(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 804 763**

(51) Int. CI.:

G06F 21/46 (2013.01)
H04L 9/08 (2006.01)
H04L 9/32 (2006.01)
H04L 29/06 (2006.01)

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(86) Fecha de presentación y número de la solicitud internacional: **15.04.2015 PCT/US2015/026017**

(87) Fecha y número de publicación internacional: **22.10.2015 WO15160983**

(96) Fecha de presentación y número de la solicitud europea: **15.04.2015 E 15780274 (5)**

(97) Fecha y número de publicación de la concesión europea: **03.06.2020 EP 3132371**

(54) Título: **Método y aparato de detección de contraseña débil**

(30) Prioridad:

16.04.2014 CN 201410153728

(45) Fecha de publicación y mención en BOPI de la traducción de la patente:
09.02.2021

(73) Titular/es:

ADVANCED NEW TECHNOLOGIES CO., LTD. (100.0%)
Cayman Corporate Centre, 27 Hospital Road George Town, Grand Cayman KY1-9008, KY

(72) Inventor/es:

ZHANG, WEN

(74) Agente/Representante:

ARIAS SANZ, Juan

DESCRIPCIÓN

Método y aparato de detección de contraseña débil

Campo técnico

La presente divulgación se refiere al campo de la tecnología de Internet y, en particular, a métodos y aparatos de detección de una contraseña débil.

Antecedentes

En el entorno de Internet existente, la información relacionada con la identidad de usuarios ya no es información privada, y la seguridad de datos y contraseñas de los usuarios se ve afectada de forma grave. Al establecer contraseñas, algunos usuarios usan contraseñas que son demasiado simples o establecen contraseñas usando información que está asociada a sí mismos o asociada a sus familiares o amigos para recordar las contraseñas fácilmente, y tales contraseñas se descifran fácilmente.

En la actualidad, un método comúnmente visto para detectar una contraseña débil de un usuario incluye principalmente: determinar si una contraseña establecida por un usuario es demasiado simple usando un diccionario de contraseñas débiles comúnmente usadas; o determinar si una contraseña establecida por el usuario está relacionada con la información de identidad del mismo basándose en información relacionada con la identidad del usuario, como un número de tarjeta de identidad, un número de teléfono móvil, un número de tarjeta bancaria, etc.

Una tecnología existente de detección de una contraseña débil de un usuario solo puede realizar la detección basándose en contraseñas débiles usadas comúnmente e información relacionada con la identidad del usuario. Sin embargo, algunos usuarios siempre usan información de identidad de las personas que tienen una estrecha relación con ellos para establecer contraseñas, y contraseñas débiles que se establecen en tales casos no pueden detectarse por la tecnología existente, y por tanto no se logra mejorar aún más la seguridad de las contraseñas de los usuarios.

El documento US2014068731 (A1) da a conocer un método, sistema o programa informático que puede usarse para administrar la fortaleza de la contraseña que incluye recibir una contraseña en un sistema de procesamiento de datos para un usuario, filtrar información personal sobre el usuario desde múltiples fuentes de datos independientes accesibles a través de una red informática, calcular la fortaleza de la contraseña por el sistema de procesamiento de datos usando un algoritmo que compara la contraseña con la información personal filtrada sobre el usuario, y presentar comentarios al usuario a través de una interfaz de usuario en un elemento de visualización de sistema de procesamiento de datos con respecto a la fortaleza de la contraseña calculada.

Sumario

Este sumario se proporciona para introducir una selección de conceptos de forma simplificada que además se describen más adelante en la descripción detallada. Este sumario no se pretende que identifique todas las características clave o características esenciales de la materia objeto reivindicada, ni se pretende que se use por sí solo como ayuda en la determinación del alcance de la materia objeto reivindicada. El término “técnicas”, por ejemplo, puede referirse a dispositivo(s), sistema(s), método(s) y/o instrucciones legibles por ordenador según lo permitido por el contexto anterior y a lo largo de la presente divulgación.

En un primer aspecto, la presente divulgación proporciona un método implementado por uno o más dispositivos informáticos tal como se define en la reivindicación 1. En un segundo aspecto, la presente divulgación proporciona un aparato para detectar una contraseña débil tal como se define en la reivindicación 7. En un tercer aspecto, la presente divulgación proporciona uno o más medios legibles por ordenador tal como se define en la reivindicación 11. Las características opcionales se definen en las reivindicaciones dependientes.

Un objetivo principal de la presente divulgación es proporcionar un método y un aparato de detección de una contraseña débil para resolver el fallo de detectar una contraseña que se establece por un usuario usando información de identidad de otros usuarios que están relacionados con el usuario en la tecnología existente.

La presente divulgación da a conocer un método para detectar una contraseña débil, que incluye: recibir una contraseña que va a detectarse; adquirir un conjunto de información de identidad de un usuario de la contraseña que va a detectarse, el conjunto de información de identidad que incluye una pluralidad de elementos de información de identidad del usuario y de usuarios relacionados con el mismo; detectar si la información de identidad asociada a la contraseña que va a detectarse existe en el conjunto de información de identidad; y determinar que la contraseña que va a detectarse es una contraseña débil si la información de identidad asociada a la contraseña que va a detectarse existe en el conjunto de información de identidad.

