

19



OFICINA ESPAÑOLA DE
PATENTES Y MARCAS

ESPAÑA



11 Número de publicación: **3 028 243**

51 Int. Cl.:

G06F 18/214 (2013.01)

G06V 10/82 (2012.01)

G06V 40/20 (2012.01)

G06V 40/40 (2012.01)

12

TRADUCCIÓN DE PATENTE EUROPEA

T3

86 Fecha de presentación y número de la solicitud internacional: **27.01.2021** **PCT/EP2021/051864**

87 Fecha y número de publicación internacional: **05.08.2021** **WO21151947**

96 Fecha de presentación y número de la solicitud europea: **27.01.2021** **E 21702262 (3)**

97 Fecha y número de publicación de la concesión europea: **30.04.2025** **EP 4097632**

54 Título: **Método para entrenar un módulo detector de bots, y módulo detector de bots entrenado a partir de los datos de entrenamiento generados mediante el método**

30 Prioridad:

28.01.2020 ES 202030066

45 Fecha de publicación y mención en BOPI de la traducción de la patente:

18.06.2025

73 Titular/es:

**UNIVERSIDAD AUTÓNOMA DE MADRID
(100.00%)
Ciudad Universitaria de Cantoblanco, Calle
Einstein 3
28049 Madrid, ES**

72 Inventor/es:

**MORALES MORENO, AYTHAMI;
ORTEGA GARCÍA, JAVIER;
FIERREZ AGUILAR, JULIÁN;
VERA RODRIGUEZ, RUBÉN;
ACIEN AYALA, ALEJANDRO;
TOLOSANA MORANCHEL, RUBEN y
BARTOLOMÉ GONZALEZ, IVAN**

74 Agente/Representante:

CONTRERAS PÉREZ, Yahel

ES 3 028 243 T3

Aviso: En el plazo de nueve meses a contar desde la fecha de publicación en el Boletín Europeo de Patentes, de la mención de concesión de la patente europea, cualquier persona podrá oponerse ante la Oficina Europea de Patentes a la patente concedida. La oposición deberá formularse por escrito y estar motivada; sólo se considerará como formulada una vez que se haya realizado el pago de la tasa de oposición (art. 99.1 del Convenio sobre Concesión de Patentes Europeas).

DESCRIPCIÓN

Método para entrenar un módulo detector de bots, y módulo detector de bots entrenado a partir de los datos de entrenamiento generados mediante el método

Referencia a solicitudes relacionadas

Esta patente reivindica prioridad de la solicitud de patente nº P202030066.

Descripción

Esta patente reivindica prioridad de la solicitud de patente nº P202030066. La presente descripción está relacionada con métodos de detección de bots, del inglés Internet Bot, más concretamente con métodos de detección basados en la interacción humana con dispositivos y el entrenamiento de modelos a partir de datos reales y sintéticos.

Antecedentes

En los últimos años el número de dispositivos móviles, smartphones o tabletas, así como el acceso a internet a través de dichos dispositivos ha aumentado, y con ello la inseguridad debido a peligros tales como: ataques cibernéticos, robos de identidad, proliferación de cuentas y/o noticias falsas, etc. En consecuencia, se ha redoblado el esfuerzo por proporcionar medidas de seguridad adecuadas para los usuarios que eviten este tipo de ataques.

El método antifraude más popular para distinguir si la interacción con un dispositivo la realiza un humano se conoce como CAPTCHA, del inglés "Completely Automated Public Turing test to tell Computer and Humans Apart". Los CAPTCHA comprenden algoritmos que determinan si un interlocutor del dispositivo es humano, mediante retos asociados a las capacidades cognitivas humanas, es decir, aptitudes para procesar la información que implican el uso de la memoria, la atención, la percepción, la creatividad y el pensamiento abstracto o analógico. Algunos ejemplos de CAPTCHA son: identificación de objetos, reconocimiento de caracteres en imágenes distorsionadas, traducción de un audio distorsionado, etc.

Sin embargo, los programas maliciosos o malwares han evolucionado, gracias en gran medida a las nuevas técnicas de Aprendizaje Profundo, y se han adaptado para poder burlar contramedidas de seguridad tales como los CAPTCHA. Los bots, programas informáticos autónomos que realizan tareas concretas a través de un conjunto de instrucciones programadas en cualquier tipo de lenguaje, se han vuelto complejos y capaces de generar comportamientos que imitan o simulan de forma muy precisa el comportamiento humano. Dichos bots son difíciles de detectar o evitar mediante métodos actuales tales como el bloqueo de direcciones IP, entre otros.

Es necesario disponer de métodos de autenticación que mejoren la seguridad, que identifiquen las interacciones no humanas de manera fiable y autenticquen la interacción humano-máquina.

El documento «Android-GAN: Defending against android pattern attacks using multi-modal generative network as anomaly detector. Expert Systems with Applications», publicado el 10/09/2019 por SANG-YUN S. et al, divulga un método para autenticar usuarios en dispositivos móviles. El método propone utilizar una red generativa antagónica (GAN) para generar datos útiles para diferenciar entre patrones de Android realizados por diferentes sujetos. Por lo tanto, el método está diseñado para extraer la información biométrica que sirve para diferenciar entre sujetos. Este método está entrenado para extraer características específicas del usuario asociadas a la información conductual y neuromotora del sujeto de manera similar a otros sistemas de autenticación biométrica. En los sistemas de autenticación de usuarios, los atacantes están representados por otros usuarios que intentan suplantar la identidad de un usuario legítimo. Por el contrario, los sistemas de detección de bots deben estar entrenados para diferenciar entre sujetos humanos y atacantes de bots. Por lo tanto, los sistemas de detección de bots están entrenados para detectar características introducidas por generadores sintéticos.

El documento «SensoryGANs: An Effective Generative Adversarial Framework for Sensorbased Human Activity Recognition», publicado el 7 de julio de 2018 en la Conferencia Internacional Conjunta sobre Redes Neuronales (IJCNN) IEEE, de WANG JIWEI et al., divulga un método para reconocer gestos. El método propone utilizar una red generativa antagónica (GAN) para generar datos útiles para diferenciar entre las diferentes acciones humanas realizadas por los usuarios (por ejemplo, quedarse, caminar y correr). Así, el método está diseñado para extraer información relevante asociada a cada una de las citadas acciones de quedarse, caminar y correr. El método se evalúa en términos de precisión de clasificación de las acciones realizadas por los seres humanos.

El documento US 10 496 809 describe una aplicación para generar una respuesta de desafío para la autenticación utilizando relaciones entre objetos.

Descripción

En la presente descripción se define un método de detección de bots basado en el análisis de una interacción con dispositivos móviles. Para ello se procesa una señal de al menos un sensor integrado en un dispositivo por medio un algoritmo de detección previamente entrenado con muestras reales de interacción humana. El algoritmo de detección permite determinar si la señal, producto de la interacción, ha sido generada a partir de una interacción humana o si por el contrario ha sido generada de forma sintética por un bot. Se propone, además, un método de entrenamiento del algoritmo de detección a través de muestras de interacción real y sintética. La generación de muestras sintéticas se realiza a través de un método de generación previamente entrenado basado en redes neuronales generativas adversarias y a través de métodos de generación basados en la observación y caracterización de señales reales. Las redes generativas antagónicas (GAN) se han utilizado en la técnica anterior para generar datos sintéticos. La presente divulgación propone el uso de GAN dentro del campo específico de la detección de bots o el seguimiento o la monitorización de la interacción de dispositivos móviles. Las GAN de la presente divulgación se entrenan mediante el seguimiento o la monitorización o el análisis de las acciones realizadas en una pantalla de un dispositivo de usuario, como un smartphone o una tableta. Las acciones monitorizadas o seguidas pueden consistir en tocar una pantalla táctil, deslizar el dedo por la pantalla, gestos humanos realizados bajo el campo de visión de una cámara instalada en el dispositivo del usuario, como la cámara frontal o trasera de un smartphone.

En un primer aspecto, se define un método para generar datos de entrenamiento de un módulo detector de bots a través de interacción humana con un dispositivo móvil. El método comprende recibir al menos una señal generada por al menos un sensor integrado en el dispositivo móvil, siendo la al menos una señal generada durante la interacción de un humano con el dispositivo móvil. El método también comprende calcular variables escalares y/o temporales de la al menos una señal generada por el sensor que caracterizan un comportamiento humano, proveyendo así datos reales de entrenamiento y generar datos de entrenamiento que comprenden al menos los datos reales de entrenamiento.

