvil y otros objetos; sensores de radiación RF para detectar los niveles de radiación RF; y otros dispositivos tales como los entenderán los expertos en la técnica.

El (los) dispositivo(s) móvil(es) 101 también comprende(n) un acelerómetro 135 y/o un giroscopio 136, que están configurados para capturar señales de movimiento del usuario 124. En al menos una realización, el acelerómetro también puede configurarse para rastrear la orientación y aceleración del dispositivo móvil. El dispositivo móvil 101 se puede ajustar (configurar) para proporcionar los valores del acelerómetro y giroscopio al procesador 110 que ejecuta los diversos módulos de software 130, incluidos, por ejemplo, el módulo de extracción de características 172, el módulo de clasificación 174 y el módulo de metaaprendizaje 175.

La interfaz de comunicación 150 también está operativamente conectada al procesador 110 y puede ser cualquier interfaz que permita la comunicación entre el dispositivo móvil 101 y los dispositivos, máquinas y/o elementos externos, incluido el servidor del sistema 105. Preferiblemente, la interfaz de comunicación incluye, entre otros, un módem, una tarjeta de interfaz de red (NIC), una interfaz de red integrada, un transmisor/receptor de radiofrecuencia (por ejemplo, Bluetooth, celular, NFC), un transmisor/receptor de comunicación satelital, un puerto de infrarrojos, una conexión USB y/o cualquier otra interfaz para conectar el dispositivo móvil a otros dispositivos informáticos y/o redes de comunicación, como redes privadas e Internet. Dichas conexiones pueden incluir una conexión por cable o una conexión inalámbrica (p. ej., usando el estándar 802.11), aunque debe entenderse que la interfaz de comunicación puede ser prácticamente cualquier interfaz que permita la comunicación hacia y desde el dispositivo móvil.

En varios puntos durante las operaciones del sistema 100 para desentrañar las características discriminatorias de un usuario y la autenticación del usuario, el dispositivo móvil 101 puede comunicarse con uno o más dispositivos informáticos, como el servidor del sistema 105 y/o el dispositivo informático

remoto 102. los dispositivos transmiten y/o reciben datos hacia y desde el dispositivo móvil 101, por lo que preferiblemente inician, mantienen y/o mejoran el funcionamiento del sistema 100, como se describirá con mayor detalle a continuación.

La figura 1D es un diagrama de bloques que ilustra una configuración ejemplar del servidor del sistema 105. El servidor del sistema 105 puede incluir un procesador 210 que está operativamente conectado a varios componentes de hardware y software que sirven para permitir la operación del sistema 100 para desentrañar las características discriminatorias de un usuario y el reconocimiento de usuarios. El procesador 210 sirve para ejecutar instrucciones para realizar varias operaciones relacionadas con el reconocimiento de usuarios, como se describirá con mayor detalle a continuación. El procesador 210 puede ser una serie de procesadores, un núcleo multiprocesador o algún otro tipo de procesador, dependiendo de la implementación particular.

En ciertas implementaciones, el procesador 210 puede acceder a una memoria 220 y/o un medio de almacenamiento 290, lo que permite que el procesador 210 reciba y ejecute 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 ordenador volátil o no volátil adecuado. Además, la memoria 220 puede ser fija o extraíble. 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, como un disco duro, una memoria flash, 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 módulos de software 230 están codificados en el almacenamiento 290 y/o en la memoria 220. Uno o más de los módulos de software 230 pueden comprender uno o más programas de software o aplicaciones que tienen un código de programa informático, o un conjunto de instrucciones ejecutadas en el procesador 210. En una realización, los módulos de software 230 pueden comprender uno o más de los módulos de software 130. Tal código de programa de computadora o instrucciones para realizar operaciones para aspectos de los sistemas y métodos descritos en este documento se pueden escribir en cualquier combinación de uno o más lenguajes de programación, como entenderán los expertos en la materia. El código del programa puede ejecutarse completamente en el servidor del sistema 105 como un paquete de software independiente, en

parte en el servidor del sistema 105 y en parte en un dispositivo informático remoto, como un dispositivo informático remoto 102 y/o dispositivo(s) móvil(es) 101 o completamente en dichos dispositivos informáticos remotos. En una o más realizaciones, como se muestra en la figura 1B, preferiblemente, entre los
5 módulos de software 230 se incluyen un módulo de extracción de características 172, un módulo de segmentación 173, un módulo de clasificación 174, un módulo de metaaprendizaje 175, un módulo de base de datos 176, un módulo de comunicación 177, y un módulo de conversión 178 que puede ser ejecutado por el procesador del servidor del sistema 210.

Además, preferiblemente almacenado en el almacenamiento 290 hay una base de datos 280. Como se describirá con mayor detalle a continuación, la base de datos 280 contiene o mantiene varios elementos y elementos de datos que se utilizan a lo largo de las diversas operaciones del sistema 100, incluidos, entre
15 otros, perfiles de usuario como se describirá con mayor detalle en este documento. Cabe señalar que, aunque la base de datos 280 se representa configurada localmente para el dispositivo informático 105, en ciertas implementaciones, la base de datos 280 o varios de los elementos de datos almacenados en ella se pueden almacenar en una memoria legible por computadora o en un medio de almacenamiento que se encuentra de forma
20 remota. y conectado al servidor del sistema 105 a través de una red (no mostrada), de una manera conocida por los expertos en la materia.

Una interfaz de comunicación 250 también está operativamente conectada al
25 procesador 210. La interfaz de comunicación 250 puede ser cualquier interfaz que permita la comunicación entre el servidor del sistema 105 y dispositivos, máquinas o elementos externos. En ciertas implementaciones, la interfaz de comunicación 250 incluye, entre otros, un módem, una tarjeta de interfaz de red (NIC), una interfaz de red integrada, un transmisor/receptor de radiofrecuencia
30 (por ejemplo, Bluetooth, celular, NFC), un satélite transmisor/receptor de comunicación, un puerto de infrarrojos, una conexión USB o cualquier otra interfaz para conectar el dispositivo informático 105 a otros dispositivos informáticos o redes de comunicación, como redes privadas e Internet. Dichas conexiones pueden incluir una conexión por cable o una conexión inalámbrica (p.

ej., utilizando el estándar 802.11), aunque debe entenderse que la interfaz de comunicación 250 puede ser prácticamente cualquier interfaz que permita la comunicación hacia y desde el procesador 210.

- 5 Las operaciones del sistema 100 y sus diversos elementos y componentes pueden apreciarse más con referencia a los métodos para desentrañar las características discriminatorias de un usuario y la autenticación del usuario usando datos de sensores de movimiento como se describe a continuación con referencia a las figuras 2, 3, 4, 5A-5D, 6A-6B, por ejemplo. Los procesos descritos
- 10 en este documento se muestran desde la perspectiva del dispositivo móvil 101 y/o el servidor del sistema 105, sin embargo, debe entenderse que los procesos pueden ser realizados, en su totalidad o en parte, por el (los) dispositivo(s) móvil(es) 101, el servidor del sistema 105 y/u otros dispositivos informáticos (por ejemplo, el dispositivo informático remoto 102) o cualquier combinación de los
- 15 anteriores. Debe apreciarse que se pueden realizar más o menos operaciones que las mostradas en las figuras y descritas en este documento. Estas operaciones también se pueden realizar en un orden diferente al descrito en este documento. También debe entenderse que uno o más de los pasos pueden ser realizados por el dispositivo móvil 101 y/o en otros dispositivos informáticos (por
- 20 ejemplo, el servidor del sistema 105 y el dispositivo informático remoto 102).

En la literatura reciente se han propuesto varios sistemas de autenticación del comportamiento del usuario (UBA) para usuarios de teléfonos inteligentes basados en sensores de movimiento. Los sistemas modernos que obtienen tasas

25 de precisión de alto nivel se basan en los principios de Aprendizaje Automático (ML) y Aprendizaje Profundo para aprender modelos discriminativos, p. "N. Neverova, C. Wolf, G. Lacey, L. Fridman, D. Chandra, B. Barbello, G. Taylor. Aprendizaje de la identidad humana a partir de patrones de movimiento. Acceso IEEE, vol. 4, págs. 1810-1820, 2016". Sin embargo, dichos modelos se evalúan

30 en conjuntos de datos recopilados de usuarios de teléfonos inteligentes, con un usuario (el propietario legítimo) por dispositivo.

La figura 2 muestra un sistema híbrido y un diagrama de flujo de proceso que muestra un sistema de identificación de usuario de teléfono inteligente estándar basado en aprendizaje automático de acuerdo con una o más realizaciones. Específicamente, la figura 2 muestra un flujo de ejecución de un sistema UBA 300 típico que puede implementarse utilizando teléfonos inteligentes. Como se muestra en la figura 2, en un sistema UBA típico 300, las señales del acelerómetro o del giroscopio se registran durante cada sesión de autenticación o registro. Luego, las señales se proporcionan como entrada a un sistema de aprendizaje automático. El sistema 300 extrae características y aprende un modelo en un conjunto de muestras de entrenamiento recopiladas durante el registro del usuario. Durante la autenticación del usuario, el modelo entrenado clasifica las señales como pertenecientes al propietario (autorizando la sesión) o como pertenecientes a un usuario diferente (rechazando la sesión). Los pasos ejemplares específicos del sistema UBA 300 se muestran a continuación:

1. Durante el registro o la autenticación del usuario, capture las señales de los sensores integrados, como el acelerómetro y el giroscopio.
2. Dentro del sistema ML, extraiga características relevantes de las señales, empleando un conjunto de técnicas de extracción de características.
3. Durante el registro, dentro del sistema ML, entrenar un modelo de clasificación sobre los vectores de características que corresponden a las señales registradas durante el registro del usuario.
4. Durante la autenticación, dentro del sistema ML, emplee el modelo de clasificación aprendido en el vector de funciones correspondiente para distinguir al usuario legítimo (propietario del teléfono inteligente) de los posibles atacantes.