La presente divulgación también da a conocer un aparato de detección de una contraseña débil, que incluye: módulo de recepción usado para recibir una contraseña que va a detectarse; un módulo de adquisición usado para adquirir un

conjunto de información de identidad de un usuario de la contraseña que va a detectarse, el conjunto de información de identidad que incluye una pluralidad de elementos de información de identidad del usuario y de usuarios relacionados con el mismo; un módulo de detección usado para detectar si la información de identidad asociada a la contraseña que va a detectarse existe en el conjunto de información de identidad; y un módulo de determinación usado para determinar que la contraseña que va a detectarse es una contraseña débil si la información de identidad asociada a la contraseña que va a detectarse existe en el conjunto de información de identidad.

En comparación con la tecnología existente, la solución técnica de la presente divulgación puede detectar si una contraseña que va a detectarse se establece por un usuario usando información de identidad del mismo o información de identidad de un usuario que está asociado de manera estrecha al mismo, determinando así si la contraseña que va a detectarse es débil o propensa a descifrarse, y por tanto, mejorando aún más la seguridad de la contraseña del usuario.

Breve descripción de los dibujos

Los dibujos adjuntos descritos en el presente documento se proporcionan para el entendimiento adicional de la presente divulgación, y constituyen una parte de la presente divulgación. Las realizaciones a modo de ejemplo de la presente divulgación y la descripción de las mismas se usan para ilustrar la presente divulgación, y no deben interpretarse como limitaciones inadecuadas a la presente divulgación. En los dibujos adjuntos:

La figura 1 es un diagrama de flujo de un método de detección de una contraseña débil según una realización de la presente divulgación.

La figura 2 es un diagrama de flujo de un procedimiento de adquisición de un conjunto de información de identidad de un usuario de una contraseña que va a detectarse según una realización de la presente divulgación.

La figura 3 es un diagrama de flujo de un procedimiento para detectar si la información de identidad asociada a una contraseña que va a detectarse existe en un conjunto de información de identidad según una realización de la presente divulgación.

La figura 4 es un diagrama de flujo de un procedimiento para determinar si existe una contraseña de detección que es idéntica a una contraseña que va a detectarse en una o más contraseñas de detección separadas a partir de cada elemento de información de identidad según una realización de la presente divulgación.

La figura 5 es un diagrama de flujo de un aparato de detección de una contraseña débil según una realización de la presente divulgación.

Descripción detallada

Una idea de la presente divulgación es determinar uno o más usuarios relacionados que están asociados de manera estrecha a un usuario basándose en actividades del usuario para adquirir una pluralidad de elementos de información de identidad del usuario y de usuarios asociados al mismo, y determinar si una contraseña establecida por el usuario está asociada a la pluralidad de elementos de información de identidad basándose en la pluralidad de elementos de información de identidad, determinando así si la contraseña que va a detectarse es una contraseña débil.

Con el fin de aclarar los objetivos, soluciones técnicas y ventajas de la presente divulgación, las soluciones técnicas de la presente divulgación se describen en el presente documento de manera clara y completa con referencia a las realizaciones a modo de ejemplo y los dibujos adjuntos correspondientes de la presente divulgación. Aparentemente, las realizaciones descritas son simplemente una parte y no toda de las realizaciones de la presente divulgación. Basándose en las realizaciones en la presente divulgación, todas las demás realizaciones obtenidas por un experto en la técnica sin realizar ningún esfuerzo creativo pertenecerán al alcance de protección de la presente divulgación.

Según una realización de la presente divulgación, se proporciona un método de detección de una contraseña débil.

Haciendo referencia a la figura 1, la figura 1 es un diagrama de flujo de un método de detección de una contraseña débil según una realización de la presente divulgación.

En S101, se recibe una contraseña que va a detectarse.

La contraseña que va a detectarse puede ser una contraseña de inicio de sesión usada cuando un usuario inicia sesión en una aplicación como una aplicación cliente o una aplicación de página web, una contraseña de verificación usada cuando el usuario usa la aplicación cliente o la aplicación de página web para realizar una operación particular (la operación particular que se basa en un servicio proporcionado por un servidor), por ejemplo, una contraseña de pago durante una transacción de pago, etc. Debe entenderse que la contraseña que va a detectarse no está limitada a la misma, sino que puede ser cualquier contraseña que necesite detectarse.

En S102, se obtiene un conjunto de información de identidad de un usuario de la contraseña que va a detectarse. El conjunto de información de identidad que incluye una pluralidad de elementos de información de identidad del usuario y de usuarios asociados al mismo.

Con el fin de ilustrar este bloque de método con mayor claridad, se describe un ejemplo de implementación opcional de este bloque de método con referencia a la figura 2.

Como se muestra en la figura 2, la figura 2 es un diagrama de flujo de un bloque de método de adquisición de un conjunto de información de identidad de un usuario de la contraseña que va a detectarse según una realización de la presente divulgación.

En S201, se determinan uno o más usuarios asociados del usuario basándose en datos de comportamiento del usuario.

El uno o más usuarios asociados del usuario pueden ser uno o más usuarios asociados de manera estrecha al usuario. Los usuarios asociados de manera estrecha al usuario pueden incluir, por ejemplo, familiares o amigos del usuario, etc. Los datos de comportamiento del usuario pueden incluir: datos de comportamiento de actividades de interacción del usuario, por ejemplo, usuarios que tienen una actividad de transacción (por ejemplo, una transferencia, que incluye la transferencia de fondos a otros usuarios o recepción de fondos transferidos de otros usuarios) con el usuario; y datos de comportamiento de actividades de navegación del usuario, por ejemplo, los usuarios por los que se ha navegado por el usuario.