Al generar datos de entrenamiento a partir de al menos una señal generada por al menos un sensor durante la interacción de un humano con un dispositivo, se tienen en cuenta aspectos biomecánicos y de contexto para poder modelar de manera más precisa y/o realista las interacciones humanas. Por lo tanto, los datos de aprendizaje son más completos, lo que mejora la calidad del entrenamiento de los módulos detectores, incrementando la seguridad de los accesos a través de los dispositivos (ya sean de manera local o a través de internet) y mejorando la usabilidad respecto a técnicas de detección tradicionales basadas, por ejemplo, en resolver puzzles o tareas cognitivas.

Los datos de entrenamiento que comprenden datos reales de entrenamiento mejora, por tanto, la detección de bots. Al comprender señales más complejas, éstas son más difíciles de imitar por los bots, por lo que los módulos de detección entrenados con los datos reales de entrenamiento discriminan de manera más fiable las interacciones no-humanas, aumentando así la seguridad y la confianza en entornos digitales.

Además, el uso de sensores integrados en el dispositivo permite la adquisición de datos reales de entrenamiento de manera más asequible, ya que no se requiere un dispositivo concreto y/o complejo para su obtención. En particular, a través de un dispositivo móvil tipo smartphone o tableta hace de la adquisición una tarea rápida y sencilla, puesto que se trata de un dispositivo de uso habitual y que no requiere habilidades especiales.

En algunos ejemplos, el método comprende sintetizar al menos una señal que modela un comportamiento humano, de manera que se puedan generar datos sintéticos de entrenamiento.

La función permite generar un número ilimitado de señales sintéticas con características similares a las que se generarían durante la interacción real de un humano. Sintetizar al menos una señal que modela un comportamiento humano no requiere entrenamiento. La operación puede basarse en funciones heurísticas obtenidas a partir de un estudio de señales generadas por humanos, como estadísticas, y funciones que permiten modelar, por ejemplo, la trayectoria espacial y la velocidad de un gesto, p. ej., funciones gaussianas, lineales, exponenciales, polinómicas.

Además, al generar datos sintéticos de entrenamiento, un módulo detector puede ser entrenado con dos tipos de datos: los reales y los sintéticos. Es decir, se pueden entrenar detectores incluyendo datos similares a los que intentarían evitar ser discriminados o clasificados como no-humanos por el discriminador, y por muestras reales provenientes de interacciones humanas reales. En este ejemplo, el módulo detector aprende a distinguir las diferencias entre datos reales y datos sintéticos para, una vez concluido el entrenamiento, poder discriminar las interacciones no-humanas de manera más fiable y efectiva.

El uso de datos de entrenamiento reales y sintéticos puede, por ejemplo, servir para generar nuevos CAPTCHAS.

En algunos ejemplos, adquirir los datos reales de interacción humana se lleva a cabo de manera transparente sin solicitar al usuario que realice una tarea de adquisición predefinida en el dispositivo móvil. Dicha adquisición transparente puede comprender el seguimiento de al menos una de las siguientes acciones realizadas por un usuario: el funcionamiento diario de un teléfono móvil, el funcionamiento diario de un teclado o panel táctil, las acciones diarias de deslizamiento en la pantalla de un dispositivo de usuario y las acciones diarias capturadas por una cámara de un dispositivo de usuario, por ejemplo, los gestos humanos realizados por un usuario bajo el campo de visión de una cámara frontal o trasera de un teléfono inteligente, sujetar el dispositivo o cambiar la ubicación del dispositivo. De esta manera, se incrementa la comodidad del usuario ya que no es necesario solicitar que realicen una o varias tareas concretas para obtener los datos de la interacción humana real. Además, de esta manera se logran datos reales de interacción humana real de manera más sencilla y rápida. La detección transparente puede llevarse a cabo mientras el usuario interacciona con un dispositivo a través de, por ejemplo, una aplicación móvil o app, una web, una plataforma online, etc.

En un segundo aspecto, se define un método de entrenamiento de un módulo detector de bots para detectar si una acción de usuario es humana o sintética, caracterizado porque comprende entrenar un módulo detector mediante un método de Aprendizaje Automático a partir de los datos de entrenamiento adquiridos de acuerdo con uno cualquiera de los ejemplos descritos.

En un tercer aspecto, se define un módulo detector de bots entrenado a partir de los datos de entrenamiento generados mediante el método de uno cualquiera de los ejemplos descritos. Al usar dicho módulo detector se incrementa la seguridad no solo en accesos a través de internet sino también de manera local, por ejemplo, en caso de que un bot sea instalado en un dispositivo sin acceso a internet.

En un cuarto aspecto, se define un método de detección de bots que comprende entrenar un módulo de detección de bots de acuerdo con un método de entrenamiento de acuerdo con uno cualquiera de los ejemplos descritos.

En un quinto aspecto se define un método de detección de bots que utiliza un módulo detector de acuerdo con uno cualquiera de los ejemplos descritos.

En un sexto aspecto se define un sistema de detección de bots que comprende un módulo detector de acuerdo con cualquiera de los ejemplos descritos, al menos una memoria y al menos un procesador para llevar a cabo un método de detección de acuerdo con una cualquiera de los ejemplos descritos.

En un séptimo aspecto se define un sistema de entrenamiento que comprende un módulo detector de acuerdo con cualquiera de los ejemplos descritos, al menos una memoria y al menos un procesador para llevar a cabo un método de entrenamiento de acuerdo con una cualquiera de los ejemplos descritos.

Breve descripción de los dibujos

A continuación, se describen ejemplos no limitativos de la presente descripción, con referencia a los dibujos que se acompañan, en los cuales:

La figura 1 ilustra esquemáticamente una vista de la parte frontal de un dispositivo de acuerdo con un ejemplo;

La figura 2 ilustra de manera esquemática el interior de un dispositivo de acuerdo con un ejemplo;

La figura 3 ilustra un diagrama de flujo de un método para generar datos de entrenamiento de un módulo detector de bots de acuerdo con un ejemplo;

La figura 4 ilustra un diagrama de flujo de un método para generar datos de entrenamiento sintéticos de acuerdo con un ejemplo;

La figura 5 ilustra un diagrama de flujo de un método para generar datos de entrenamiento sintéticos de acuerdo con un ejemplo;

La figura 6 ilustra esquemáticamente una red generativa y un algoritmo interconectados para ser entrenados en modo adversario de acuerdo con un ejemplo;

La figura 7 ilustra esquemáticamente una red generativa entrenada de acuerdo con un ejemplo;

La figura 8 ilustra un diagrama de flujo de un método para detectar bots de acuerdo con un ejemplo; y

La figura 9 ilustra esquemáticamente un módulo detector de acuerdo con un ejemplo.

Descripción detallada de ejemplos

- 5 Para clarificar algunos de los términos empleados en la presente solicitud, se incluyen a continuación las definiciones de dichos términos.
- Se entiende por “dispositivo”, un dispositivo móvil y/o vestible tales como teléfonos móviles o inteligentes, tabletas, pulseras inteligentes, gafas inteligentes, etc.
- 10 Se entiende por “uso transparente” el uso libre del dispositivo por parte de un usuario, es decir, sin solicitar al usuario que realice tareas concretas para que se generen los datos requeridos. Entre otras, las tareas concretas pueden incluir: seleccionar de entre una pluralidad imágenes distorsionadas, aquellas que representen un objeto predefinido; dibujar una figura concreta en la pantalla, etc.
- 15 Se entiende por “bot” un programa de ordenador diseñado en cualquier lenguaje de programación y que efectúa tareas repetitivas de manera automática. En muchos casos se utilizan para reducir la carga de trabajo y realizar tareas de manera más efectiva que un humano. Sin embargo, en algunos casos pueden usarse para usos maliciosos como, por ejemplo: ocupar el ancho de banda mediante la descarga de sitios web enteros, ataques de denegación de servicio mediante el envío de cientos o incluso miles de peticiones a un servidor web, propagación de contenidos interesados en redes sociales como por ejemplo noticias falsas, etc.
- 20 Se entiende por “ataques de bot” las inseguridades creadas tanto a través de los accesos vía internet como las surgidas de manera local, es decir, en un dispositivo que no tenga acceso a internet.
- 25 Se entiende por “interacción de un humano con el dispositivo” o “interacción humana real” a cualquier interacción realizada por un ser humano. Las interacciones pueden ser conscientes, por ejemplo, la introducción de caracteres; o inconscientes, por ejemplo, la navegación por una página web; de un usuario humano con el dispositivo, a través de la pantalla táctil o mediante cualquier otro medio, por ejemplo, el modo de sujetar el dispositivo o el cambio de ubicación del mismo.
- 30 Se entiende por “comportamiento humano” una pauta o conducta inherente al ser humano que ningún otro animal o máquina posee o puede poseer.
- 35 Se entiende por “señal sintética” una señal de origen artificial, es decir, que no ha sido generada por un sensor debido a la interacción de un humano, y que imita una señal proveniente de un sensor generada tras una interacción humana.
- Se entiende por “método artesanal” un método de generación de señales sintéticas experimental basado en la observación, análisis y caracterización de señales.
- 40 Se entiende por “Aprendizaje Automático”, del inglés Machine Learning, el conjunto de técnicas y/o algoritmos que ayudan a una máquina a adaptarse, aprender y/o evolucionar a través del análisis sucesivo de datos, mejorando así su rendimiento.
- 45 Por último, se entiende por “porcentaje de confianza” un porcentaje que evalúa la probabilidad de que la señal analizada por un módulo detector represente una interacción humana. Es decir, el porcentaje de confianza cuantifica el porcentaje de comportamiento humano presente en una señal.
- 50 La Figura 1 muestra un dispositivo 100 que puede comprender una pantalla 110, por ejemplo, una pantalla táctil; y al menos un accionador 120, que puede estar configurado para encender el dispositivo, bajar/subir el volumen, etc. En el ejemplo de la Figura 1 se muestra un teléfono inteligente (o smartphone), aunque en algunos ejemplos el dispositivo puede ser cualquier dispositivo móvil, como por ejemplo una tableta, una pulsera inteligente, unas gafas inteligentes, etc., que permita la interacción de un usuario para acceder y/o navegar por internet, interactuar con una app, publicar contenido en redes sociales, o comunicarse con otros usuarios mediante servicios de mensajería o correo.
- 55 El dispositivo puede comprender una pluralidad de funciones para facilitar la interacción de un usuario humano, es decir, para permitir, por ejemplo, introducción de texto o selección a través de la pantalla. En el ejemplo de la Figura 1, la pantalla 110 comprende una función de teclado virtual 111 para permitir la introducción de texto y/o caracteres de escritura.
- 60 Por otro lado, una interacción humana real también puede comprender, entre otras: la presión con la que un usuario presiona las teclas de un teclado virtual, cuantificable a través de un sensor de presión; el cambio de localización del