En este entorno, el límite de decisión de los sistemas de ML puede verse influido por las características discriminatorias del dispositivo o la acción en lugar de las características discriminatorias del usuario. Se realizaron experimentos para probar esta hipótesis. Los resultados empíricos indican que, en realidad, es más fácil confiar en las funciones que corresponden a los dispositivos que en las funciones que corresponden a los usuarios. Este problema no se ha señalado ni abordado en la literatura anterior. Sin embargo, este problema se vuelve problemático cuando los atacantes pueden obtener un teléfono inteligente propiedad de un usuario legítimo e intentan autenticarse en una aplicación que

está protegida por un sistema UBA. Además, los atacantes podrían hacerse pasar por el usuario legítimo tras un minucioso análisis e imitación de los movimientos realizados durante la autenticación. Si el sistema ML se basa en las características más destacadas que caracterizan el dispositivo o las acciones, es probable que otorgue acceso al atacante a la aplicación. Por lo tanto, el sistema ML tendrá una mayor tasa de falsos positivos y no podrá rechazar tales ataques.

Para resolver este problema, el sistema 300 podría configurarse para pedirle al usuario que se autentique en múltiples dispositivos, usando diferentes movimientos (por ejemplo, autenticarse con la mano izquierda, mano derecha, mientras está sentado, de pie, etc.) y, con el fin de para obtener muestras negativas del mismo dispositivo, el sistema 300 podría solicitar al usuario que permita que otra persona realice varias sesiones de autenticación en su propio dispositivo. Sin embargo, todas estas son soluciones poco prácticas que conducen a un proceso de registro engorroso.

En consecuencia, aquí se proporcionan métodos y sistemas que brindan una solución práctica en dos etapas al problema intrínseco de los sistemas UBA basados en sensores de movimiento, es decir, separando las características discriminatorias del usuario de las características discriminatorias del dispositivo y la acción. En una o más realizaciones de la presente solicitud, los métodos divulgados se componen de las siguientes dos etapas principales de procesamiento:

1. Para eliminar las características que discriminan el movimiento o la acción del usuario (p. ej., deslizar el dedo, gestos), las señales de movimiento se cortan en fragmentos muy pequeños y se aplica un sistema ML en cada uno de los fragmentos individuales. Dado que la señal completa no se puede reconstruir a partir de estos fragmentos, los movimientos (acciones genéricas realizadas por el usuario) ya no se pueden identificar. Sin embargo, estos pequeños fragmentos de la señal original aún contienen características discriminatorias para el usuario y el dispositivo.

2. Para eliminar las características que discriminan el dispositivo, se aplica un conjunto de algoritmos de traducción (por ejemplo, modelos generativos como Redes Antagónicas Generativas Coherentes con el Ciclo, para Cycle-GAN cortas) para simular sesiones de autenticación en un conjunto de dispositivos predefinido. Los modelos generativos están entrenados para tomar fragmentos de señales como entrada y proporcionar como salida fragmentos similares que incluyen características de los dispositivos de nuestro conjunto predefinido. Después de infundir funciones de diferentes dispositivos en las señales de un determinado usuario, el sistema ML puede aprender qué funciones no cambian entre dispositivos. Estas son las características que ayudan a discriminar al usuario respectivo.

Mediante el uso de uno o más algoritmos de traducción, como Cycle-GAN, en la segunda etapa, se logra la traducción del comportamiento del usuario de teléfono inteligente a teléfono inteligente, lo que ayuda a enmascarar las características que describen los sensores del teléfono inteligente y revelan aquellas que dan forma al comportamiento del usuario. Una consecuencia positiva de aclarar el comportamiento legítimo del usuario es que el sistema UBA se vuelve más vigilante y es más difícil de falsificar, es decir, se reduce la tasa de falsos positivos. En una o más realizaciones, los sistemas (por ejemplo, el sistema 100) y los métodos descritos proporcionan un sistema UBA mejorado o, alternativamente, pueden incorporarse a un sistema UBA convencional para mejorar el sistema UBA existente.

Convencionalmente, los mecanismos comunes de autenticación de dispositivos móviles, como los PIN, las contraseñas gráficas y los escaneos de huellas dactilares, ofrecen una seguridad limitada. Estos mecanismos son susceptibles de adivinación (o suplantación de identidad en el caso de los escaneos de huellas dactilares) y de ataques de canal lateral, como manchas, reflejos y ataques de captura de video. Como resultado, los métodos de autenticación continua basados en señales biométricas de comportamiento están en el centro de atención tanto en el ámbito académico como en el industrial.

El primer artículo de investigación que analiza los datos del acelerómetro para reconocer la forma de andar de un usuario de dispositivo móvil es “E. Vildjiounaite, S.-M. Makela, M. Lindholm, R. Riihimaki, V. Kyllonen, J. Mantyjarvi, H. Ailisto. Biometría multimodal discreta para garantizar la privacidad y la seguridad de la información con dispositivos personales. En: Actas de la Conferencia Internacional sobre Computación Pervasiva, 2006”.

Desde entonces, la comunidad investigadora ha propuesto una variedad de sistemas UBA, tales como: “N. Clarke, S. Furnell. Autenticación avanzada de usuarios para dispositivos móviles. Informática y seguridad, vol. 26, no. 2, 2007” y “P. Campisi, E. Maiorana, M. Lo Bosco, A. Neri. Autenticación de usuarios mediante dinámica de pulsación de teclas para teléfonos móviles. Procesamiento de Señales, IET, vol .3, no. 4, 2009”, centrándose en la dinámica de las pulsaciones de teclas, y “C. Shen, T. Yu, S. Yuan, S., Y. Li, X. Guan. Análisis de rendimiento del comportamiento del sensor de movimiento para la autenticación de usuarios en teléfonos inteligentes. Sensores, vol. 16, núm. 3, págs. 345–365, 2016”, “A. Buriro, B. Crispo, F. Del Frari, K. Wrona. Hold & Sign: una nueva biometría de comportamiento para la autenticación de usuarios de teléfonos inteligentes. En: Actas de Talleres de Seguridad y Privacidad, 2016”, “G. Canfora, P. di Notte F. Mercaldo, C. A. Visaggio. Una metodología para la autenticación silenciosa y continua en entornos móviles. En: Actas de la Conferencia Internacional sobre Comercio Electrónico y Telecomunicaciones, pp. 241-265, 2016”, “N. Neverova, C. Wolf, G. Lacey, L. Fridman, D. Chandra, B. Barbellio, G. Taylor. Aprendizaje de la identidad humana a partir de patrones de movimiento. Acceso IEEE, vol. 4, pp. 1810-1820, 2016”, centrándose en técnicas de Aprendizaje Automático o Profundo.

Los métodos presentados en la literatura de investigación o las patentes no abordan el problema de las señales de movimiento que contienen características específicas de los usuarios, las acciones y los dispositivos en conjunto. Se han reportado altos niveles de rendimiento en trabajos recientes, cuando los usuarios realizan autenticaciones, cada uno en su propio dispositivo. En este entorno, no está claro si las tasas de precisión de alto nivel de los modelos de aprendizaje automático se deben a la capacidad de los modelos para discriminar entre

usuarios o entre dispositivos. Este problema ocurre porque cada usuario se autentica en su propio dispositivo y los dispositivos no se comparten entre los usuarios.

- 5 Los experimentos realizados con un conjunto de usuarios que realizan autenticaciones en un conjunto de dispositivos, de modo que cada usuario puede autenticarse en cada dispositivo, revelan que en realidad es más fácil discriminar entre dispositivos (la precisión es de alrededor del 98%) que discriminar entre usuarios (la precisión es alrededor del 93%). Esto sugiere que los sistemas UBA
10 presentados en la literatura de investigación y las patentes tienen más probabilidades de funcionar bien porque se basan en características específicas de los dispositivos en lugar de características específicas de los usuarios. Dichos sistemas son propensos a una alta tasa de falsos positivos (los atacantes están autorizados en el sistema), cuando los atacantes realizan autenticaciones en un
15 dispositivo robado al propietario.

Dado que este problema no se ha discutido en la literatura, al menos en el contexto de la identificación de usuarios basada en señales de movimiento para sensores de teléfonos inteligentes, los sistemas y métodos descritos son los
20 primeros en abordar la tarea de desentrañar las características específicas de los usuarios, acciones y dispositivos. En al menos una realización, el método comprende una o más de dos etapas/enfoques, uno que separa las características específicas de los usuarios y dispositivos de las características específicas de las acciones, y otro que separa las características específicas de
25 los usuarios de las específicas de los dispositivos.

Este último enfoque está inspirado en una investigación reciente sobre la transferencia de estilos de imagen basada en redes adversarias generativas. En
30 “I. Goodfellow, J. Pouget-Abadie, M. Mirza, B. Xu, D. Warde-Farley, S. Ozair, A. Courville, Y. Bengio. Redes generativas adversarias. En: Actas de Avances en Sistemas de Procesamiento de Información Neuronal, pp. 2672-2680, 2014”, los autores introdujeron Generative Adversarial Networks (GAN), un modelo compuesto por dos redes neuronales, un generador y un discriminador, que generan nuevos (realistas) imágenes aprendiendo la distribución de muestras de

entrenamiento a través de la minimización de la divergencia Kullback-Leibler. Se propusieron varios otros enfoques basados en GAN para mapear la distribución de un conjunto de imágenes de origen a un conjunto de imágenes de destino, es decir, realizar transferencia de estilo. Por ejemplo, métodos como “J.Y. Zhu, T. Park, P. Isola, A.A. Efros. Traducción de imagen a imagen no emparejada utilizando redes antagónicas coherentes con el ciclo. En: Actas de la Conferencia Internacional IEEE sobre Visión por Computador, pp. 2223-2232, 2017” y “J. Kim, M. Kim, H. Kang, K. Lee. U-GAT-IT: redes atencionales generativas no supervisadas con normalización de instancia de capa adaptativa para traducción de imagen a imagen. arXiv preprint arXiv:1907.10830, 2019” agrega una pérdida de consistencia de ciclo entre las distribuciones de origen y de destino. Sin embargo, estos métodos existentes son específicos para la transferencia de estilo de imagen.