Específicamente, las estadísticas sobre los datos de comportamiento del usuario pueden recogerse y analizarse para adquirir uno o más usuarios asociados de la manera más estrecha al usuario como usuarios asociados del usuario. Un número del uno o más usuarios asociados pueden determinarse según situaciones específicas. Por ejemplo, mediante la recopilación de estadísticas sobre usuarios que han interactuado con el usuario, un número predeterminado de usuarios (TopN) que han interactuado con el usuario con mayor frecuencia puede tratarse como usuarios asociados del usuario. Alternativamente, uno o más usuarios que han interactuado con el usuario durante más de un número predeterminado de veces pueden tratarse como usuarios asociados del usuario.

En S202, se adquieren uno o más elementos de información de identidad del usuario y uno o más elementos de información de identidad de cada usuario asociado en el uno o más usuarios asociados para formar el conjunto de información de identidad del usuario. Cada elemento de información de identidad puede hacerse de múltiples caracteres (por ejemplo, dígitos, letras), y la información de identidad puede incluir información como un nombre, un número de tarjeta de identidad, un número de teléfono móvil, un número de cuenta bancaria/número de tarjeta, etc. Específicamente, pueden adquirirse uno o más elementos de información de identidad en la información de identidad mencionada anteriormente del usuario y uno o más elementos de información de identidad en la información de identidad mencionada anteriormente de cada usuario asociado del usuario para formar el conjunto de información de identidad del usuario.

Volviendo a la figura 1, se realiza la detección para saber si la información de identidad asociada a la contraseña que va a detectarse existe en el conjunto de información de identidad en S103. Específicamente, se realiza la detección para saber si la contraseña que va a detectarse se establece por el usuario usando la información de identidad del mismo o la información de identidad de un usuario que está asociado de manera estrecha al mismo.

Para ilustrar de forma más clara este bloque de método, se describe un ejemplo de implementación opcional de este bloque de método con referencia a la figura 3.

Haciendo referencia a la figura 3, la figura 3 muestra un diagrama de flujo de un bloque de método para detectar si la información de identidad asociada a la contraseña que va a detectarse existe en el conjunto de información de identidad (es decir, S103) según una realización de la presente divulgación. Debe indicarse que la figura 3 muestra un diagrama de flujo para determinar si la información de identidad está asociada a la contraseña que va a detectarse para cada elemento de información de identidad.

En S301, cada elemento de información de identidad del conjunto de información de identidad se separa en una o más contraseñas de detección basándose en una longitud de la contraseña que va a detectarse.

Según una realización de la presente divulgación, una longitud de la contraseña que va a detectarse puede adquirirse primero de un sistema. Cada elemento de información de identidad se separa entonces en una o más contraseñas de detección que tienen la misma longitud que la contraseña que va a detectarse basándose en la longitud de la contraseña. La una o más contraseñas de detección que se separan a partir de cada elemento de información de identidad se usan para su comparación con la contraseña que va a detectarse en un siguiente bloque de método para determinar si ese elemento de información de identidad está asociado a la contraseña.

Específicamente, para cualquier elemento de información de identidad, la información de identidad puede separarse en un número de contraseñas de detección (L-M+1) cuya longitud es M según un orden de caracteres (como dígitos,

letras) en la información de identidad, en el que L es la longitud de la información de identidad, y M es la longitud de la contraseña que va a detectarse. Por ejemplo, suponiendo que la longitud de la contraseña que va a detectarse es de seis, un elemento de información de identidad “123456789” puede separarse en cuatro contraseñas de detección: “123456”, “234567”, “345678” y “456789”.

En S302, se hace una determinación para saber si existe una contraseña de detección que sea idéntica a la contraseña que va a detectarse en la una o más contraseñas de detección que se separan a partir de cada elemento de información de identidad.

Haciendo referencia a la figura 4, la figura 4 muestra un diagrama de flujo de un bloque de método para determinar si existe una contraseña de detección que sea idéntica a la contraseña que va a detectarse en la una o más contraseñas de detección separadas a partir de cada elemento de información de identidad (es decir, S302) según una realización de la presente divulgación.

Como se muestra en la figura 4, para una o más contraseñas de detección separadas a partir de cada elemento de información de identidad, la una o más contraseñas de detección se encriptan de manera individual usando una clave secreta particular para generar uno o más textos cifrados de detección correspondientes a la una o más contraseñas de detección en S401.

Específicamente, cuando el usuario introduce una contraseña (por ejemplo, una entrada enviada cuando el usuario establece una contraseña o una entrada enviada cuando el usuario usa una contraseña para realizar una verificación relacionada), (el sistema) puede usar una clave secreta particular para encriptar la contraseña introducida por el usuario para generar un texto cifrado de la contraseña para evitar que se robe la contraseña del usuario con el fin de garantizar la seguridad de la contraseña del usuario. Por tanto, la contraseña introducida por el usuario recibida (por el servidor) o la contraseña almacenada preestablecida por el usuario (en el servidor) es el texto cifrado que está encriptado usando la clave secreta particular. Por tanto, cuando se recibe la contraseña que va a detectarse, lo que realmente se recibe es el texto cifrado generado al encriptar la contraseña que va a detectarse usando la clave secreta particular. Por tanto, puede adquirirse la clave secreta particular. La una o más contraseñas de detección se encriptan de manera individual usando la clave secreta particular para generar uno o más textos cifrados de detección correspondientes a cada contraseña de detección, con el fin de facilitar la comparación entre el uno o más textos cifrados de detección y el texto cifrado de la contraseña que va a detectarse para determinar si existe un texto cifrado de detección que sea idéntico al texto cifrado de la contraseña que va a detectarse.