dispositivo medido mediante un sistema de localización (GPS); o la inclinación al sujetar el dispositivo medible gracias a un acelerómetro y/o un giroscopio.

La Figura 2 ilustra de manera esquemática el interior del dispositivo de la Figura 1. El dispositivo 100 puede comprender al menos un sensor integrado 131, 132, 133, 134, 135, 136, 137, 138. En algunos ejemplos, el dispositivo puede comprender una pluralidad de sensores que pueden usarse de manera individual o conjunta para adquirir datos de una interacción humana real. Los sensores pueden ser, por ejemplo, un sistema de posicionamiento global 131, GPS; un sistema wifi 132; un dispositivo Bluetooth 133; un acelerómetro 134; un giroscopio 135; un micrófono 136; un sensor de presión 137; un sensor de adquisición de rasgos de pulsación de teclas 138, un magnetómetro no ilustrado; etc.

En algún ejemplo, cuando la interacción humana comprende interaccionar a través de la pantalla táctil, puede tenerse en cuenta el tamaño de la pantalla para normalizar los datos obtenidos de la misma, para evitar así discrepancias debido a la diferencia de tamaño entre diferentes dispositivos.

Cada sensor puede generar al menos una señal como consecuencia de la interacción humana real con el dispositivo. El micrófono, por ejemplo, genera una única señal a partir de una onda acústica al producirse la interacción humana. Sin embargo, y dependiendo del sensor, pueden generarse varias señales en un mismo sensor. Por ejemplo, el acelerómetro genera tres señales relacionadas con los tres grados de libertad de un dispositivo situado en un espacio tridimensional.

En algunos ejemplos, la interacción humana real puede ser definida o caracterizada mediante la señal o señales generadas un único sensor, por ejemplo, un sensor de adquisición de rasgos de pulsación de teclas. En otro ejemplo, la interacción humana puede definirse mediante la combinación de las señales generadas por varios sensores. Por ejemplo, mediante las señales generadas por el acelerómetro y el sensor de presión.

En caso de combinar varias señales provenientes de al menos dos sensores diferentes, los datos reales que caracterizan interacciones humanas pueden ser más complejos y evitar, o dificultar notablemente, que un bot genere señales sintéticas similares a las señales de interacción humana real generadas por los sensores. Estos datos reales de interacción humana se pueden emplear, por ejemplo, para generar datos de entrenamiento que pueden usarse para entrenar un módulo de detección de bots, de manera que aprenda a discernir o detectar y discriminar bots de manera más fiable.

La Figura 3 ilustra un método 300 para generar datos de entrenamiento de un módulo detector de bots de simulación de interacción humana con un dispositivo. El método 300 puede comprender recibir, en el bloque 301, al menos una señal generada por al menos un sensor integrado en el dispositivo 100 de la Figura 1. Dicha señal puede ser generada durante la interacción de un humano con el dispositivo 1 para poder tener en cuenta aspectos o rasgos propios de la interacción de un usuario humano con el dispositivo. En algunos ejemplos, el método puede comprender recibir varias señales generadas por un único sensor o por varios sensores.

En algunos ejemplos, adquirir los datos reales de interacción humana se lleva a cabo de manera transparente, es decir, sin solicitar al usuario que realice una tarea de adquisición predefinida en el dispositivo móvil.

El método 300 puede comprender además calcular, en el bloque 302, variables de la al menos una señal generada por el al menos un sensor. Las variables pueden ser escalares y/o temporales, dependiendo del sensor, y pueden ser características que caracterizan o modelan un comportamiento humano, por ejemplo, coordenadas cartesianas, duración, perfiles de velocidad, aceleración etc. En algunos ejemplos, el sensor que genera la señal es un acelerómetro, y las variables calculadas son tanto escalares como temporales, más concretamente duración, distancia, desplazamiento, ángulo, velocidad y eficiencia del movimiento.

Para calcular las variables se puede usar funciones explícitamente programadas para ello o algoritmos entrenados para caracterizar de forma automática dichas señales, por ejemplo, redes neuronales que pueden variar dependiendo de la(s) variable(s) a calcular. En algunos ejemplos, la distancia puede calcularse mediante una función que calcula la distancia euclídea entre las coordenadas finales y las iniciales.

Mediante el cálculo de las variables se puede proveer datos reales de entrenamiento.

El método puede comprender, en el bloque 303, generar datos entrenamiento que comprenden al menos los datos reales de entrenamiento. De esta manera el módulo de entrenamiento puede entrenarse con datos reales de entrenamiento que modelan de manera más precisa las interacciones humanas con un dispositivo.

El método 300 comprende además entrenar al menos una función a partir de los datos reales de interacción humana. La función está configurada para sintetizar al menos una señal que modela un comportamiento humano.

La síntesis o elaboración de la al menos una señal se lleva a cabo de diferentes maneras, como por ejemplo de manera artesanal, es decir, mediante un método de síntesis basado en la observación, el análisis y la caracterización de una señal (ver Figura 4); o a través un método que comprende el entrenamiento en modo adversario de una red neuronal generativa, o Generador; y un algoritmo de discriminación, o Discriminador; (ver Figura 5).

La Figura 4 muestra un diagrama de flujo de un método 400 para sintetizar al menos una señal que modela un comportamiento humano. El método 400 puede comprender, en el bloque 401, recibir una pluralidad de señales generadas por el al menos un sensor integrado y, calcular un conjunto de características comunes de la pluralidad de señales para caracterizar un comportamiento humano, en el bloque 402.

Las características comunes son aquellas que sirven para modelar el comportamiento humano, y que puede variar dependiendo de cada sensor. Como por ejemplo en caso de que se capture un gesto, por ejemplo, un barrido; a través de la pantalla táctil del dispositivo, las características comunes de las señales son, entre otras: dirección, duración, desplazamiento, ángulo, etc.

Por ejemplo, en un gesto realizado por un usuario sobre la pantalla del dispositivo es definido por N muestras Las características comunes pueden calcularse mediante vectores de coordenadas espaciales y de tiempos (x, y, t) . Por ejemplo, la duración del gesto se calcular como $t(N)-t(1)$ y el desplazamiento como $\sum_{i=1}^{N-1} [\|((x(i),y(i))-(x(i+1),y(i+1)))\|]$, siendo $\| \cdot \|$ el operador distancia euclídea.

El método 400 comprende además realizar, en el bloque 403, un análisis estadístico de las características comunes para obtener una variabilidad. El análisis estadístico comprende calcular variables estadísticas como la media, la desviación estándar, etc. mediante métodos de estimación de densidades de probabilidad de histogramas, por ejemplo. La variabilidad obtenida refleja una variabilidad natural, es decir una duración, direccionalidad, ángulo y velocidad similar a la producida por un gesto humano y puede servir, por ejemplo, para filtrar señales que muy difícilmente podrían pertenecer a un comportamiento humano, por ejemplo, una señal que refleje una frecuencia de pulsación de teclas irreal o imposible de llevar a cabo por un humano, 2000 millones de veces por segundo.