En una o más realizaciones de la presente solicitud, las redes neuronales generativas profundas se adaptan a datos de señales de movimiento centrándose en transferir características de señales de datos de sensores de movimiento a señales, en el dominio del tiempo. Más específicamente, las capas convolucionales y las capas de agrupación que son componentes centrales de las redes neuronales generativas profundas se modifican para realizar las operaciones convolucionales y de agrupación, respectivamente, solo en el dominio del tiempo. Además, en al menos una realización, las GAN coherentes con el ciclo se emplean para transferir señales en una configuración de múltiples dominios (por ejemplo, una configuración de múltiples dispositivos que puede comprender 3 o más dispositivos). Por el contrario, las GAN existentes operan en el dominio de la imagen y se aplican para transferir estilo entre solo dos dominios (por ejemplo, entre imágenes naturales y pinturas).

De acuerdo con una o más realizaciones, y como se mencionó anteriormente, para separar las características discriminatorias del usuario de las características discriminatorias del dispositivo y la acción, se proporciona un método de dos etapas.

La primera etapa se basa esencialmente en el preprocesamiento de las señales, antes de entregarlas como entrada al sistema ML. El preprocesamiento consiste en dividir la señal en varios fragmentos. El número de fragmentos, su longitud, así como el intervalo utilizado para seleccionar los fragmentos son parámetros de la etapa de preprocesamiento propuesta y pueden tener un impacto directo en la precisión y el tiempo. Por ejemplo, se establece un número fijo de fragmentos y una longitud fija para cada fragmento. En este caso, el intervalo para extraer fragmentos se calcula a partir de una señal teniendo en cuenta la longitud de la señal. Las autenticaciones más rápidas producirán señales más cortas y es posible que los fragmentos se superpongan, mientras que las autenticaciones más lentas producirán señales más largas y es posible que los fragmentos no cubran toda la señal (se perderán algunas partes). Otro ejemplo es fijar el intervalo y la duración de la señal, obteniendo un número diferente de fragmentos dependiendo de la duración de la señal de entrada. Otro ejemplo más es fijar el número de fragmentos y calcular los intervalos y las longitudes correspondientes para cubrir todas las señales de entrada. Todos los casos ejemplificados (y otros casos similares) están cubiertos por el enfoque de preprocesamiento de la presente solicitud realizado por los sistemas revelados. Los fragmentos resultantes están sujetos además a la tubería de clasificación y extracción de características de un sistema UBA ejemplar, como se ilustra en la figura 3.

La figura 3 muestra un diagrama que muestra un sistema de dispositivo móvil ejemplar y un diagrama de flujo de proceso 305 para la identificación del usuario mediante la eliminación de características discriminatorias de la acción, basado en el aprendizaje automático, de acuerdo con una o más realizaciones. En una realización, el proceso puede implementarse utilizando uno o más elementos del sistema 100 (por ejemplo, el dispositivo móvil 100, solo o junto con el servidor del sistema 105). Como se muestra en la figura 3, las señales de acelerómetro o giroscopio (señales de movimiento) 310 son registradas por el dispositivo móvil 101 durante cada sesión de autenticación. Luego, el sistema (por ejemplo, el procesador del dispositivo móvil 100 y/o el servidor del sistema 105) divide las señales 310 en N fragmentos o segmentos 315 más pequeños (potencialmente superpuestos). Los fragmentos 315 se consideran muestras individuales y se proporcionan como entrada a un sistema de aprendizaje automático. Luego, el

sistema de aprendizaje automático extrae características y aprende un modelo en un conjunto de muestras de capacitación recopiladas durante el registro del usuario. Durante la autenticación del usuario, el sistema de aprendizaje automático clasifica los fragmentos 315 como pertenecientes al propietario o como pertenecientes a un usuario diferente. Se puede aplicar un enfoque de metaaprendizaje o un voto mayoritario (ponderado) sobre las etiquetas o puntajes asignados a los fragmentos (extraídos de una señal registrada durante una sesión de autenticación) para autorizar o rechazar la sesión.

- 10 Los sistemas y métodos ejemplares descritos en este documento pueden implementarse usando datos de sensores de movimiento capturados durante sesiones de autenticación implícita y/o explícita. La autenticación explícita se refiere a una sesión de autenticación en la que se solicita al usuario que realice una acción prescrita utilizando el dispositivo móvil. Por el contrario, la autenticación implícita se refiere a una sesión de autenticación de usuario que se realiza sin solicitar explícitamente al usuario que realice ninguna acción. El objetivo de dividir las señales de movimiento 310 en fragmentos 315, es decir, aplicar el procesamiento previo descrito anteriormente, es eliminar las características discriminatorias de la acción. Durante la autenticación explícita o implícita, el usuario puede realizar diferentes acciones, aunque las autenticaciones explícitas pueden presentar menor variabilidad. De hecho, en las sesiones de autenticación explícita, es probable que el usuario siempre realice los mismos pasos, por ejemplo, escanear un código QR, apuntar el teléfono inteligente hacia la cara, colocar un dedo en el escáner de huellas dactilares, etc.
- 25 Sin embargo, estos pasos se pueden realizar con una mano (izquierda o derecha) o con las dos manos, el usuario puede realizarlos sentado en una silla, de pie o caminando. En cada uno de estos casos, las señales de movimiento registradas serán diferentes. Puede aparecer un problema si el usuario realiza los pasos de autenticación con una mano durante el registro y con la otra mano durante la autenticación, ya que el modelo ML entrenado no generalizará bien dichos cambios. En esta situación, un sistema convencional rechazará al usuario legítimo, teniendo así una alta tasa de falsos negativos. La misma situación prevalece más en la autenticación de usuario implícita, es decir, mientras el usuario interactúa con alguna aplicación sensible a los datos, por ejemplo, una

aplicación bancaria. En esta configuración, no solo la forma en que se mueven las manos o la pose del usuario, por ejemplo, puede ser diferente, sino también las acciones realizadas por el usuario (gestos de toque en diferentes lugares de la pantalla, gestos de deslizamiento en diferentes direcciones, etc.). La forma más

5 directa de separar (clasificar) tales acciones es observar los cambios en las señales de movimiento a lo largo del tiempo, desde el comienzo de la grabación hasta el final. El objetivo aquí, sin embargo, es eliminar la capacidad del sistema para separar acciones. Si las señales de movimiento 310 se separan en pequeños fragmentos 315, que se tratan de forma independiente, como es el

10 enfoque implementado por una o más realizaciones del sistema divulgado para separar las características discriminatorias de un usuario de teléfono inteligente de las señales de movimiento, el sistema ML ya no tendrá la oportunidad de ver toda la señal grabada como un todo. Al no saber qué fragmento va a dónde, el sistema ML no podrá reconocer la acción, que solo se puede identificar al mirar la

15 grabación completa. Esto sucede porque volver a juntar los fragmentos en un orden diferente corresponderá a una acción diferente. Se observó que la etapa de preprocesamiento de la señal de los métodos presentes mejora la precisión del reconocimiento en un 4%, cuando los usuarios realizan un conjunto de acciones mientras entrenan el sistema ML y un conjunto diferente de acciones durante la

20 prueba. Dado que el sistema ML toma una decisión (por ejemplo, genera una etiqueta o calcula una puntuación) para cada fragmento, el sistema puede aplicar un esquema de votación o un modelo de metaaprendizaje en el conjunto de decisiones (etiquetas o puntuaciones) correspondientes a una autenticación para determinar si el usuario que realiza la autenticación es legítimo o no.

25 Es bien sabido que los sensores de hardware se pueden identificar fácilmente observando la salida producida por estos sensores, debido a defectos incorporados, como se detalla en “N. Khanna, A. K. Mikkilineni, A. F. Martone, G. N. Ali, GTC Chiu, J. P. Allebach, E. J. Delp. Una encuesta de métodos de

30 caracterización forense para dispositivos físicos. Investigación digital, vol. 3, págs. 17-28, 2006”. Por ejemplo, en “K.R. Akshatha, A. K. Karunakar, H. Anitha, U. Raghavendra, D. Shetty. Identificación de cámaras digitales usando PRNU: un enfoque basado en características. Investigación digital, vol. 19, pp. 69-77, 2016”, los autores describen un método para identificar la cámara de un teléfono

inteligente mediante el análisis de fotografías capturadas, mientras que en “A. Ferreira, L. C. Navarro, G. Pinheiro, J.A. dos Santos, A. Rocha. Atribución de impresoras láser: exploración de nuevas funciones y más allá. Internacional de Ciencias Forenses, vol. 247, pp. 105-125, 2015”, los autores presentan un enfoque para identificar un dispositivo de impresión láser mediante el análisis de las páginas impresas. De manera similar, los sensores del acelerómetro y del giroscopio pueden identificarse de manera única analizando las señales de movimiento producidas. Esto significa que las señales de movimiento registradas durante el registro y la autenticación del usuario contendrán inherentemente características discriminatorias del dispositivo. Con base en datos de sistemas anteriores, se ha determinado que es mucho más fácil identificar el teléfono inteligente según las señales de movimiento registradas (la precisión es del 98 %), que identificar a los usuarios (la precisión es del 93 %) o las acciones (la precisión es del 92%).

Si bien la división de las señales en fragmentos elimina las características discriminatorias de la acción, no alivia el problema causado por las características discriminatorias del dispositivo. El principal problema es que las características discriminatorias del dispositivo y las características discriminatorias del usuario (propietario del teléfono inteligente) se entrelazan dentro de las señales de movimiento registradas durante el registro del usuario y dentro de los fragmentos resultantes después de nuestro paso de preprocesamiento.