En S402, se hace una determinación en cuanto a si existe un texto cifrado de detección que sea idéntico a un texto cifrado de la contraseña que va a detectarse en el uno o más textos cifrados de detección. El texto cifrado de la contraseña que va a detectarse se genera encriptando la contraseña que va a detectarse usando la clave secreta particular.

Específicamente, el uno o más textos cifrados de detección pueden compararse con el texto cifrado de la contraseña que va a detectarse, para determinar si cada texto cifrado de detección es idéntico al texto cifrado de la contraseña que va a detectarse uno por uno.

En S403, si existe un texto cifrado de detección que es idéntico al texto cifrado de la contraseña que va a detectarse en el uno o más textos cifrados de detección, se hace una determinación de que existe una contraseña de detección que es idéntica a la contraseña que va a detectarse en la una o más contraseñas de detección.

El uno o más textos cifrados de detección y el texto cifrado de la contraseña que va a detectarse se generan mediante encriptación usando la misma clave secreta (es decir, la clave secreta particular). Por tanto, al detectar cualquier texto cifrado de detección que es idéntico al texto cifrado de la contraseña que va a detectarse, se hace una determinación de que una contraseña de detección correspondiente al texto cifrado de detección (es decir, la contraseña de detección a partir de la cual se genera el texto cifrado de detección) es idéntica a la contraseña que va a detectarse. Además, se hace una determinación adicional de que existe una contraseña de detección que es idéntica a la contraseña que va a detectarse en la una o más contraseñas de detección. Si no existe texto cifrado de detección que sea idéntico al texto cifrado de la contraseña que va a detectarse en el uno o más textos cifrados de detección, se hace una determinación de que no existe una contraseña de detección que sea idéntica a la contraseña que va a detectarse en la una o más contraseñas de detección en S404.

Volviendo a la figura 3, después de que cada elemento de información de identidad en el conjunto de información de identidad ha pasado de manera individual por los bloques de método S401-S404 tal como se describieron anteriormente, si se encuentra que existe una contraseña de detección que es la misma que la contraseña que va a detectarse en la una o más contraseñas de detección separadas a partir de cualquier elemento de información de identidad, se hace una determinación de que este elemento de información de identidad está asociada a la contraseña que va a detectarse en el S303, es decir, se hace una determinación de que la información de identidad asociada a la contraseña que va a detectarse existe en el conjunto de información de identidad. Si no se encuentra que exista ninguna contraseña de detección idéntica a la contraseña que va a detectarse en la una o más contraseñas de detección separadas de un elemento de información de identidad, se hace una determinación de que este elemento

de información de identidad no está asociado a la contraseña que va a detectarse en S304.

Si no existe una contraseña de detección que sea idéntica a la contraseña que va a detectarse en la una o más contraseñas de detección separadas de cualquier elemento de información de identidad, se hace una determinación de que no existe información de identidad asociada a la contraseña que va a detectarse en el conjunto de información de identidad.

Se describe una implementación del bloque de método S103 con referencia a las figuras 3 y 4 anteriormente en detalle, y se vuelve a la figura 1 de aquí en adelante en el presente documento para su posterior descripción. En S104, si la información de identidad asociada a la contraseña que va a detectarse existe en el conjunto de información de identidad, se hace una determinación de que la contraseña que va a detectarse es una contraseña débil.

Específicamente, la pluralidad de elementos de información de identidad en el conjunto de información de identidad se procesa según los bloques de método S301-S304 uno por uno para determinar si cada elemento de información de identidad está asociado a la contraseña que va a detectarse por separado. Si algún elemento de información de identidad en el conjunto de información de identidad está asociado a la contraseña que va a detectarse, esto indica que el usuario establece la contraseña que va a detectarse usando ese elemento de información de identidad. Como tal, la contraseña que va a detectarse puede ser propensa a descifrarse y, por tanto, es una contraseña débil.

Si no existe información de identidad asociada a la contraseña que va a detectarse en el conjunto de información de identidad, esto indica que la contraseña que va a detectarse no está asociada a ningún elemento de información de identidad en el conjunto de información de identidad. En otras palabras, el usuario no usa ningún elemento de información de identidad en el conjunto de información de identidad para establecer la contraseña que va a detectarse. Como tal, se hace una determinación de que la contraseña que va a detectarse pasa la detección en S105, es decir, la contraseña que va a detectarse no es una contraseña débil, y pasa la detección.

La solución técnica de la presente divulgación puede usarse para detectar si una contraseña de un usuario se establece por el usuario usando información de identidad del usuario o información de identidad de un usuario asociado relacionado de manera estrecha con el mismo, y puede usarse antes o después de llevar a cabo una detección de contraseña débil que emplea un diccionario de contraseñas débiles.

La presente divulgación además proporciona un aparato de detección de una contraseña débil.

La figura 5 muestra de manera esquemática un diagrama de bloques estructural de un aparato de detección de una contraseña débil según una realización de la presente divulgación.

Según una realización de la presente divulgación, el aparato 500 incluye: un módulo de recepción 501, un módulo de adquisición 502, un módulo de detección 503 y un módulo de determinación 504.