El método 400 también comprende generar, en el bloque 404, datos sintéticos de entrenamiento que comprenden un dato inicial y datos sucesivos que difieren del dato inicial de acuerdo con la variabilidad. Es decir, se genera una pluralidad de datos que son diferentes entre sí pero dentro de un rango de variabilidad predeterminado o natural, estimado por ejemplo, las densidades de probabilidad de histogramas para que puedan considerarse similares a una señal de interacción humana real. Las señales sintéticas pueden generarse sintetizando, por ejemplo, el desplazamiento y la velocidad de los gestos. Para ello, un método para sintetizar al menos una señal que modele el comportamiento humano puede emplear funciones matemáticas lineales y exponenciales que permitan generar una o varias señales sintéticas con características similares a las humanas. Por ejemplo, si un gesto, como un barrido, se captura a través de la pantalla táctil del dispositivo, las características comunes de las señales son, entre otras: dirección, duración, desplazamiento, ángulo, etc. Los datos sintéticos se caracterizan por una dirección sintetizada, una duración sintetizada, un desplazamiento sintetizado y un ángulo sintetizado.

Asimismo, el método 400 puede comprender generar, en el bloque 405, datos de entrenamiento que comprenden al menos los datos sintéticos de entrenamiento. Los datos de entrenamiento pueden, en consecuencia, comprender datos de entrenamiento tanto reales como sintéticos. Estos datos de entrenamiento heterogéneos reducen el riesgo de clasificar comportamientos tanto sintéticos como humanos. Al entrenar un módulo detector de bots con datos reales de entrenamiento y con datos sintéticos de entrenamiento se obtiene un detector más eficiente y fiable para discriminar interacciones no humanas.

La Figura 5 muestra un diagrama de flujo de otro método 500 para sintetizar al menos una señal que modela un comportamiento humano. El método 500 puede comprender proporcionar, en el bloque 501, una red neuronal generativa configurada para generar al menos una señal sintética, por ejemplo, a partir de una señal de ruido aleatorio. La red neuronal generativa puede comprender al menos dos entradas, una primera entrada para introducir una señal que sirva de base para generar la función sintética, por ejemplo, una señal de ruido aleatorio; y una segunda entrada para introducir una señal que modifique o influya la generación de las sucesivas/subsiguientes señales sintéticas, como por ejemplo una señal de retroalimentación.

El método 500 puede comprender proporcionar, en el bloque 502, un algoritmo de discriminación configurado para discriminar entre datos reales y sintéticos. Es decir, el algoritmo puede estar configurado para recibir una señal, analizarla y proporcionar una medida de confianza para determinar si la misma es debido a una interacción humana real o a una interacción sintética. El algoritmo de discriminación puede, en algunos ejemplos, ser una red neuronal u otro tipo algoritmo de aprendizaje supervisado como por ejemplo una Máquina de Vector Soporte, Bosques Aleatorios o Random Forest, etc., y puede comprender al menos tres entradas. Una primera entrada puede estar

configurada para recibir la señal a analizar, por ejemplo, una señal sintética generada por una red neuronal generativa; una segunda entrada para recibir una señal con la que comparar la señal a analizar, por ejemplo, una señal generada por un sensor tras una interacción humana real; y, una tercera entrada, que se utiliza durante el entrenamiento, para introducir una señal que modifica o influye en el resultado del algoritmo de discriminación, es decir que modifica los parámetros del propio algoritmo de discriminación, durante las comparaciones sucesivas/subsiguientes del proceso de entrenamiento.

El algoritmo de discriminación está configurado para generar como salida durante el entrenamiento una función de pérdidas. La función de pérdidas es proporcional al error cometido al discriminar. Una vez entrenado, el algoritmo puede estar configurado para discriminar una señal de entrada, por ejemplo, una señal generada por la red neuronal generativa, es decir: para analizar y comparar la señal de entrada con una señal generada por un sensor debido a una interacción humana real; y dar como salida un porcentaje de su similitud con los patrones reales humanos.

El método 500 puede comprender además entrenar iterativamente, en el bloque 503, la red neuronal generativa y el algoritmo de discriminación en modo adversario. Es decir, la red neuronal puede generar una pluralidad de funciones sucesivas que son discriminadas o analizadas por el algoritmo discriminador, y el resultado puede retroalimentar tanto la red neuronal generativa como el propio algoritmo de discriminación en un juego de suma cero que permita mejorar el rendimiento de ambos.

Para llevar a cabo el entrenamiento en modo adversario, se pueden introducir como entradas de la red neuronal generativa la función de pérdidas generada por el algoritmo de discriminación, y al menos una señal de ruido aleatorio para generar una señal sintética. Una señal de ruido aleatorio comprende un vector de N números aleatorios que sirve de semilla para la red neuronal generativa para generar señales a partir del mismo.

Por otro lado, se pueden introducir como entradas del algoritmo discriminador la señal sintética generada por la red neuronal generativa, una señal generada por un sensor integrado tras una interacción humana real y/o los datos reales de entrenamiento; y la función de pérdidas generada por el algoritmo de discriminación.

El entrenamiento puede llevarse a cabo hasta que el valor absoluto de la diferencia de funciones de pérdidas entre iteraciones sucesivas esté comprendido entre un 0.0001% y un 20%. Es decir, hasta que el método de entrenamiento no es capaz de mejorar las salidas y/o el código de la red neuronal generativa ni del algoritmo de discriminación.

Al terminar el proceso de entrenamiento se obtiene una red neuronal generativa entrenada (ver Figura 7) y un algoritmo discriminador entrenado. La red neuronal generativa entrenada puede ser utilizada para generar muestras sintéticas que permitan entrenar mejores modelos de detección de bots. Por otro lado, el algoritmo de discriminación entrenado puede ser usado como detector de bots.

Al conseguir que la diferencia de funciones de pérdidas entre iteraciones sucesivas esté comprendida entre un 0.0001%, es decir, una variabilidad pequeña entre las funciones de pérdidas de iteraciones sucesivas, se consigue que la red neuronal generativa ha aprendido suficiente, es decir, que la diferencia entre las sucesivas señales generadas no es significativa y que es capaz de generar señales sintéticas muy parecida a las señales que podría generar un sensor tras una interacción humana real.

El método 500 puede comprender generar, en el bloque 504, datos sintéticos de entrenamiento que comprenden al menos una señal sintética generada por la red neuronal generativa entrenada a la que puede introducirse como señal de entrada una señal de ruido aleatorio. Finalmente, el método 500 puede comprender generar, en el bloque 505, datos de entrenamiento que comprenden al menos los datos sintéticos de entrenamiento. Es decir, los datos de entrenamiento que pueden usarse para entrenar un detector de bots comprenderán al menos una señal sintética generada por una red neuronal entrenada, por lo que el detector aprenderá a discriminar de manera más eficaz, lo cual aumentará considerablemente la seguridad y la fiabilidad del módulo detector.

La Figura 6 ilustra esquemáticamente una red neuronal generativa 610, y un algoritmo discriminador 620 conectados para el entrenamiento en modo adversario de acuerdo con un ejemplo. La red neuronal generativa 610 puede comprender dos entradas: una señal de ruido aleatoria 1 y una señal de retroalimentación 3, por ejemplo, la salida del algoritmo discriminador; y una señal de salida 4, por ejemplo, una función sintética.

El algoritmo discriminador 620 puede comprender tres entradas: una señal sintética 4, por ejemplo generada por la red neuronal generativa; una señal de datos reales 2, por ejemplo, una señal generada por un sensor integrado en un dispositivo móvil tras una interacción y/o datos reales de entrenamiento, y una señal de retroalimentación 3, por ejemplo la salida del algoritmo discriminador 620. La señal de retroalimentación 3, es decir, la salida del discriminador 620, puede comprender una función de pérdidas que refleje la probabilidad de que esa señal ha sido generada por un humano o un bot.

El discriminador se alimenta con señales humanas reales y con señales sintéticas generadas por la red neuronal generativa. La función de pérdidas reflejará con valores elevados cuando el discriminador no es capaz de diferenciar cada tipo de señal (humana o sintética) mientras que reflejará valores próximos a cero cuando la discriminación sea correcta. Este proceso se repite de forma iterativa usando la función de pérdidas para mejorar el rendimiento tanto del discriminador como de la red neuronal generativa.