De acuerdo con otro aspecto destacado, los sistemas y métodos para desentrañar las características discriminatorias de un usuario de teléfono inteligente de las señales de movimiento descritas en este documento brindan una solución a este problema que no requiere que el usuario (propietario del teléfono inteligente) realice pasos adicionales además del registro estándar utilizando un solo dispositivo. Los métodos y sistemas divulgados para desentrañar las características discriminatorias de un usuario de un dispositivo de los datos del sensor de movimiento y autenticar a un usuario de los datos del sensor de movimiento están inspirados, en parte, por el éxito de las Redes adversarias generativas consistentes con el ciclo en la traducción de imagen a imagen con transferencia de estilo. Como se muestra en “J.Y. Zhu, T. Park, P.

Isola, A.A. Efros. Traducción de imagen a imagen no emparejada utilizando redes antagónicas coherentes con el ciclo. En: Actas de la Conferencia Internacional IEEE sobre Visión por Computador, pp. 2223-2232, 2017”, una Cycle-GAN puede reemplazar el estilo de una imagen con un estilo diferente, manteniendo su contenido. De manera similar, los sistemas y métodos descritos reemplazan el dispositivo utilizado para registrar una señal de movimiento con un dispositivo diferente, manteniendo las características discriminatorias del usuario. Sin embargo, como se señaló anteriormente, los métodos existentes eran específicos para la transferencia de estilo de imagen, mientras que el enfoque descrito en este documento está dirigido específicamente a transferir características de las señales de datos del sensor de movimiento de un dispositivo en particular a señales simuladas para otro dispositivo, en el dominio del tiempo.

En consecuencia, en una o más realizaciones, el sistema 100 implementa al menos un algoritmo de traducción, como Cycle-GAN, para la traducción de señal a señal, como se ilustra en la figura 4. Específicamente, la figura 4 es un diagrama de una red adversa generativa coherente con el ciclo (Cycle-GAN) ejemplar 400 para traducción de señal a señal de acuerdo con una o más realizaciones. Como se muestra en la figura 4 y de acuerdo con al menos una realización, una señal de entrada x , registrada en un dispositivo X , se traduce usando el generador G , para que parezca como si estuviera registrada en un dispositivo diferente Y . La señal se traduce de nuevo al dispositivo original X utilizando el generador F . Un discriminador D_Y discrimina entre las señales registradas en el dispositivo Y y las señales generadas por G . El generador G está optimizado para engañar al discriminador D_Y , mientras que el discriminador D_Y está optimizado para separar las muestras, de manera antagónica. Además, la Red adversa generativa (formada por los generadores G y F y el discriminador D_Y) está optimizada para reducir el error de reconstrucción calculado después de traducir la señal x al dispositivo original X . En al menos una realización, la optimización se realiza usando descenso de gradiente estocástico (o una de sus muchas variantes), un algoritmo que se usa comúnmente para optimizar redes neuronales, como entenderán los expertos en la materia. Las gradientes se calculan con respecto a una función de pérdida y se propagan hacia atrás a través de la red neuronal utilizando la regla de la cadena, como entenderán los

expertos en la materia. En una o más realizaciones, la optimización de las redes neuronales se puede realizar utilizando algoritmos evolutivos. Sin embargo, debe entenderse que los métodos divulgados no se limitan a la optimización por descenso de gradiente o algoritmos evolutivos.

- 5 Agregar el error de reconstrucción a la función de pérdida general asegura la consistencia del ciclo. Además de traducir del dispositivo X al dispositivo Y, Cycle-GAN se entrena simultáneamente para transferir del dispositivo Y al dispositivo X. Por lo tanto, al final, los sistemas y métodos descritos traducen las señales en ambas direcciones. En una o más realizaciones, la función de pérdida utilizada para entrenar la Cycle-GAN para la traducción de señal a señal en ambas
- 10 direcciones es:

$$\mathcal{L}_{\text{ciclo-GAN}}(G, F, D_X, D_Y, x, y) = \mathcal{L}_{\text{GAN}}(G, D_Y, x, y) + \mathcal{L}_{\text{GAN}}(F, D_X, x, y) + \lambda \cdot \mathcal{L}_{\text{ciclo}}(G, F, x, y),$$

- G y F son generadores;
- 15 • D_X y D_Y son discriminadores;
- x y y son señales de movimiento (fragmentos) del dispositivo X y del dispositivo Y, respectivamente;
- λ es un parámetro que controla la importancia de la consistencia del ciclo con respecto a la pérdida de GAN;
- 20 • $\mathcal{L}_{\text{GAN}}(G, D_Y, x, y) = E_{y \sim P_{\text{datos}}(y)} [\log(D_Y(y))] + E_{x \sim P_{\text{datos}}(x)} [\log(1 - D_Y(G(x)))]$ es la pérdida de entropía cruzada que corresponde a la traducción del dispositivo X al dispositivo Y, donde $E[\blacksquare]$ es el valor esperado y $P_{\text{datos}}(\blacksquare)$ es la distribución de probabilidad de las muestras de datos;
- $\mathcal{L}_{\text{GAN}}(F, D_X, x, y) = E_{x \sim P_{\text{datos}}(x)} [\log(D_X(x))] + E_{y \sim P_{\text{datos}}(y)} [\log(1 - D_X(F(y)))]$ es
- 25 la pérdida de entropía cruzada que corresponde a la traslación del dispositivo Y al dispositivo X;
- $\mathcal{L}_{\text{ciclo}}(G, F, x, y) = E_{x \sim P_{\text{datos}}(x)} [\|F(G(x)) - x\|_1] + E_{y \sim P_{\text{datos}}(y)} [\|G(F(y)) - y\|_1]$ es la suma de las pérdidas de consistencia de ciclo para ambas traslaciones, donde $\|\blacksquare\|_1$ es la norma l_1 .

30

Además o alternativamente al Ciclo GAN, el modelo U-GAT-IT presentado en “J. Kim, M. Kim, H. Kang, K. Lee. U-GAT-IT: redes atencionales generativas no supervisadas con normalización de instancia de capa adaptativa para traducción de imagen a imagen. arXiv preprint arXiv:1907.10830, 2019” se puede incorporar

a los sistemas y métodos actuales para la traducción de señal a señal. El modelo U-GAT-IT incorpora módulos de atención, tanto en el generador como en el discriminador, y una función de normalización (Normalización de Instancia de Capa Adaptativa), con el fin de mejorar la traducción del dominio de origen al dominio de destino. Los mapas de atención se obtienen con un clasificador auxiliar, mientras que los parámetros de la función de normalización se aprenden durante el entrenamiento. En al menos una realización, la función de pérdida utilizada para entrenar U-GAT-IT es:

$$\mathcal{L}_{\text{U-GAT-IT}}(G, F, D_X, D_Y, x, y) = \lambda_1 \cdot (\mathcal{L}_{\text{GAN}}(G, D_Y, x, y) + \mathcal{L}_{\text{GAN}}(F, D_X, x, y)) + \\ + \lambda_2 \cdot \mathcal{L}_{\text{ciclo}}(G, F, x, y) + \lambda_3 \cdot \mathcal{L}_{\text{identidad}}(G, F, x, y) + \lambda_4 \cdot \mathcal{L}_{\text{CAM}}(G, F, D_X, D_Y, x, y)$$

dónde:

- G y F son generadores;
- D_X y D_Y son discriminadores;
- x y y son señales de movimiento (fragmentos) del dispositivo X y del dispositivo Y , respectivamente;
- λ_1 , λ_2 , λ_3 y λ_4 son parámetros que controlan la importancia de los diversos componentes de pérdida;
- $\mathcal{L}_{\text{GAN}}(G, D_Y, x, y) = E_{y \sim P_{\text{datos}}(y)} [(D_Y(y))^2] + E_{x \sim P_{\text{datos}}(x)} [(1 - D_Y(G(x)))^2]$ es la pérdida por mínimos cuadrados que corresponde a la traslación del dispositivo X al dispositivo Y ;

$\mathcal{L}_{\text{GAN}}(f, D_x, x, y) = E_{x \sim P_{\text{datos}}(x)} [(D_x(x))^2] + E_{y \sim P_{\text{datos}}(y)} [(1 - D_x(F(y)))^2]$ es la pérdida por mínimos cuadrados que corresponde a la traslación del dispositivo Y al dispositivo X ;

5 $\mathcal{L}_{\text{ciclo}}(G, F, x, y) = E_{x \sim P_{\text{datos}}(x)} [\|F(G(x)) - x\|^1] + E_{y \sim P_{\text{datos}}(y)} [\|G(F(y)) - y\|^1]$ es la suma de las pérdidas de consistencia de ciclo para ambas traducciones y $\|\cdot\|^1$ es la norma l_1 ;

$\mathcal{L}_{\text{identidad}}(G, F, x, y) = E_{y \sim P_{\text{datos}}(y)} [\|G(y) - y\|^1] + E_{x \sim P_{\text{datos}}(x)} [\|F(x) - x\|^1]$ es la suma de las pérdidas de identidad que aseguran que las distribuciones de amplitud de las señales de entrada y salida sean similares;

10 $\mathcal{L}_{\text{CAM}}(G, F, D_x, D_y, x, y) = E_{y \sim P_{\text{datos}}(y)} [(D_y(y))^2] + E_{x \sim P_{\text{datos}}(x)} [(1 - D_y(G(x)))^2] + E_{x \sim P_{\text{datos}}(x)} [(D_x(x))^2] + E_{y \sim P_{\text{datos}}(y)} [(1 - D_x(F(y)))^2]$ es la suma de las pérdidas por mínimos cuadrados que introducen los mapas de atención.