El módulo de recepción 501 puede usarse para recibir una contraseña que va a detectarse.

El módulo de adquisición 502 puede usarse para la adquisición de un conjunto de información de identidad de un usuario de la contraseña que va a detectarse, incluyendo el conjunto de información de identidad múltiples elementos de información de identidad del usuario y de usuarios asociados al mismo.

El módulo de detección 503 puede usarse para detectar si la información de identidad asociada a la contraseña que va a detectarse existe en el conjunto de información de identidad.

El módulo de determinación 504 puede usarse para determinar que la contraseña que va a detectarse es una contraseña débil si la información de identidad asociada a la contraseña que va a detectarse existe en el conjunto de información de identidad.

Según una realización de la presente divulgación, el módulo de adquisición 502 puede incluir: un módulo de determinación de usuario asociado 505 y un módulo de adquisición de información de identidad 506.

El módulo de determinación de usuario asociado 505 puede usarse para determinar uno o más usuarios asociados del usuario basándose en datos de comportamiento del usuario.

El módulo de adquisición de información de identidad 506 puede usarse para obtener uno o más elementos de información de identidad del usuario y uno o más elementos de información de identidad de cada usuario asociado en el uno o más usuarios asociados para formar el conjunto de información de identidad del usuario.

Según una realización de la presente divulgación, el módulo de detección 503 puede incluir: un módulo de separación 507, un módulo de evaluación 508 y un primer módulo de determinación 509.

El módulo de separación 507 puede usarse para dividir cada elemento de información de identidad en el conjunto de

información de identidad en una o más contraseñas de detección según una longitud de la contraseña que va a detectarse.

El módulo de evaluación 508 puede usarse para determinar si existe una contraseña de detección que sea idéntica a la contraseña que va a detectarse en la una o más contraseñas de detección divididas a partir de cada elemento de información de identidad.

El primer módulo de determinación 509 puede usarse para determinar que un elemento de información de identidad está asociado a la contraseña que va a detectarse cuando existe una contraseña de detección que es idéntica a la contraseña que va a detectarse en una o más contraseñas de detección separadas del elemento de información de identidad.

Según una realización de la presente divulgación, el módulo de evaluación 508 puede incluir: un submódulo de generación 510, un submódulo de evaluación 511 y un submódulo de determinación 512.

El submódulo de generación 510 puede usarse para encriptar de manera individual la una o más contraseñas de detección usando una clave secreta particular para generar uno o más textos cifrados de detección correspondientes a una o más contraseñas de detección.

El submódulo de evaluación 511 puede usarse para determinar si existe un texto cifrado de detección que sea idéntico a un texto cifrado de la contraseña que va a detectarse en el uno o más textos cifrados de detección, en el que el texto cifrado de la contraseña que va a detectarse se genera mediante la encriptación de la contraseña que va a detectarse usando la clave secreta particular.

El submódulo de determinación 512 puede usarse para determinar que existe una contraseña de detección que sea idéntica a la contraseña que va a detectarse en la una o más contraseñas de detección si existe un texto cifrado de detección que es idéntico al texto cifrado de la contraseña que va a detectarse en el uno o más textos cifrados de detección.

Dado que las funciones implementadas por el aparato 500 de esta realización corresponden básicamente a las realizaciones de método como se muestra en las figuras 1-4 anteriormente, puede hacerse referencia a partes que no se describen en detalle en esta realización con respecto a la descripción relacionada en las anteriores realizaciones, y no se describen de manera redundante en el presente documento.

Además, el aparato 500 puede implementarse como uno o más dispositivos informáticos. En una configuración típica, un dispositivo informático incluye uno o más procesadores/unidades centrales de procesamiento (CPU) 513, una interfaz de entrada/salida 514, una interfaz de red 515 y una memoria 516.

La memoria 516 puede incluir una forma de medio legible por ordenador, como memoria volátil, memoria de acceso aleatorio (RAM) y/o memoria no volátil, como memoria de solo lectura (ROM) o memoria flash RAM. La memoria 516 es un ejemplo de un medio legible por ordenador.

El medio legible por ordenador puede incluir un tipo permanente o no permanente, un medio extraíble o no extraíble, que puede lograr el almacenamiento de información usando cualquier método o tecnología. La información puede incluir una instrucción legible por ordenador, una estructura de datos, un módulo de programa u otros datos. Ejemplos de medios de almacenamiento por ordenador incluyen, pero no se limitan a, memoria de cambio de fase (PRAM), memoria estática de acceso aleatorio (SRAM), memoria dinámica de acceso aleatorio (DRAM), otros tipos de memoria de acceso aleatorio (RAM), memoria de solo lectura (ROM), memoria programable de solo lectura borrable electrónicamente (EEPROM), memoria flash rápida u otra tecnología de almacenamiento interno, memoria de solo lectura en disco compacto (CD-ROM), disco versátil digital (DVD) u otro almacenamiento óptico, cinta magnética de casete, almacenamiento en disco magnético u otros dispositivos de almacenamiento magnético, o cualquier otro medio de no transmisión, que pueda usarse para almacenar información a la que pueda accederse por un dispositivo informático. Tal como se define en el presente documento, los medios legibles por ordenador no incluyen medios transitorios, como señales de datos moduladas y ondas portadoras.