Una vez entrenado, el algoritmo discriminador comprende: una entrada, al menos una señal proveniente de al menos un sensor que capture la interacción humana; una salida que refleje la probabilidad de que esa señal ha sido generada por un humano o un bot. típicamente es un valor entre 0 y 1, donde los en donde valores cercanos a 1 significan una alta probabilidad de que la señal provenga de un bot y; los valores cercanos a 0, una alta probabilidad de que la señal provenga de la interacción por parte de un humano.

La Figura 7 muestra esquemáticamente una red neuronal generativa entrenada 700. La red neuronal generativa entrenada 700 puede comprender como entrada 5 una señal, por ejemplo, una señal de ruido aleatorio; que sirve de base para generar una señal sintética y como salida 6 una señal sintética. La señal sintética generada por la red neuronal generativa entrenada 700 puede usarse, por ejemplo, como dato sintético de entrenamiento para entrenar un detector de bots, ya que la red neuronal ha aprendido lo suficiente para generar funciones sintéticas muy similar a la señal generada por un sensor. En algunos ejemplos, la una red neuronal generativa entrenada 700 puede recibir como entrada 5 una pluralidad de señales de ruido aleatorio, para generar una pluralidad de señales sintéticas que pueden usarse, por ejemplo, como datos sintéticos de entrenamiento para entrenar un detector de bots.

Al usar una red neuronal entrenada para generar los datos sintéticos de entrenamiento de un detector de bots, se consigue un mejor rendimiento ya que el detector no solo aprende de datos reales que modelan de manera más específica y compleja las interacciones humanas, sino también de señales generadas a partir de los mismos. Es decir, mediante el uso de datos reales de entrenamiento y de datos sintéticos de entrenamiento, se pueden obtener módulos detectores de bots con una mejorada eficacia en detección de bots, de manera que se incrementa la seguridad, por ejemplo, en los accesos a cuentas bancarias o dominios web, interacción en redes sociales, comunicación entre usuarios y terceros, gestión de cuentas digitales, etc.

La Figura 8 muestra un diagrama de flujo de un método 800 de entrenamiento de un módulo detector de bots para detectar si una acción de usuario es humana o sintética. El método 800 puede comprender entrenar, en el bloque 801, un módulo detector mediante un método de Aprendizaje Automático a partir de los datos reales de entrenamiento adquiridos de acuerdo con cualquiera de los ejemplos descritos. De modo que puede obtener un módulo detector de bots entrenado, es decir, capaz de detectar de manera si el usuario que está interactuando es un bot.

En algunos ejemplos, el método 800 puede comprender entrenar el módulo detector con datos reales de entrenamiento y con una pluralidad datos sintéticos de entrenamiento generados de acuerdo con una cualquiera de los ejemplos descritos, por ejemplo, mediante un método artesanal o con una red neuronal entrenada en modo adversario junto con un algoritmo discriminador. El entrenamiento puede utilizar algoritmos de clasificación o discriminación como Máquina de Soporte de Vectores (del inglés Support Vector Machine), Bosque Aleatorio (del inglés Random Forest) o Perceptrón Multicapa (del inglés Multilayer Perceptron).

Al entrenar el módulo con datos reales de entrenamiento reales y sintéticos, la eficacia y fiabilidad de las detecciones del módulo detector se incrementa considerablemente. Como consecuencia, la seguridad y confianza en entornos digitales puede incrementarse notablemente ya que se pueden discriminar un mayor número de usuarios no-humanos.

El método 800 puede comprender además detectar, en el bloque 802, bots mediante el módulo detector entrenando.

El módulo detector puede recibir una señal de entrada y dar como salida un porcentaje de confianza que refleje la probabilidad de que la señal de entrada sea generada por una interacción humana real.

El método 800 de entrenamiento de un módulo detector de bots para detectar si una acción del usuario es humana o sintética puede comprender las siguientes características:

-recopilar de datos: se pueden proporcionar los datos reales especificados en el primer aspecto de la divulgación y los datos sintéticos especificados en la presente divulgación. Se puede proporcionar un método de entrenamiento con al menos 5000 muestras sintéticas por sensor. Se pueden haber adquirido varias muestras, por ejemplo decenas de miles de muestras, a lo largo de algunos años observando y registrando gestos humanos, usos humanos de un dispositivo móvil o uso humano de la pantalla de un dispositivo;

-preprocesar de los datos recopilados: en el caso de los gestos de deslizamiento en la pantalla, se pueden seleccionar gestos de al menos 0,3 segundos de duración. Estos gestos pueden normalizarse para que todos tengan la misma coordenada y/o dirección de origen;
 los datos normalizados pueden dividirse en un 60 % de los datos que pueden utilizarse para el entrenamiento, un 20 % de los datos para la validación y un 20 % de los datos para las pruebas;
 -entrenar el módulo detector de bots proporcionando el 60 % de los datos normalizados para el entrenamiento; el entrenamiento puede comprender: tasa de aprendizaje $\alpha = 2 \cdot 10^{-4}$, optimizador Adam con $\beta_1 = 0,5$, $\beta_2 = 0,999$ y $\epsilon = 10^{-8}$. El sistema puede entrenarse durante 50 épocas con un tamaño de lote de 128 muestras tanto para el generador como para el discriminador. La función de pérdida puede ser «entropía cruzada binaria» para el discriminador y «error cuadrático medio» para el generador.
 -ajustar los hiperparámetros con el 20 % de datos normalizados para la validación. Los hiperparámetros pueden ser los siguientes: Ambas redes GAN pueden entrenarse utilizando más de 10 000 muestras humanas extraídas de la HuMldb (base de datos de interacción humana móvil);
 -y probar los datos clasificados resultantes con el 20 % de los datos normalizados para la prueba.

En la presente divulgación se propone un método de síntesis basado en una red generativa antagónica (GAN). La GAN se compone de dos redes denominadas: generador y discriminador. Estas redes pueden estar formadas por arquitecturas denominadas redes neuronales recurrentes (RNN), en particular, un modelo RNN denominado red de memoria a corto y largo plazo (LSTM). Estas LSTM pueden tener múltiples parámetros. La siguiente descripción representa una implementación de ejemplo, pero una persona experta puede modificar ligeramente algunos o todos los parámetros y obtener resultados similares. En concreto, los LSTM pueden estar compuestos por dos capas LSTM de 128 unidades seguidas de una capa «densa» de 128 unidades. Mientras que un objetivo de aprendizaje del generador puede ser sintetizar muestras de la forma más realista posible, el objetivo de aprendizaje del discriminador puede ser clasificar muestras humanas a partir de muestras sintéticas. Esto puede lograrse mediante una función de pérdida conocida como «minimax loss».

Las señales sintéticas generadas según cualquiera de los métodos de la presente divulgación, y las señales humanas pueden parametrizarse. Por ejemplo, la velocidad, la aceleración, la duración, la trayectoria, etc., pueden parametrizarse para obtener un vector característico para cada gesto, que puede denominarse «vector característico de longitud fija». Los vectores de las muestras reales y las muestras sintéticas pueden utilizarse para entrenar un clasificador binario que pueda distinguir entre humano o bot. Una vez entrenado el clasificador, puede utilizarse para discriminar un gesto entre gesto humano o gesto bot, que no se hayan utilizado durante el entrenamiento. Además, el clasificador puede parametrizar el gesto y determinar si se trata de un gesto producido por un humano o un bot. Las máquinas de vectores de soporte o el bosque aleatorio pueden utilizarse como clasificador o discriminador.

Los resultados pueden registrarse en tablas de resultados (puede verlos en el artículo que le hemos enviado). Podemos incluir resultados si cree que sería de ayuda.

En cuanto a la infraestructura informática que puede utilizarse para entrenar los modelos, puede utilizarse un PC con Windows y procesador i7, 32 GB de RAM... No se requiere ningún hardware específico.

La Figura 9 muestra de manera esquemática un módulo detector de bots 900 entrenado a partir de los datos de entrenamiento generados mediante el método de acuerdo con uno cualquiera de los ejemplos descritos. En algunos ejemplos, el módulo puede ser entrenado con datos reales de entrenamiento. En algunos ejemplos, el módulo puede ser entrenado, además, con datos sintéticos de entrenamiento generados de acuerdo con una cualquiera de los ejemplos descritos, por ejemplo, mediante una red neuronal generativa entrenada. En un ejemplo, el módulo es un dispositivo detector de bots.

El módulo detector de bots 900 puede estar configurado para recibir una señal de entrada 7, por ejemplo, una señal proveniente de un dispositivo móvil, y para generar una salida 8 que puede comprender un porcentaje de confianza para dar a conocer la probabilidad de que la señal de entrada 7 haya sido generada por la interacción de un humano con el dispositivo, es decir, de que se trate de una interacción humana real.