En una o más realizaciones, para obtener resultados de transferencia que se
 15 generalicen a través de múltiples dispositivos, se usan varios modelos Cycle-GAN (o U-GAT-IT) para transferir señales entre varios pares de dispositivos. En al menos una realización, se establece un número fijo de teléfonos inteligentes T y se recopilan señales de movimiento de cada uno de los dispositivos T . En una o más realizaciones, se establece un número fijo de usuarios que realizan el
 20 registro en cada uno de los dispositivos T . La recopilación de datos se realiza antes de que el sistema UBA se implemente en producción, es decir, nunca se solicita a los usuarios finales que realicen registros en los dispositivos T , lo que sería inviable. El número de Cycle-GAN entrenadas es T , de modo que cada Cycle-GAN aprende a traducir las señales de un dispositivo en particular a todos
 25 los demás dispositivos y viceversa, como se ilustra en las figuras 5A-5D, que se analizan con más detalle a continuación.

Un objetivo de los sistemas y métodos descritos en el presente documento es obtener modelos Cycle-GAN genéricos que puedan traducir una señal capturada en algún dispositivo original a uno de los dispositivos T del conjunto, independientemente del dispositivo original. En al menos una realización, se puede lograr el mismo alcance usando diferentes arquitecturas GAN, varias profundidades de redes, tasas de aprendizaje o algoritmos de optimización. La capacidad de generalización se asegura aprendiendo a traducir de múltiples dispositivos a uno solo en lugar de solo aprender a traducir de un dispositivo a otro. Por lo tanto, los algoritmos de traducción (por ejemplo, Cycle-GAN) de las realizaciones descritas se pueden aplicar para traducir una señal capturada en el dispositivo de algún usuario a uno de los dispositivos T del conjunto, sin conocer al usuario ni tener información sobre el dispositivo que él/ella. ella está usando, durante el entrenamiento de los algoritmos de traducción (por ejemplo, modelos Cycle-GAN). Cada vez que la señal original se traduce a uno de los dispositivos T, las características del dispositivo del propietario se reemplazan con las características de un determinado dispositivo del conjunto de dispositivos T, manteniendo las características específicas del usuario. Al alimentar tanto las señales originales como las traducidas al sistema ML de acuerdo con una o más realizaciones del sistema para desentrañar las características discriminatorias de un usuario de un dispositivo de los datos del sensor de movimiento, el sistema ML ya no puede aprender características discriminatorias específicas. al dispositivo original. Esto sucede porque el sistema ML está configurado para colocar (clasificar) señales originales y traducidas en la misma clase, y la forma más relevante de obtener dicho límite de decisión es observar las características que son discriminatorias para el usuario.

Realizaciones Ejemplares

Las realizaciones ejemplares de los presentes sistemas y métodos se analizan con más detalle a continuación con referencia a las figuras 5A-5D, 6A-6B y 1A-1D, junto con aplicaciones prácticas de las técnicas y otros escenarios prácticos donde los sistemas y métodos para desentrañar las características discriminatorias de un usuario de un dispositivo y la autenticación basada en

señales de movimiento capturadas por los sensores de movimiento del dispositivo móvil se puede aplicar.

En una o más realizaciones, los métodos descritos en el presente documento proporcionan una canalización de ejecución de UBA modificada. La canalización

5 de ejecución UBA modificada es capaz de separar las características discriminatorias del usuario de las características discriminatorias de las acciones y los dispositivos, como se ejemplifica en las figuras 5A-5D. Las figuras 5A-5D muestran un sistema y diagrama de flujo para desentrañar las características discriminatorias de un usuario de un dispositivo móvil de los datos del sensor de movimiento y autenticar a un usuario de acuerdo con una o más realizaciones. Los pasos en el diagrama de flujo de las figuras 5A-5D se puede realizar utilizando el sistema de ejemplo para desentrañar las características discriminatorias de un usuario de un dispositivo de los datos del sensor de movimiento que incluyen, por ejemplo, el dispositivo móvil 101 y/o el servidor del sistema 105 del sistema 100. Los pasos en el diagrama de flujo de las figuras 5A-5D se detallan a continuación:

1. Durante el registro o la autenticación del usuario, las señales de movimiento 310 son capturadas por el dispositivo móvil 101 desde los sensores integrados, como un acelerómetro y un giroscopio.
2. Las señales de movimiento 310 se dividen en fragmentos más pequeños 315.
3. Usando un conjunto de Cycle-GAN entrenadas 400, se generan nuevas señales 500 (señales traducidas), simulando la sesión de autenticación del usuario en otros dispositivos.
- 25 4. Dentro del sistema ML 505, las características relevantes se extraen de los fragmentos de señal originales y traducidos para formar vectores de características, empleando un conjunto de técnicas de extracción de características.
5. Durante el registro, dentro del sistema ML 505, se entrena un modelo de clasificación en los vectores de características que corresponden a los fragmentos de señal 500 grabados y traducidos.
- 30 6. Durante la autenticación, dentro del sistema ML 505, el modelo de clasificación aprendido se emplea en los vectores de características que corresponden a los fragmentos de señal registrados y traducidos.

7. Durante la autenticación, para distinguir al usuario legítimo (propietario del teléfono inteligente) de posibles atacantes, se emplea un esquema de votación o un modelo de metaaprendizaje sobre las puntuaciones o etiquetas obtenidas para los fragmentos grabados y traducidos que corresponden a una sesión de autenticación.

Estos pasos y otros se describen y ejemplifican adicionalmente en los siguientes métodos ejemplares de las figuras 6A-6B.

- 10 De acuerdo con una o más realizaciones, la figura 6A revela un diagrama de bloques de alto nivel que muestra un flujo de cálculo para desentrañar las características discriminatorias de un usuario de un dispositivo de los datos del sensor de movimiento. En una o más realizaciones, el método de la figura 6A puede ser realizado por los presentes sistemas, como el sistema ejemplar 100 de
- 15 la figura 1A. Si bien muchos de los siguientes pasos se describen como realizados por el dispositivo móvil 101 (figura 1A), en ciertas realizaciones, uno o más de los siguientes pasos pueden ser realizados por el servidor del sistema (servidor back-end) 105, que es en comunicación con el dispositivo móvil 101.
- 20 Con referencia a la figura 5A y las figuras 1A-1D, el proceso comienza en el paso S105, donde se configura el procesador del dispositivo móvil 101, mediante la ejecución de uno o más módulos de software (p. ej., el módulo de interfaz de usuario 170), para hacer que al menos un sensor de movimiento (p. ej., acelerómetro 135, giroscopio 136) del dispositivo móvil para capturar datos del
- 25 usuario en forma de una o más señales de movimiento. En una o más realizaciones, las señales de movimiento son señales multieje que corresponden al movimiento físico o las interacciones del usuario con el dispositivo recopiladas durante un dominio de tiempo específico del al menos un sensor de movimiento del dispositivo móvil. El movimiento físico del usuario puede ser en forma de un
- 30 "gesto" (p. ej., tocar con el dedo o deslizar el dedo) u otra interacción física con el dispositivo móvil (p. ej., levantar el dispositivo móvil). Por ejemplo, los sensores de movimiento pueden recolectar o capturar señales de movimiento correspondientes al usuario que escribe su firma en el aire (una interacción "explícita") o al usuario tocando su teléfono (una interacción "implícita"). Como

tales, las señales de movimiento contienen características que son específicas (discriminatorias) del usuario, la acción realizada por el usuario (por ejemplo, un gesto) y el dispositivo móvil en particular.

- 5 En una o más realizaciones, la recopilación o captura de señales de movimiento por parte de los sensores de movimiento del dispositivo móvil se puede realizar durante una o más ventanas de tiempo predeterminadas, que preferiblemente son ventanas de tiempo cortas. Por ejemplo, en al menos una realización, la ventana de tiempo puede ser de aproximadamente 2 segundos. En al menos una
- 10 realización, como durante el registro de un usuario, el dispositivo móvil puede configurarse para recopilar (capturar) señales de movimiento del usuario indicándole que realice un gesto particular o una interacción explícita. Además, en al menos una realización, el dispositivo móvil puede configurarse para recopilar señales de movimiento sin avisar al usuario, de modo que las señales de
- 15 movimiento recopiladas representen gestos implícitos o interacciones del usuario con el dispositivo móvil. En una o más realizaciones, el procesador del dispositivo móvil 101 puede configurarse ejecutando uno o más módulos de software (por ejemplo, el módulo de base de datos 176) para guardar las señales de movimiento capturadas en la base de datos 185 del dispositivo móvil o,
- 20 alternativamente, las señales de movimiento capturadas se pueden guardar en la base de datos 280 del servidor back-end 105.

En el paso S110, el procesador del dispositivo móvil se configura, mediante la ejecución de uno o más módulos de software (por ejemplo, el módulo de

- 25 segmentación 173), para dividir en segmentos la una o más señales de movimiento capturadas. Específicamente, las señales de movimiento capturadas se dividen en un número N de fragmentos o segmentos más pequeños. Como se discutió anteriormente, los sistemas y métodos divulgados están configurados, en parte, para abordar el problema de distinguir, en señales de movimiento,
- 30 características que son específicas o únicas para un usuario particular y características que discriminan la acción realizada por el usuario. Como tal, al dividir las señales de movimiento en segmentos, se eliminan las características discriminatorias de las acciones realizadas por el usuario. En una o más realizaciones, el paso de dividir una o más señales de movimiento capturadas en

segmentos comprende dividir cada señal de movimiento en un número fijo de segmentos, donde cada segmento tiene una longitud fija. En una o más realizaciones, al menos algunos de los segmentos o fragmentos son segmentos o fragmentos superpuestos.