La memoria 516 puede incluir el módulo de programa 517 y los datos de programa 518. Los módulos y/o submódulos anteriores pueden incluirse en la memoria 516, por ejemplo, el módulo de programa 517. Pueden encontrarse detalles de estos módulos y submódulos en la descripción anterior y, por lo tanto, no se describen de forma redundante en el presente documento.

Debe indicarse además que, términos como “comprender”, “incluir” o cualquier otra variación de los mismos tienen por objeto cubrir las inclusiones no exclusivas. El proceso, método, producto o aparato que incluye una serie de elementos no solo incluye esos elementos, sino que también incluye otros elementos que no están enumerados de forma explícita, o incluye además elementos que ya existían tal dicho proceso, método, producto o aparato. En una condición sin limitaciones adicionales, un elemento definido por la frase “incluyen un/una...” no excluye la existencia de ningún otro elemento similar del proceso, método, producto o aparato.

Un experto en la técnica debe entender que las realizaciones de la presente divulgación pueden proporcionarse como un método, un sistema o un producto de programa informático. Por tanto, la presente divulgación puede implementarse como una realización de hardware completamente, una realización de software completamente, o una realización que es una combinación de software y hardware. Además, la presente divulgación puede ser en forma de producto de programa informático implementado en uno o más medios de almacenamiento que pueden usarse por ordenador (incluyendo, pero sin limitarse a, un dispositivo de almacenamiento de disco magnético, un CD-ROM, un dispositivo de almacenamiento óptico, y similares), incluyendo códigos de programa que pueden usarse por ordenador.

Las descripciones anteriores son meramente realizaciones a modo de ejemplo de la presente divulgación, y no están destinadas a limitar la presente divulgación. Para un experto en la técnica, la presente divulgación puede tener diversas modificaciones y variaciones. Cualquiera de las modificaciones, sustituciones equivalentes, mejoras o similares que se hagan sin apartarse de la presente divulgación deben incluirse en el alcance de las reivindicaciones de la presente divulgación.

REIVINDICACIONES

1. Un método implementado por uno o más dispositivos informáticos, comprendiendo el método:

recibir (S101) una contraseña que va a detectarse;

adquirir (S102) un conjunto de información de identidad de un usuario de la contraseña que va a detectarse, incluyendo el conjunto de información de identidad una pluralidad de elementos de información de identidad del usuario y de usuarios asociados del mismo;

detectar (S103) si la información de identidad asociada a la contraseña que va a detectarse existe en el conjunto de información de identidad; y

determinar si la contraseña que va a detectarse es una contraseña débil basándose al menos en parte en el resultado de la detección,

en el que la detección (S103) comprende:

dividir (S301) cada elemento de información de identidad en el conjunto de información de identidad en una o más contraseñas de detección basándose en una longitud de la contraseña que va a detectarse; y

determinar (S302) si existe una contraseña de detección que es idéntica a la contraseña que va a detectarse en la una o más contraseñas de detección divididas a partir de cada elemento de información de identidad.

2. El método según la reivindicación 1, que comprende además determinar (S104) que la contraseña que va a detectarse es la contraseña débil en respuesta a la detección de que la información de identidad asociada a la contraseña que va a detectarse existe en el conjunto de información de identidad.

3. El método según la reivindicación 1, que comprende además determinar (S105) que la contraseña que va a detectarse no es la contraseña débil en respuesta a la detección de que no existe información de identidad asociada a la contraseña que va a detectarse en el conjunto de información de identidad.

4. El método según cualquier reivindicación anterior, en el que adquirir (S102) el conjunto de información de identidad del usuario de la contraseña que va a detectarse comprende:

determinar (S201) uno o más usuarios asociados del usuario basándose en datos de comportamiento del usuario; y

adquirir (S202) uno o más elementos de información de identidad del usuario y uno o más elementos de información de identidad de cada usuario asociado del uno o más usuarios asociados para formar el conjunto de información de identidad del usuario.

5. El método según cualquier reivindicación anterior, que comprende además determinar que:

un elemento de información de identidad está asociado a la contraseña que va a detectarse si existe una contraseña de detección que sea idéntica a la contraseña que va a detectarse en una o más contraseñas de detección divididas del elemento de información de identidad; o

no está asociada ninguna información de identidad a la contraseña que va a detectarse si no se encuentra que exista ninguna contraseña de detección idéntica a la contraseña que va a detectarse en la una o más contraseñas de detección divididas a partir de cada elemento de información de identidad.

6. El método según cualquier reivindicación anterior, en el que determinar si la contraseña de detección que es idéntica a la contraseña que va a detectarse existe en la una o más contraseñas de detección divididas a partir de cada elemento de información de identidad comprende:

encriptar de manera individual (S401) la una o más contraseñas de detección usando una clave secreta particular para generar uno o más textos cifrados de detección correspondientes a la una o más contraseñas de detección; y

determinar (S402) si existe un texto cifrado de detección que sea idéntico a un texto cifrado de la contraseña que va a detectarse en el uno o más textos cifrados de detección, en el que el texto cifrado de la contraseña que va a detectarse se genera encriptando la contraseña que va a detectarse usando la clave secreta particular.