A pesar de que se han descrito aquí sólo varios ejemplos, son posibles otras alternativas, modificaciones, usos y/o equivalentes las mismas. Además, todas las posibles combinaciones de los ejemplos descritos quedan también cubiertas. Así, el alcance de la presente descripción no debe limitarse al ejemplo particular, sino que debe determinarse únicamente por una lectura apropiada de las siguientes reivindicaciones. Los signos de referencia relacionados con dibujos entre paréntesis son únicamente para intentar aumentar la comprensión de la reivindicación y no deben interpretarse como limitativos del alcance de la reivindicación.

REIVINDICACIONES

1. Método (800) para entrenar un módulo detector de bots a través de Aprendizaje Automático para detectar si una acción de usuario es humana o sintética, usando datos de entrenamiento adquiridos por un método para generar datos de entrenamiento de un módulo detector de bots a través de interacción humana con un dispositivo móvil, el método para generar datos de entrenamiento comprendiendo:
5 recibir (301) al menos una señal generada por al menos un sensor integrado en el dispositivo móvil, siendo la al menos una señal generada durante la interacción de un humano con el dispositivo móvil; en el que recibir la al menos una señal generada se lleva a cabo mediante el seguimiento de al menos una de las siguientes acciones
10 realizadas por un usuario: funcionamiento diario de un teléfono móvil, funcionamiento diario de un teclado o panel táctil, acciones diarias de deslizamiento en la pantalla de un dispositivo de usuario y acciones diarias capturadas por una cámara de un dispositivo de usuario, sujetar el dispositivo o cambiar la ubicación del dispositivo;
calcular (302) variables escalares y/o temporales de la al menos una señal generada por el sensor que caracteriza un gesto humano, proveyendo así datos reales de entrenamiento; y
15 sintetizar al menos una señal que modela un gesto humano para generar (504) datos sintéticos de entrenamiento, los datos sintéticos comprendiendo una dirección sintetizada, una duración sintetizada, un desplazamiento sintetizado y un ángulo sintetizado, en el que sintetizar la al menos una señal que modela un gesto humano comprende:
proporcionar (501) una red neuronal (610) generativa configurada para generar al menos una señal sintética, la red neuronal generativa comprendiendo al menos dos entradas;
20 proporcionar (502) un algoritmo de discriminación (620) configurado para discriminar entre datos reales y sintéticos, y para generar como salida una función de pérdidas que define el error cometido al discriminar, donde el algoritmo comprende al menos tres entradas;
entrenar iterativamente (503) la red neuronal (610) generativa y el algoritmo de discriminación en modo adversario
25 introduciendo como entradas de la red neuronal generativa:
-la función de pérdidas (3) generada por el algoritmo de discriminación; y
-al menos una señal de ruido aleatorio (1) para generar la al menos una señal sintética; e introduciendo como entradas del algoritmo de discriminación (620):
-la al menos una señal sintética (4) generada por la red neuronal generativa,
30 -la al menos una señal (2) generada por el al menos un sensor integrado y/o los datos reales de entrenamiento, y
-la función de pérdidas (3) generada por el algoritmo de discriminación;
hasta que el valor absoluto de la diferencia de funciones de pérdidas entre iteraciones sucesivas está comprendido entre un 0.0001% y un 20%, obteniendo así una red neuronal generativa entrenada;
generar (504) datos sintéticos de entrenamiento que comprenden al menos una señal sintética generada por la red neuronal generativa entrenada, al introducir como entrada al menos una señal de ruido aleatorio;
35 generar (303, 505) datos de entrenamiento que comprenden al menos los datos sintéticos de entrenamiento, y donde el método para entrenar el módulo detector de bots comprende entrenar (801) el módulo detector de bots con una pluralidad de datos sintéticos de entrenamiento.
- 40 2. Método para entrenar un módulo detector de bots de acuerdo con la reivindicación 1, caracterizado porque sintetizar la al menos una señal que modela un gesto humano comprende un método de síntesis basado en la observación, análisis y caracterización de la al menos una señal generada por el sensor, el método de síntesis comprendiendo:
recibir (401) una pluralidad de señales generadas por el al menos un sensor integrado;
45 calcular (402) un conjunto de características comunes de la pluralidad de señales, las características comunes, incluyendo al menos una de un grupo que comprende dirección, duración, desplazamiento y ángulo, para caracterizar un comportamiento humano;
realizar (403) un análisis estadístico de las características comunes para obtener una variabilidad;
generar (404) datos sintéticos de entrenamiento que comprenden un dato inicial y datos sucesivos que difieren del dato inicial de acuerdo con la variabilidad; y
50 generar (405) datos de entrenamiento que comprenden al menos los datos sintéticos de entrenamiento.
3. Método para entrenar un módulo detector de bots de acuerdo con una cualquiera de las reivindicaciones 1 a 2, donde el al menos un sensor integrado es un sistema de posicionamiento global, GPS, y/o un sistema wifi, y/o un
55 dispositivo Bluetooth, y/o un acelerómetro, y/o un giroscopio, y/o un magnetómetro, y/o un sensor de presión y/o un sensor de adquisición de rasgos de pulsación de teclas.
4. Método para entrenar un módulo detector de bots según una cualquiera de las reivindicaciones 1 a 3 que comprende:
60 preprocesar los datos de entrenamiento reales y la pluralidad de datos de entrenamiento sintéticos, seleccionando gestos de deslizamiento de más de 0,3 segundos en una pantalla;
normalizar dichos gestos para proporcionar al menos una de las siguientes características: misma coordenada de origen y dirección;

dividir los datos normalizados en tres grupos, cada uno de los cuales comprende el 60 % de los datos normalizados para el entrenamiento, el 20 % de los datos normalizados para la validación y el 20 % de los datos normalizados para la prueba;

- 5 entrenar el módulo detector de bots proporcionando el 60 % de los datos normalizados para el entrenamiento;
ajustar los hiperparámetros con el 20 % de los datos normalizados para la validación y
probar los datos clasificados resultantes con el 20 % de los datos normalizados para la prueba.

- 10 5. Módulo (900) detector de bots entrenado por un método para entrenar un módulo detector de bots según una cualquiera de las reivindicaciones 1 a 4, el módulo detector de bots configurado para recibir una señal de entrada proveniente de al menos un sensor de un dispositivo móvil, y para generar una salida que comprende un porcentaje de confianza, donde el porcentaje de confianza comprende un porcentaje probabilístico de que la señal de entrada es generada por una interacción humana real.