5

Continuando con la referencia a la figura 5A, en el paso S115, el procesador del dispositivo móvil se configura ejecutando uno o más módulos de software 530 (por ejemplo, el módulo de conversión 178), para convertir los segmentos en segmentos traducidos utilizando uno o más módulos entrenados. algoritmos de traducción, como Cycle-consistent Generative Adversarial Networks (Cycle-GAN). Como se discutió anteriormente, los presentes sistemas y métodos están configurados, en parte, para abordar el problema de distinguir, en las señales de movimiento, entre características que son específicas o únicas para un usuario en particular y características que discriminan el dispositivo móvil del usuario. . Al convertir los segmentos en segmentos traducidos usando Cycle-GAN, el presente método elimina de manera efectiva las características discriminatorias del dispositivo móvil de la(s) señal(es) de datos de movimiento recopilada(s) proporcionada(s) al modelo ML.

10

15

20

25

30

Más específicamente, de acuerdo con una o más realizaciones, los fragmentos/segmentos se consideran muestras individuales, y estos fragmentos/segmentos se proporcionan como entrada para uno o más algoritmos de traducción (por ejemplo, Cycle-GAN). En una o más realizaciones que utilizan Cycle-GAN, cada Cycle-GAN se entrena fuera de línea en un conjunto de datos separado de señales de movimiento recopiladas en un conjunto predefinido, T, de diferentes dispositivos. Dado un segmento como entrada, Cycle-GAN convierte cada segmento en un segmento traducido, de modo que el segmento traducido corresponde a un segmento tal como se habría grabado en un dispositivo del conjunto predefinido de dispositivos T que es diferente del dispositivo móvil. del usuario En otras palabras, los segmentos traducidos comprenden una o más señales de movimiento sintéticas que simulan señales de movimiento que se originan en otro dispositivo. Por ejemplo, el segmento de entrada de la señal de movimiento x grabada en un dispositivo X se traduce mediante una Cycle-GAN (generador) G, para que parezca que se grabó en un dispositivo Y diferente.

Cada vez que se traduce un segmento original utilizando uno de los Cycle-GAN, las funciones del propio dispositivo del usuario se reemplazan con las funciones de un determinado dispositivo del conjunto predefinido de dispositivos T, manteniendo las funciones específicas del usuario. Como se mencionó anteriormente, un objetivo del proceso es separar las características en las señales de movimiento que son específicas (discriminatorias) del usuario y aquellas características que son meramente específicas (discriminatorias) de un dispositivo utilizado por el usuario. Por lo tanto, de acuerdo con al menos una realización, para obtener resultados específicos para el usuario de manera que el usuario pueda identificarse a través de múltiples dispositivos, se utilizan varios modelos Cycle-GAN (o U-GAT-IT u otros algoritmos de traducción) para traducir el segmento entre varios dispositivos. En una o más realizaciones, se establece un número fijo de dispositivos (por ejemplo, teléfonos inteligentes) T y se recopilan segmentos de señales de movimiento de cada uno de los dispositivos T. También se establece un número fijo de usuarios que realizan el registro en cada uno de los dispositivos T. Como tal, se entrena un número determinado de Cycle-GAN de modo que cada Cycle-GAN aprenda a traducir los segmentos de un dispositivo en particular a todos los demás dispositivos del conjunto y viceversa, como se ilustra en la figura 4A. Por lo tanto, de acuerdo con al menos una realización, el presente sistema da como resultado modelos Cycle-GAN genéricos que pueden traducir una señal capturada en algún dispositivo original a otro dispositivo en un conjunto predefinido de dispositivos T, independientemente del dispositivo original.

Se observa que, en al menos una realización, este paso se puede lograr usando diferentes arquitecturas GAN, varias profundidades de redes, tasas de aprendizaje o algoritmos de optimización. La capacidad de generalización se asegura aprendiendo a traducir de varios dispositivos a uno solo en lugar de solo aprender a traducir de un dispositivo a otro. Así, las Cycle-GAN se pueden aplicar para traducir una señal capturada en el dispositivo de un usuario a otro dispositivo del conjunto de dispositivos T sin conocer al usuario ni tener información sobre el dispositivo que está utilizando, durante el entrenamiento de la Cycle-GAN. Cada vez que los segmentos originales se traducen a uno de los

dispositivos T del conjunto, las funciones del dispositivo del usuario se reemplazan con las funciones de otro dispositivo del conjunto de dispositivos T, manteniendo las funciones específicas del usuario.

- 5 En una o más realizaciones del paso S115, una vez que se traducen los segmentos de entrada, se configura el procesador del dispositivo móvil, mediante la ejecución de uno o más módulos de software (por ejemplo, el módulo de conversión 178), para volver a traducir los segmentos. Por ejemplo, como se mencionó en el ejemplo anterior, el segmento de entrada de la señal de
- 10 movimiento x grabada en un dispositivo X se traduce utilizando una Cycle-GAN (generador) G, para que parezca que se grabó en un dispositivo Y diferente. El segmento traducido luego se vuelve a traducir al dispositivo original X usando una Cycle-GAN (generador) F. De acuerdo con al menos una realización, un discriminador D_Y luego discrimina entre las señales registradas en el dispositivo Y
- 15 y las señales generadas por Cycle-GAN (generador) G. El generador G está optimizado para engañar al discriminador D_Y , mientras que el discriminador D_Y está optimizado para separar las muestras, de manera antagónica. Además, en al menos una realización, todo el sistema está optimizado para reducir el error de reconstrucción calculado después de traducir la señal x de vuelta al dispositivo
- 20 original X. Agregar el error de reconstrucción a la función de pérdida general asegura la consistencia del ciclo.

Continuando con la referencia a la figura 5A, en el paso S120, el procesador del dispositivo móvil se configura mediante la ejecución de uno o más módulos de

25 software (por ejemplo, el módulo de extracción de características 172), para proporcionar los segmentos y los segmentos traducidos a un dispositivo de aprendizaje automático. sistema. Los segmentos y los segmentos traducidos proporcionados como entradas al sistema de aprendizaje automático se consideran muestras individuales.

30

En el paso S125, el procesador del dispositivo móvil se configura luego, mediante la ejecución de uno o más módulos de software, para extraer características discriminatorias del usuario de los segmentos y segmentos traducidos utilizando el sistema de aprendizaje automático que aplica uno o más algoritmos de extracción de características. Por ejemplo, en una o más realizaciones durante un proceso de registro de usuario, el procesador está configurado para extraer características relevantes de los segmentos y los segmentos traducidos para formar vectores de características usando una o más técnicas de extracción de características. En el paso S127, el procesador se configura para emplear y entrenar un modelo de clasificación aprendido sobre los vectores de características que corresponden a los segmentos y los segmentos traducidos. En al menos una realización, el sistema de aprendizaje automático puede ser una red neuronal profunda de extremo a extremo, que comprende pasos de extracción de características (S125) y clasificación (S127). En una o más realizaciones, el sistema de aprendizaje automático puede estar formado por dos componentes (un extractor de características y un clasificador) o tres componentes (un extractor de características, un método de selección de características, no mostrado, y un clasificador). En cualquiera de las realizaciones, está presente un componente entrenable, a saber, una red neuronal profunda o un clasificador. El componente entrenable generalmente se entrena en un conjunto de datos de muestras (fragmentos de señales de movimiento) y etiquetas correspondientes (identificadores de usuario) mediante la aplicación de un algoritmo de optimización, por ejemplo, descenso de gradiente, con respecto a una función de pérdida que expresa qué tan bien es el componente entrenable. capaz de predecir las etiquetas correctas para las muestras de datos de entrenamiento (segmentos originales o traducidos recopilados durante el registro del usuario), como entenderían los expertos en la materia. El objetivo del algoritmo de optimización es minimizar la función de pérdida, es decir, mejorar la capacidad predictiva del componente entrenable. En el paso S130, el método finaliza.

La figura 6B revela un diagrama de bloques de alto nivel que muestra un flujo de cálculo para autenticar a un usuario en un dispositivo móvil a partir de datos de sensores de movimiento de acuerdo con al menos una realización. Con

referencia ahora a la figura 5B, el método comienza en los pasos S105. Los pasos S105 - S120, como se muestra en la figura 6B, son los mismos pasos descritos anteriormente con respecto al método que se muestra en la figura 6A. Específicamente, en el paso S105, el dispositivo móvil captura una o más señales de movimiento de un usuario, y en el paso S110, la una o más señales de movimiento capturadas se dividen en segmentos. En el paso S115, los segmentos se convierten en segmentos traducidos usando uno o más algoritmos de traducción entrenados (por ejemplo, Cycle-GAN), y en el paso S120, los segmentos y los segmentos traducidos se proporcionan a un sistema de aprendizaje automático.

Con referencia continua a la figura 5B y las figuras 1A-1D, después del paso S120, en el paso S135 se configura el procesador del dispositivo móvil, mediante la ejecución de uno o más módulos de software (por ejemplo, el módulo de clasificación 174), para clasificar (por ejemplo, puntuar, asignar probabilidades de clase a) los segmentos y segmentos traducidos. Más específicamente, en una o más realizaciones, los vectores de características que representan segmentos y segmentos traducidos se analizan y califican. En una o más realizaciones, los segmentos y los segmentos traducidos pueden corresponder a una sesión de autenticación de modo que los segmentos y los segmentos traducidos se puntúan de acuerdo con un modelo de aprendizaje automático, por ejemplo, un clasificador o una red neuronal profunda, que se entrenó previamente, en el paso S127 en la figura 6A, sobre los datos recopilados durante el registro del usuario.

En el paso S140, el dispositivo móvil se configura mediante la ejecución de uno o más módulos de software 130 (p. ej., el módulo de metaaprendizaje 175), para aplicar un esquema de votación o un modelo de metaaprendizaje sobre las puntuaciones (p. ej., probabilidades de clase) asignadas a los segmentos y segmentos traducidos obtenidos durante una sesión de autenticación. Al aplicar el esquema de votación o el modelo de metaaprendizaje, el dispositivo móvil se configura para proporcionar una decisión unánime para autorizar o rechazar al usuario. En una o más realizaciones, la decisión unánime de la sesión se basa en un esquema de votación o modelo de metaaprendizaje que se aplica a las puntuaciones de todos los segmentos y segmentos traducidos.