7. Un aparato (500) para detectar una contraseña débil, que comprende:

un módulo de recepción (501) usado para recibir una contraseña que va a detectarse;

un módulo de adquisición (502) usado para adquirir un conjunto de información de identidad de un usuario de la contraseña que va a detectarse, incluyendo el conjunto de información de identidad una pluralidad de elementos de información de identidad del usuario y de usuarios asociados del mismo;

un módulo de detección (503) usado para detectar si la información de identidad asociada a la contraseña que va a detectarse existe en el conjunto de información de identidad; y

un módulo de determinación (504) usado para determinar que la contraseña que va a detectarse es una contraseña débil si la información de identidad asociada a la contraseña que va a detectarse existe en el conjunto de información de identidad,

en el que el módulo de detección (503) comprende:

un módulo de separación (507) usado para separar cada elemento de información de identidad en el conjunto de información de identidad en una o más contraseñas de detección según una longitud de la contraseña que va a detectarse; y

un módulo de evaluación (508) usado para determinar si existe una contraseña de detección idéntica a la contraseña que va a detectarse en la una o más contraseñas de detección separadas a partir de cada elemento de información de identidad.

8. El aparato según la reivindicación 7, en el que el módulo de adquisición (502) comprende:

un módulo de determinación de usuario asociado (505) usado para determinar uno o más usuarios asociados del usuario basándose en datos de comportamiento del usuario; y

un módulo de adquisición de información de identidad (506) usado para adquirir uno o más elementos de información de identidad del usuario y uno o más elementos de información de identidad de cada usuario asociado en el uno o más usuarios asociados para formar el conjunto de información de identidad del usuario.

9. El aparato según la reivindicación 7 o la reivindicación 8, en el que el módulo de detección (503) comprende además:

un primer módulo de determinación (509) usado para determinar que un elemento de información de identidad está asociado a la contraseña que va a detectarse si la contraseña de detección idéntica a la contraseña que va a detectarse existe en una o más contraseñas de detección separadas a partir de la información de identidad.

10. El aparato según la reivindicación 9, en el que el módulo de evaluación (508) comprende:

un submódulo de generación (510) configurado para encriptar por separado la una o más contraseñas de detección usando una clave secreta particular para generar uno o más textos cifrados de detección correspondientes a la una o más contraseñas de detección;

un submódulo de evaluación (511) configurado para determinar si existe un texto cifrado de detección idéntico a un texto cifrado de la contraseña que va a detectarse en el uno o más textos cifrados de detección, en el que el texto cifrado de la contraseña que va a detectarse se genera encriptando la contraseña que va a detectarse usando la clave secreta particular; y

un submódulo de determinación (512) usado para determinar que la contraseña de detección idéntica a la contraseña que va a detectarse existe en la una o más contraseñas de detección si el texto cifrado de detección idéntico al texto cifrado de la contraseña que va a detectarse existe en el uno o más textos cifrados de detección.

11. Uno o más medios legibles por ordenador (516) que almacenan instrucciones ejecutables que, cuando se ejecutan por uno o más procesadores (513), provocan que el uno o más procesadores realicen actos que comprenden:

recibir (S101) una contraseña que va a detectarse;

adquirir (S102) un conjunto de información de identidad de un usuario de la contraseña que va a detectarse, incluyendo el conjunto de información de identidad una pluralidad de elementos de información de identidad del usuario y de usuarios asociados del mismo;

detectar (S103) si la información de identidad asociada a la contraseña que va a detectarse existe en el conjunto de información de identidad; y

determinar si la contraseña que va a detectarse es una contraseña débil basándose al menos en parte en el resultado de la detección,

en el que la detección (S103) comprende:

dividir (S301) cada elemento de información de identidad en el conjunto de información de identidad en una o más contraseñas de detección basándose en una longitud de la contraseña que va a detectarse; y

determinar (S302) si existe una contraseña de detección que sea idéntica a la contraseña que va a detectarse en la una o más contraseñas de detección divididas a partir de cada elemento de información de identidad.

12. El uno o más medios legibles por ordenador según la reivindicación 11, los actos que comprenden además:

determinar (S104) que la contraseña que va a detectarse es la contraseña débil en respuesta a la detección de que la información de identidad asociada a la contraseña que va a detectarse existe en el conjunto de información de identidad; o

determinar (S105) que la contraseña que va a detectarse no es la contraseña débil en respuesta a la detección de que no existe información de identidad asociada a la contraseña que va a detectarse en el conjunto de información de identidad.

13. El uno o más medios legibles por ordenador según la reivindicación 11 o la reivindicación 12, en el que adquirir (S102) el conjunto de información de identidad del usuario de la contraseña que va a detectarse comprende:

determinar (S201) uno o más usuarios asociados del usuario basándose en datos de comportamiento del usuario; y

adquirir (S202) uno o más elementos de información de identidad del usuario y uno o más elementos de información de identidad de cada usuario asociado del uno o más usuarios asociados para formar el conjunto de información de identidad del usuario.

14. El uno o más medios legibles por ordenador según cualquiera de las reivindicaciones 11 a 13, que comprende además determinar que:

un elemento de información de identidad está asociado a la contraseña que va a detectarse si existe una contraseña de detección que sea idéntica a la contraseña que va a detectarse en una o más contraseñas de detección divididas del elemento de información de identidad; o

no está asociada ninguna información de identidad a la contraseña que va a detectarse si no se encuentra que exista ninguna contraseña de detección idéntica a la contraseña que va a detectarse en la una o más contraseñas de detección divididas a partir de cada elemento de información de identidad.