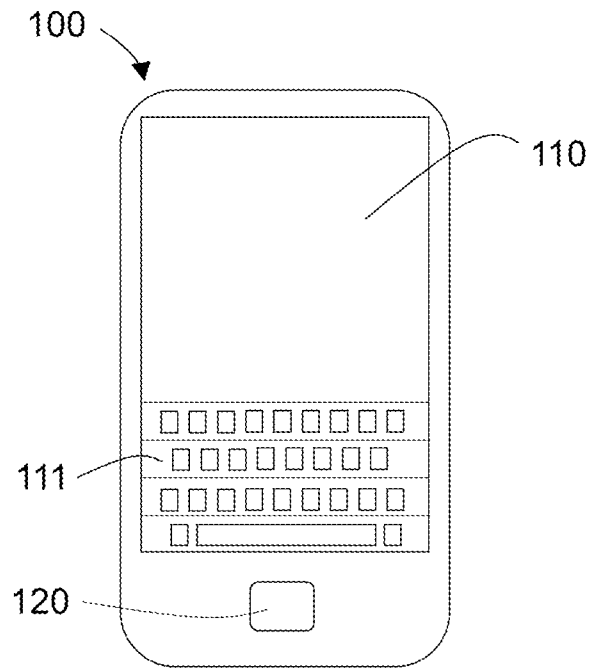


FIG. 1

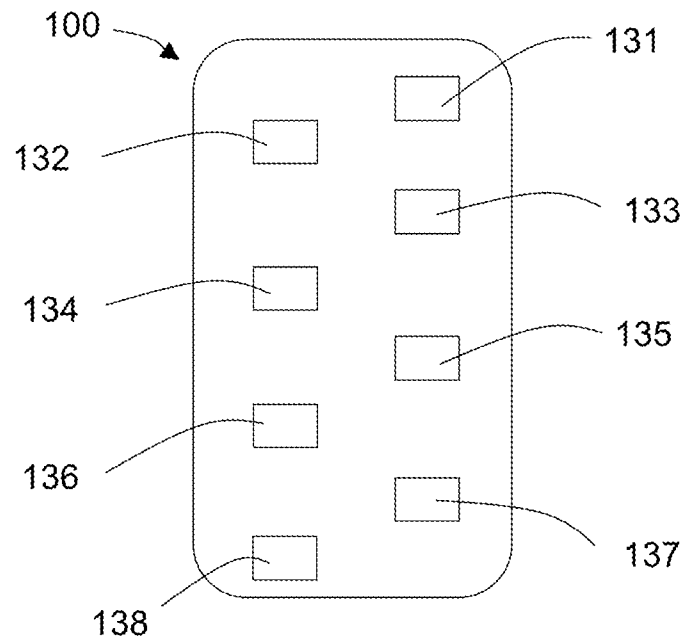


FIG. 2

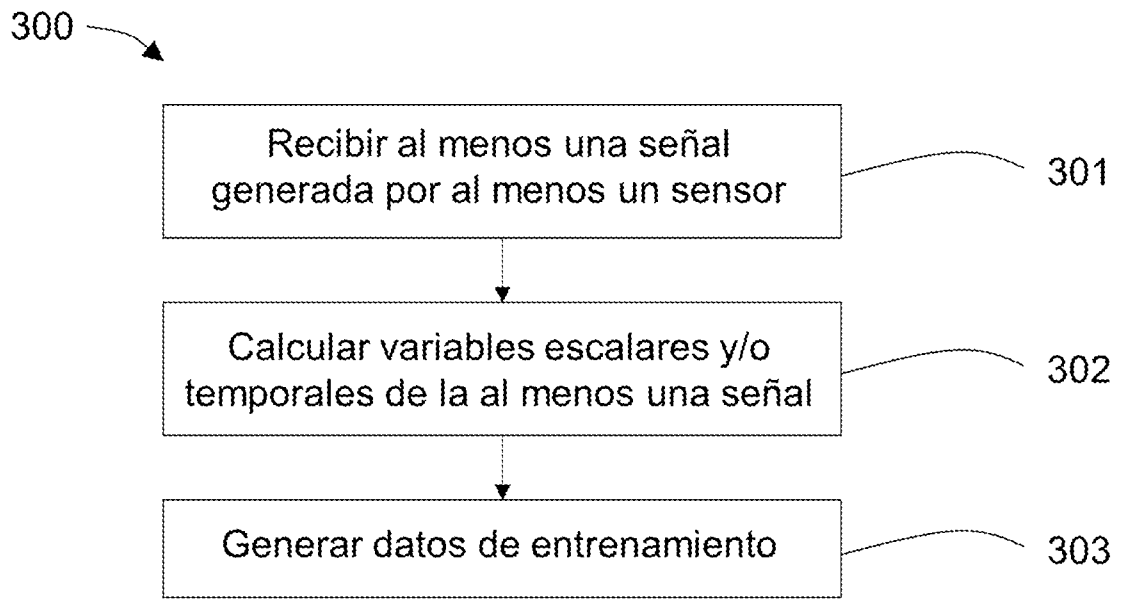


FIG. 3

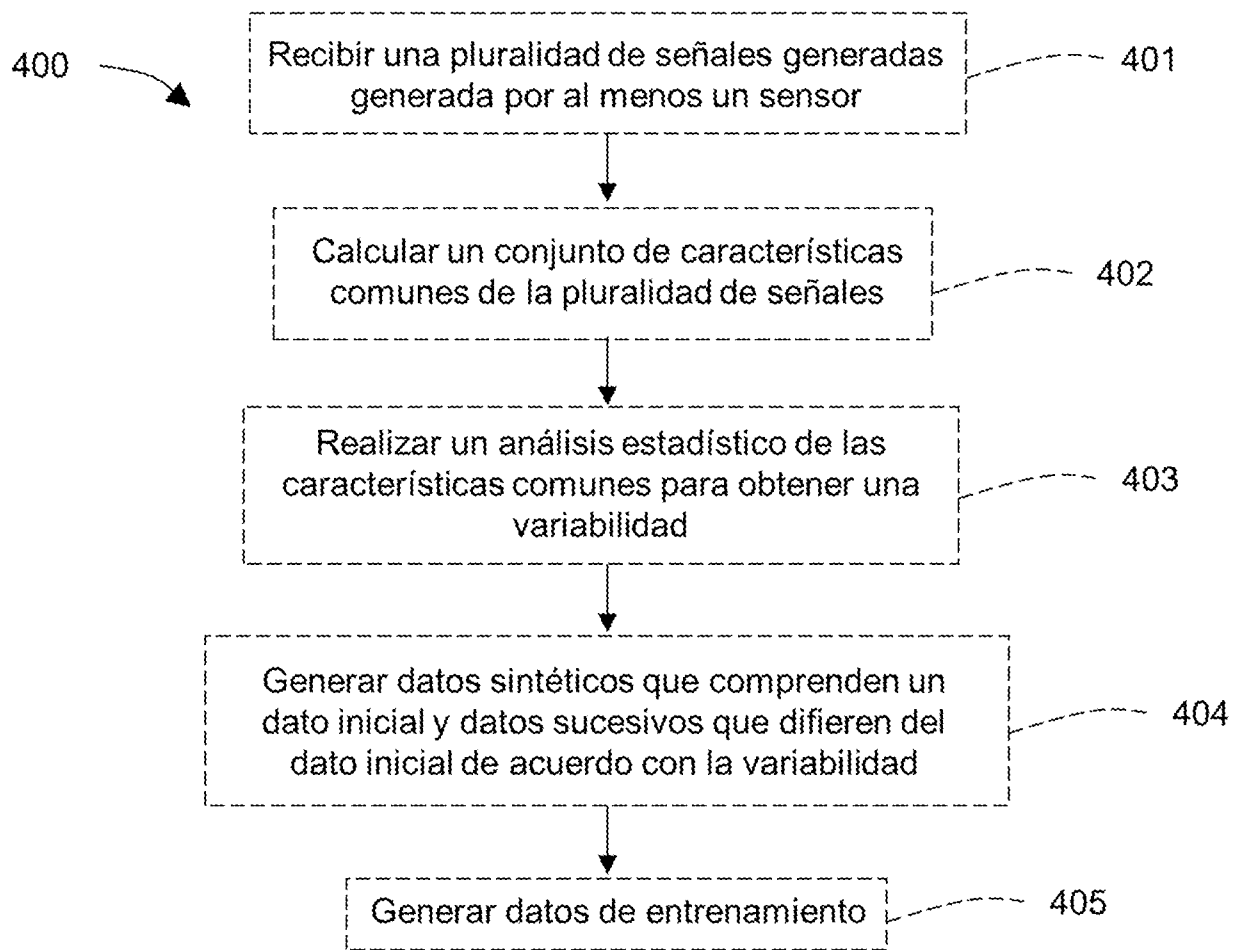
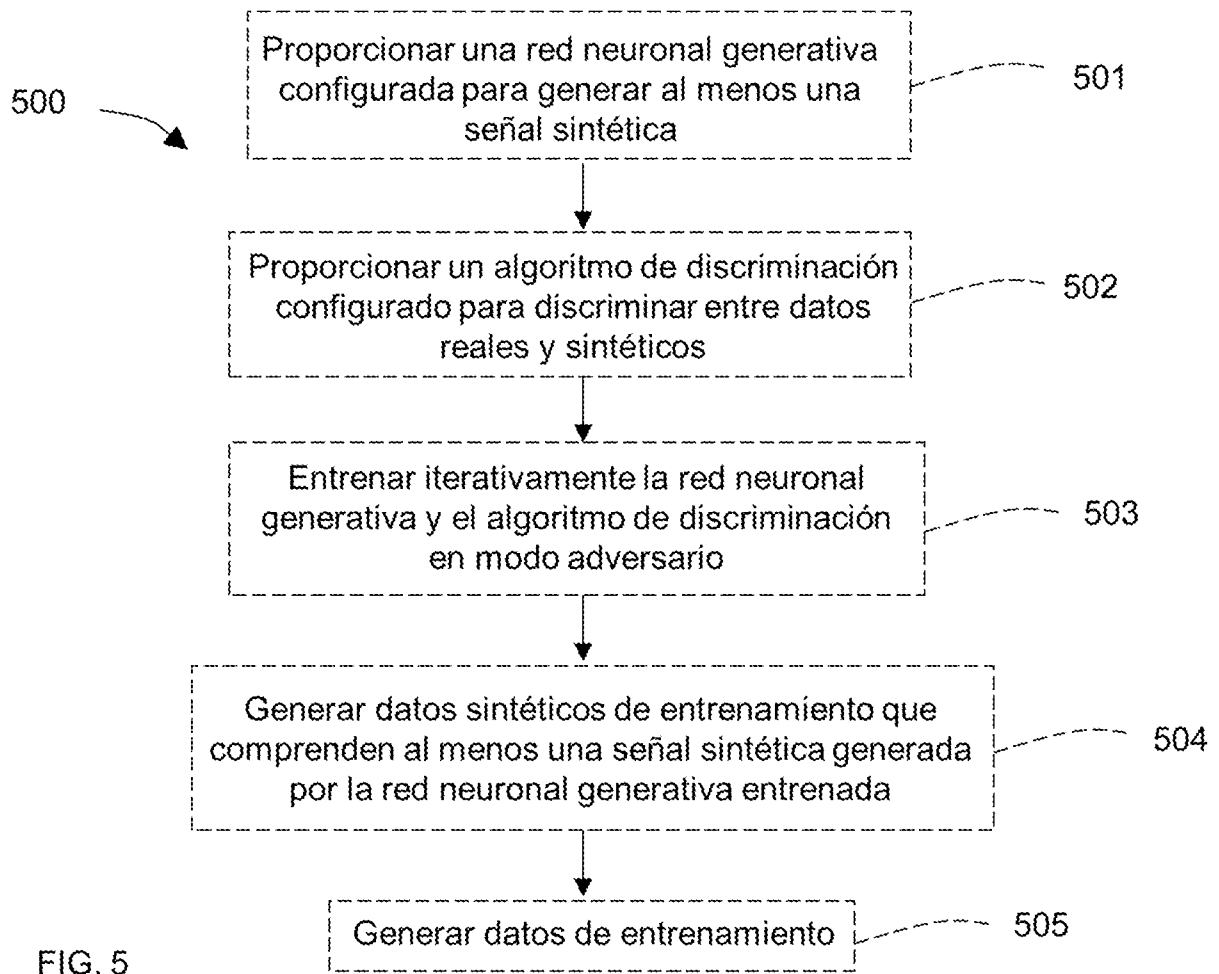