Finalmente, en el paso S145 se configura el dispositivo móvil, mediante la ejecución de uno o más módulos de software (por ejemplo, el módulo de metaaprendizaje 175), para determinar en base al paso de votación o metaaprendizaje si el usuario es un usuario autorizado. Como se mencionó

5 anteriormente, los segmentos y los segmentos traducidos se puntúan de acuerdo con las probabilidades de clase dadas como salida por un modelo de aprendizaje automático que se entrenó, durante el registro, para identificar a un usuario conocido. Como tal, según el esquema de votación o el metal-aprendiz aplicado a las puntuaciones de los segmentos respectivos y los segmentos traducidos, el

10 procesador está configurado para determinar si los segmentos y los segmentos traducidos pertenecen o no a un usuario (autorizado) en particular y, por lo tanto, en última instancia determinar si el usuario es un usuario autorizado o un usuario no autorizado. El proceso de autenticación descrito en este documento se refiere a la autenticación uno a uno (verificación del usuario). En el paso S150, finaliza el

15 método para autenticar a un usuario basado en los datos del sensor de movimiento.

Resultados experimentales

20 En esta sección, los resultados experimentales obtenidos con el método de desentrañado descrito en este documento se presentan de acuerdo con una o más realizaciones. Se usaron dos conjuntos de datos diferentes en los siguientes experimentos. El primer conjunto de datos (en lo sucesivo, la base de datos 5x5) consta de señales registradas por el acelerómetro y el giroscopio de 5 teléfonos

25 inteligentes, cuando las utilizan 5 personas para realizar autenticaciones. Se pidió a los individuos que variaran la posición durante la autenticación (es decir, ponerse de pie o sentarse y usar la mano derecha o la izquierda), realizando así diferentes acciones genéricas. En cada posición, se capturaron señales de 50 autenticaciones, lo que significa que cada individuo realizó un total de 1000

30 autenticaciones en cada uno de los 5 teléfonos inteligentes, es decir, el número total de sesiones es 5000. El segundo conjunto de datos (en adelante, la base de datos 3x3) se formó con las mismas variaciones posicionales que en el primero, pero con 3 personas diferentes y 3 teléfonos inteligentes diferentes.

Las señales de cada base de datos se dividieron en 25 fragmentos en la fase de preprocesamiento. Los fragmentos de señal resultantes del conjunto de datos 5x5 se utilizan para entrenar 5 Cycle-GAN con el fin de traducir señales hacia y desde los 5 dispositivos. Luego, cada uno de los fragmentos de señal obtenidos de la base de datos 3x3 se alimentan a las GAN entrenadas obteniendo, de esta manera, un conjunto de señales completamente nuevo. Estas nuevas señales (traducidas) se dividen a su vez en dos subconjuntos: uno que se usa para entrenar y el otro que se usa para probar un sistema ML para la identificación del usuario basado en señales de movimiento.

Es bien sabido que el entrenamiento GAN es altamente inestable y difícil, porque se requiere el GAN para encontrar un equilibrio de Nash de un juego minimax no convexo con parámetros dimensionales altos. Sin embargo, en estos experimentos se observó un descenso monótono de la función de pérdida para las redes generativas, sustentando la idea de que se logró un punto de equilibrio.

Al dividir las señales en fragmentos, se capturaron las características discriminatorias del usuario y se minimizó la importancia de los movimientos (acciones). Una prueba clara es que al alimentar los fragmentos de señal (sin aplicar GAN) en el sistema ML, se observó un aumento de precisión del 4 % en el reconocimiento del usuario. La traducción del comportamiento del usuario en diferentes dispositivos móviles (mediante la aplicación de GAN) condujo a un aumento adicional en la precisión del reconocimiento del usuario en otro 3% (en relación con la precisión obtenida al usar solo los fragmentos de señal). Por lo tanto, se puede concluir que a través de la simulación de características de varios dispositivos, se obtuvo un sistema ML que es más robusto e invariable a las características del dispositivo.

Junto con el crecimiento de la cantidad de dispositivos móviles, la frecuencia de los ataques ha aumentado significativamente. Por lo tanto, en los últimos años se han propuesto varios algoritmos de análisis del comportamiento del usuario, incluidos los sistemas basados en señales capturadas por sensores de movimiento durante la autenticación del usuario. Un problema importante al que

se enfrentan los algoritmos basados en datos de sensores de movimiento en la actualidad es que es muy difícil separar las características específicas de los usuarios de las específicas de las acciones y los dispositivos. Los sistemas y métodos de la presente solicitud abordan este problema dividiendo las señales de movimiento en fragmentos y utilizando algoritmos de traducción (por ejemplo, Cycle-GAN) para traducir las señales a otros dispositivos, sin necesidad de realizar ningún cambio en el proceso de registro del usuario.

De hecho, dividir las señales en partes más pequeñas ayuda a reducir la influencia de las acciones (realizadas por el usuario) sobre el límite de decisión del sistema ML, lo que aumenta la precisión de la identificación del usuario en un 4 %, como se muestra en los ejemplos anteriores. Además, es bien sabido que los sensores de diferentes dispositivos son diferentes debido al proceso de fabricación, incluso si los dispositivos son de la misma marca y modelo y salen de la misma línea de producción. Este hecho conduce a una importante influencia de los sensores del dispositivo móvil sobre el límite de decisión del sistema ML para la identificación del usuario. De acuerdo con una o más realizaciones, los sistemas y métodos descritos en este documento, que utilizan GAN, simulan autenticaciones de múltiples dispositivos en función de señales de movimiento grabadas de un dispositivo arbitrario, disminuyen la influencia de los dispositivos móviles sobre el sistema ML y aumentan la influencia de las características que son específicas para el usuario. Los sistemas y métodos divulgados mejoran aún más la precisión del sistema ML en aproximadamente un 3%. En consecuencia, en general, en una o más realizaciones, los presentes sistemas y métodos pueden aumentar el rendimiento en un 7%, reduciendo las tasas tanto de falsos positivos como de falsos negativos.

Los sistemas y métodos ejemplares para desentrañar las características discriminatorias de un usuario de un dispositivo de las señales de movimiento y para autenticar a un usuario en un dispositivo móvil de las señales de movimiento se establecen en los siguientes ítems:

Ítem 1. Un método implementado por computadora para desentrañar las características discriminatorias de un usuario de un dispositivo de las señales de

movimiento capturadas por un dispositivo móvil que tiene uno o más sensores de movimiento, un medio de almacenamiento, instrucciones almacenadas en el medio de almacenamiento y un procesador configurado mediante la ejecución de las instrucciones, que comprenden:

5

dividir, con el procesador, cada señal de movimiento capturada en segmentos;

convertir, con el procesador usando uno o más algoritmos de traducción entrenados, los segmentos en segmentos traducidos;

10

proporcionar, con el procesador, los segmentos y los segmentos traducidos a un sistema de aprendizaje automático; y

extraer, con el procesador usando el sistema de aprendizaje automático que aplica uno o más algoritmos de extracción de características, características discriminatorias del usuario de los segmentos y segmentos traducidos.

15

Ítem 2. El método del ítem 1, en el que las características discriminatorias del usuario se utilizan para identificar al usuario en el uso futuro del dispositivo por parte del usuario.

20

Ítem 3. El método de los ítems anteriores, en el que uno o más sensores de movimiento comprenden al menos uno de un giroscopio y un acelerómetro.

25

Ítem 4. El método de los ítems anteriores, en donde las una o más señales de movimiento corresponden a una o más interacciones entre el usuario y el dispositivo móvil.

Ítem 5. El método de los ítems anteriores, en donde las señales de movimiento incluyen características discriminatorias del usuario, características discriminatorias de acciones realizadas por el usuario y características discriminatorias del dispositivo móvil.

30

Ítem 6. El método del ítem 5, en el que el paso de dividir una o más señales de movimiento capturadas en segmentos elimina las características discriminatorias de las acciones realizadas por el usuario.

5

Ítem 7. El método del ítem 5, donde el paso de convertir los segmentos en los segmentos traducidos elimina las características discriminatorias del dispositivo móvil.

10 Ítem 8. El método de los ítems anteriores, en donde uno o más algoritmos de traducción entrenados comprenden una o más Redes adversarias generativas consistentes con el ciclo (Cycle-GAN), y en donde los segmentos traducidos comprenden señales de movimiento sintéticas que simulan señales de movimiento que se originan en otro dispositivo.

15

Ítem 9. El método de los ítems anteriores, donde el paso de dividir una o más señales de movimiento capturadas en segmentos comprende dividir cada señal de movimiento en un número fijo de segmentos, donde cada segmento tiene una longitud fija.

20

Ítem 10. Un método implementado por computadora para autenticar a un usuario en un dispositivo móvil a partir de señales de movimiento capturadas por un dispositivo móvil que tiene uno o más sensores de movimiento, un medio de almacenamiento, instrucciones almacenadas en el medio de almacenamiento y
25 un procesador configurado mediante la ejecución de las instrucciones. que comprende:

dividir, con el procesador, la una o más señales de movimiento capturadas en segmentos;

30 convertir, con el procesador usando uno o más algoritmos de traducción entrenados, los segmentos en segmentos traducidos;

- proporcionar, con el procesador, los segmentos y los segmentos traducidos a un sistema de aprendizaje automático; y
- clasificar, con el procesador, los segmentos y segmentos traducidos como pertenecientes a un usuario autorizado o como pertenecientes a un usuario no
- 5 autorizado mediante la asignación de una puntuación a cada uno de los segmentos y segmentos traducidos; y
- aplicar, con el procesador, un esquema de votación o un modelo de metaaprendizaje sobre las puntuaciones asignadas a los segmentos y segmentos traducidos; y
- 10 determinar, con el procesador, en base al esquema de votación o modelo de metaaprendizaje, si el usuario es un usuario autorizado.

- Ítem 11. El método del ítem 10, en donde el paso de puntuación comprende:
- comparar los segmentos y los segmentos traducidos con características del
- 15 usuario autorizado extraídas de segmentos de muestra proporcionados por el usuario autorizado durante un proceso de inscripción, en el que las características se almacenan en el medio de almacenamiento; y
- asignar a cada segmento una puntuación basada en el modelo de clasificación.

- 20 Ítem 12. El método del ítem 10 u 11, en el que uno o más sensores de movimiento comprenden al menos uno de un giroscopio y un acelerómetro.

- Ítem 13. El método de los ítems 10-12, donde el paso de dividir una o más señales de movimiento capturadas en segmentos comprende dividir cada señal
- 25 de movimiento en un número fijo de segmentos, donde cada segmento tiene una longitud fija.

Ítem 14. El método de los ítems 10-13, en el que al menos una parte de los segmentos se superponen.

Ítem 15. El método de los ítems 10-14, donde uno o más algoritmos de traducción
5 entrenados comprenden uno o más Cycle-GAN, y donde el paso de conversión comprende:

traducir los segmentos a través de un primer generador en los segmentos traducidos, que imitan los segmentos generados en otro dispositivo; y

volver a traducir los segmentos traducidos a través de un segundo generador
10 para imitar los segmentos generados en el dispositivo móvil.

Ítem 16. El método de los ítems 10-15, en el que los segmentos traducidos comprenden señales de movimiento sintéticas que simulan señales de movimiento que se originan en otro dispositivo.

Ítem 17. El método de los ítems 10-16, en donde el paso de provisión comprende:

extraer, con el procesamiento usando una o más técnicas de extracción de características, características de los segmentos y segmentos traducidos para
20 formar vectores de características; y

emplear un modelo de clasificación aprendido sobre los vectores de características que corresponden a los segmentos y los segmentos traducidos.

Ítem 18. Un sistema para desentrañar las características discriminatorias de un usuario de un dispositivo de las señales de movimiento capturadas en un dispositivo móvil que tenga al menos un sensor de movimiento y que autentique a un usuario en el dispositivo móvil, el sistema comprende:

una interfaz de comunicación de red;

30 un medio de almacenamiento legible por computadora;

un procesador configurado para interactuar con la interfaz de comunicación de red y el medio de almacenamiento legible por computadora y ejecutar uno o más módulos de software almacenados en el medio de almacenamiento, que incluyen:

- 5 para dividir cada señal de movimiento capturada en segmentos;
- un módulo de conversión que, cuando se ejecuta, configura el procesador para convertir los segmentos en segmentos traducidos utilizando una o más redes adversas generativas coherentes con el ciclo (Cycle-GAN) entrenadas;
- un módulo de extracción de características que, cuando se ejecuta, configura el
- 10 procesador para extraer características discriminatorias del usuario de los segmentos y segmentos traducidos, utilizando el procesador un sistema de aprendizaje automático;

- un módulo de clasificación que cuando se ejecuta configura el procesador para
- 15 asignar puntajes a los segmentos y segmentos traducidos y determinar si los segmentos y segmentos traducidos pertenecen a un usuario autorizado o a un usuario no autorizado en base a sus puntajes respectivos; y

- un módulo de metaaprendizaje que al ejecutarse configura el procesador para
- 20 aplicar un esquema de votación o un modelo de metaaprendizaje en base a las puntuaciones asignadas a los segmentos y segmentos traducidos en base a los segmentos almacenados correspondientes al usuario.

- Ítem 19. El sistema del ítem 18, en donde el al menos un sensor de movimiento
- 25 comprende al menos uno de un giroscopio y un acelerómetro.

Ítem 20. El sistema de los ítems 18-19, donde el módulo de conversión configura el procesador para traducir los segmentos a través de un primer generador en los segmentos traducidos, que imitan los segmentos generados en otro dispositivo y vuelven a traducir los segmentos traducidos a través de un segundo generador para imitar segmentos generados en el dispositivo móvil.

Ítem 21. El sistema de los ítems 18-20, en donde el módulo de extracción de características está además configurado para emplear un modelo de clasificación aprendido sobre las características extraídas que corresponden a los segmentos y los segmentos traducidos.

En este ítem, se debe tener en cuenta que, aunque gran parte de la descripción anterior se ha dirigido a sistemas y métodos para desentrañar las características discriminatorias de un usuario y la autenticación del usuario utilizando datos de sensores de movimiento, los sistemas y métodos descritos en este documento pueden implementarse y/o utilizarse de manera similar. implementado en escenarios, situaciones y entornos más allá de los escenarios referenciados.

Si bien esta especificación contiene muchos detalles de implementación específicos, estos no deben interpretarse como limitaciones en el alcance de cualquier implementación o de lo que se puede reclamar, sino más bien como descripciones de características que pueden ser específicas de realizaciones particulares de implementaciones particulares. Ciertas características que se describen en esta especificación en el contexto de realizaciones separadas también pueden implementarse en combinación en una sola realización. Por el contrario, varias características que se describen en el contexto de una sola realización también pueden implementarse en múltiples realizaciones por separado o en cualquier subcombinación adecuada. Además, aunque las características pueden describirse anteriormente como actuando en ciertas combinaciones e incluso afirmarse inicialmente como tales, una o más características de una combinación reivindicada pueden, en algunos casos, eliminarse de la combinación, y la combinación reivindicada puede dirigirse a una subcombinación o variación. de una subcombinación.

De manera similar, aunque las operaciones se representan en los dibujos en un orden particular, esto no debe entenderse como que requieren que dichas operaciones se realicen en el orden particular mostrado o en orden secuencial, o que se realicen todas las operaciones ilustradas, para lograr los resultados
5 deseados. En determinadas circunstancias, la multitarea y el procesamiento en paralelo pueden resultar ventajosos. Además, la separación de varios componentes del sistema en las realizaciones descritas anteriormente no debe entenderse como que requiere tal separación en todas las realizaciones, y debe entenderse que los componentes y sistemas del programa descritos
10 generalmente pueden integrarse juntos en un solo producto de software o empaquetarse en múltiples productos de software.

La terminología utilizada aquí tiene el propósito de describir realizaciones particulares únicamente y no pretende ser limitativa de la invención. Como se usa
15 aquí, las formas singulares "un", "una" y "el" también incluyen las formas plurales, a menos que el contexto indique claramente lo contrario. Se entenderá además que los términos "comprende" y/o "que comprende", cuando se usan en esta especificación, especifican la presencia de características, números enteros, pasos, operaciones, elementos y/o componentes establecidos, pero no excluyen
20 la presencia o adición de una o más características, números enteros, pasos, operaciones, elementos, componentes y/o grupos de los mismos. Cabe señalar que el uso de términos ordinales como "primero", "segundo", "tercero", etc., en las reivindicaciones para modificar un elemento de reivindicación no implica por sí mismo ninguna prioridad, precedencia u orden de un elemento de reivindicación.
25 sobre otro o el orden temporal en el que se realizan los actos de un método, pero se utilizan simplemente como etiquetas para distinguir un elemento de reivindicación que tiene un nombre determinado de otro elemento que tiene el mismo nombre (pero para el uso del término ordinal) para distinguir la reivindicación elementos. Además, la fraseología y la terminología utilizada en
30 este documento tienen fines descriptivos y no deben considerarse como limitantes.

El uso de "que incluye", "que comprende" o "que tiene", "que comprende", "que involucra" y variaciones de los mismos en este documento pretende abarcar los elementos enumerados a continuación y sus equivalentes, así como elementos adicionales. Debe entenderse que los mismos números en los dibujos

5 representan elementos similares a través de varias figuras, y que no todos los componentes y/o pasos descritos e ilustrados con referencia a las figuras son necesarios para todas las realizaciones o disposiciones.

Por tanto, las realizaciones y disposiciones ilustrativas de los sistemas y métodos descritos proporcionan un método implementado por ordenador, un sistema

10 informático y un producto de programa informático para la autenticación de usuarios utilizando datos de sensores de movimiento. El diagrama de flujo y los diagramas de bloques de las figuras ilustran la arquitectura, la funcionalidad y el funcionamiento de posibles implementaciones de sistemas, métodos y productos

15 de programas informáticos según diversas realizaciones y disposiciones. En este sentido, cada bloque en el diagrama de flujo o diagramas de bloques puede representar un módulo, segmento o porción de código, que comprende una o más instrucciones ejecutables para implementar la(s) función(es) lógica(s) especificada(s). También se debe tener en cuenta que, en algunas

20 implementaciones alternativas, las funciones anotadas en el bloque pueden ocurrir fuera del orden anotado en las figuras. Por ejemplo, dos bloques mostrados en sucesión pueden, de hecho, ejecutarse sustancialmente al mismo tiempo, o los bloques a veces pueden ejecutarse en el orden inverso, dependiendo de la funcionalidad involucrada. También se observará que cada

25 bloque de los diagramas de bloques y/o la ilustración del diagrama de flujo, y las combinaciones de bloques en los diagramas de bloques y/o la ilustración del diagrama de flujo, pueden implementarse mediante sistemas basados en hardware de propósito especial que realizan las funciones o actos especificados, o combinaciones de hardware de propósito especial e instrucciones de

30 computadora.

El tema descrito anteriormente se proporciona solo a modo de ilustración y no debe interpretarse como una limitación. Se pueden realizar diversas modificaciones y cambios al objeto descrito aquí sin seguir las realizaciones y

aplicaciones de ejemplo ilustradas y descritas, y sin apartarse del verdadero espíritu y alcance de la presente invención, que se establece en las siguientes reivindicaciones.