FIG. 4



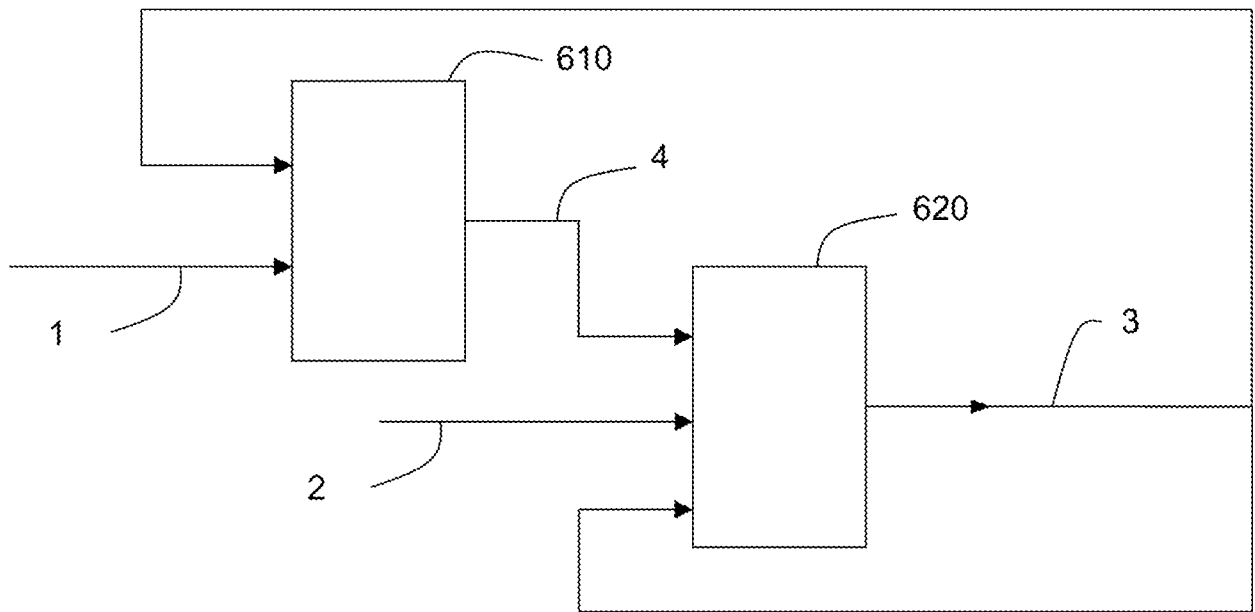


FIG. 6

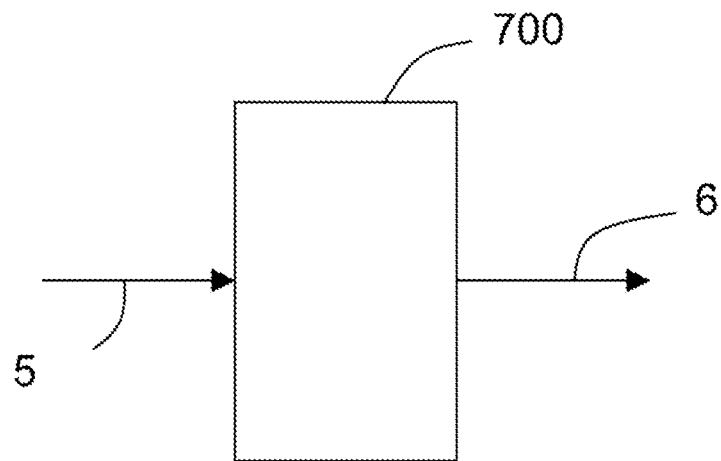


FIG. 7

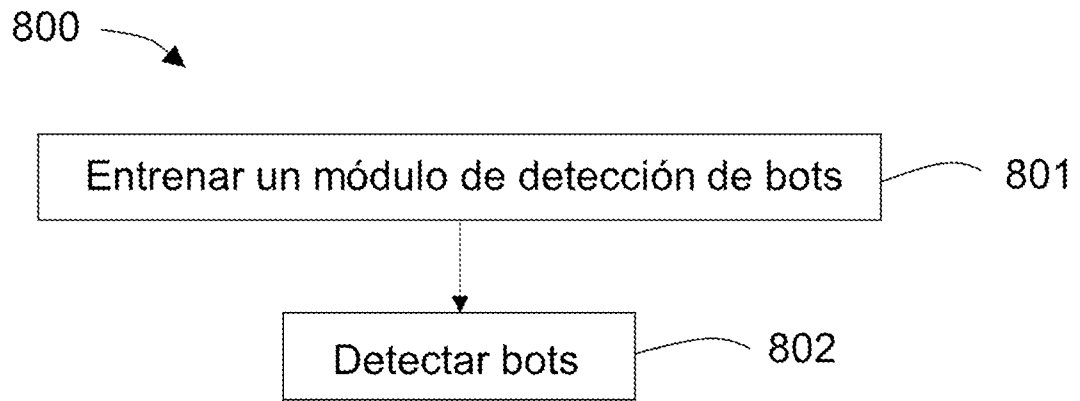


FIG. 8

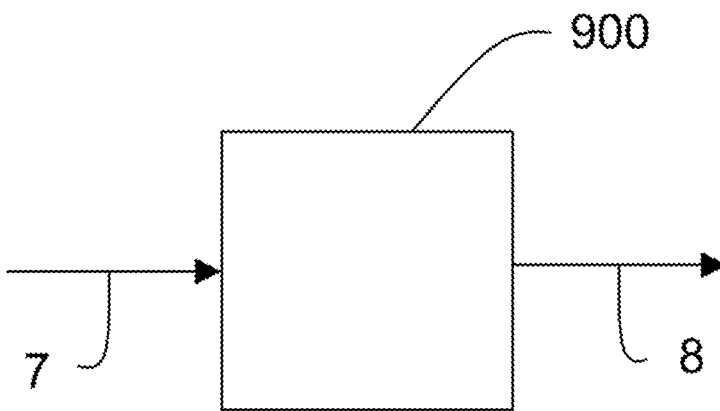


FIG. 9

REFERENCIAS CITADAS EN LA DESCRIPCIÓN

5 *Esta lista de referencias citadas por el solicitante es únicamente para la comodidad del lector. No forma parte del documento de la patente europea. A pesar del cuidado tenido en la recopilación de las referencias, no se pueden excluir errores u omisiones y la EPO niega toda responsabilidad en este sentido.*

Documentos de patentes citados en la descripción

10

- US 10 496 809.

Literatura diferente de patentes citada en la descripción

15

- Android-GAN: Defending against android pattern attacks using multi-modal generative network as anomaly detector. Expert Systems with Applications, publicado el 10/09/2019 por SANG-YUN S. et al.
- SensoryGANs: An Effective Generative Adversarial Framework for Sensorbased Human Activity Recognition, publicado el 7 de julio de 2018 en la Conferencia Internacional Conjunta sobre Redes Neuronales (IJCNN) IEEE, de

20

WANG JIWEI et al.