15. El uno o más medios legibles por ordenador según la reivindicación 14, en el que determinar si la contraseña de detección que es idéntica a la contraseña que va a detectarse existe en la una o más contraseñas de detección divididas a partir de cada elemento de información de identidad comprende:

encriptar de manera individual (S401) la una o más contraseñas de detección usando una clave secreta particular para generar uno o más textos cifrados de detección correspondientes a la una o más contraseñas de detección; y

determinar (S402) si existe un texto cifrado de detección que sea idéntico a un texto cifrado de la contraseña que va a detectarse en el uno o más textos cifrados de detección, en el que el texto cifrado de la contraseña que va a detectarse se genera encriptando la contraseña que va a detectarse usando la clave secreta particular.

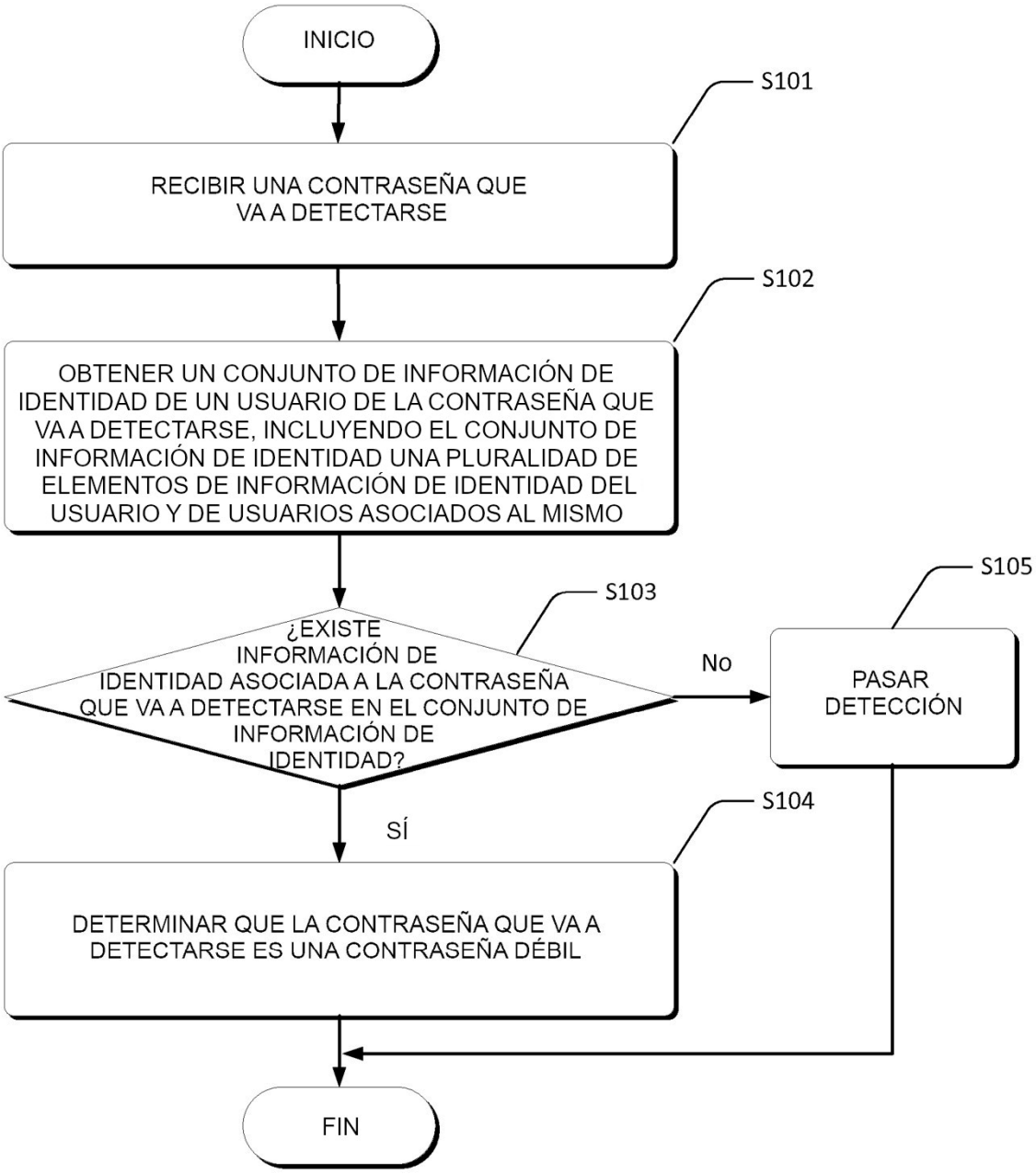
INICIO
S101
RECIBIR UNA CONTRASEÑA QUE VA A DETECTARSE
S102
OBTENER UN CONJUNTO DE INFORMACIÓN DE IDENTIDAD DE UN USUARIO DE LA CONTRASEÑA QUE VA A DETECTARSE, INCLUYENDO EL CONJUNTO DE INFORMACIÓN DE IDENTIDAD UNA PLURALIDAD DE ELEMENTOS DE INFORMACIÓN DE IDENTIDAD DEL USUARIO Y DE USUARIOS ASOCIADOS AL MISMO
S103
¿EXISTE INFORMACIÓN DE IDENTIDAD ASOCIADA A LA CONTRASEÑA QUE VA A DETECTARSE EN EL CONJUNTO DE INFORMACIÓN DE IDENTIDAD?
No
S105
PASAR DETECCIÓN
SÍ
S104
DETERMINAR QUE LA CONTRASEÑA QUE VA A DETECTARSE ES UNA CONTRASEÑA DÉBIL
FIN

FIG. 1

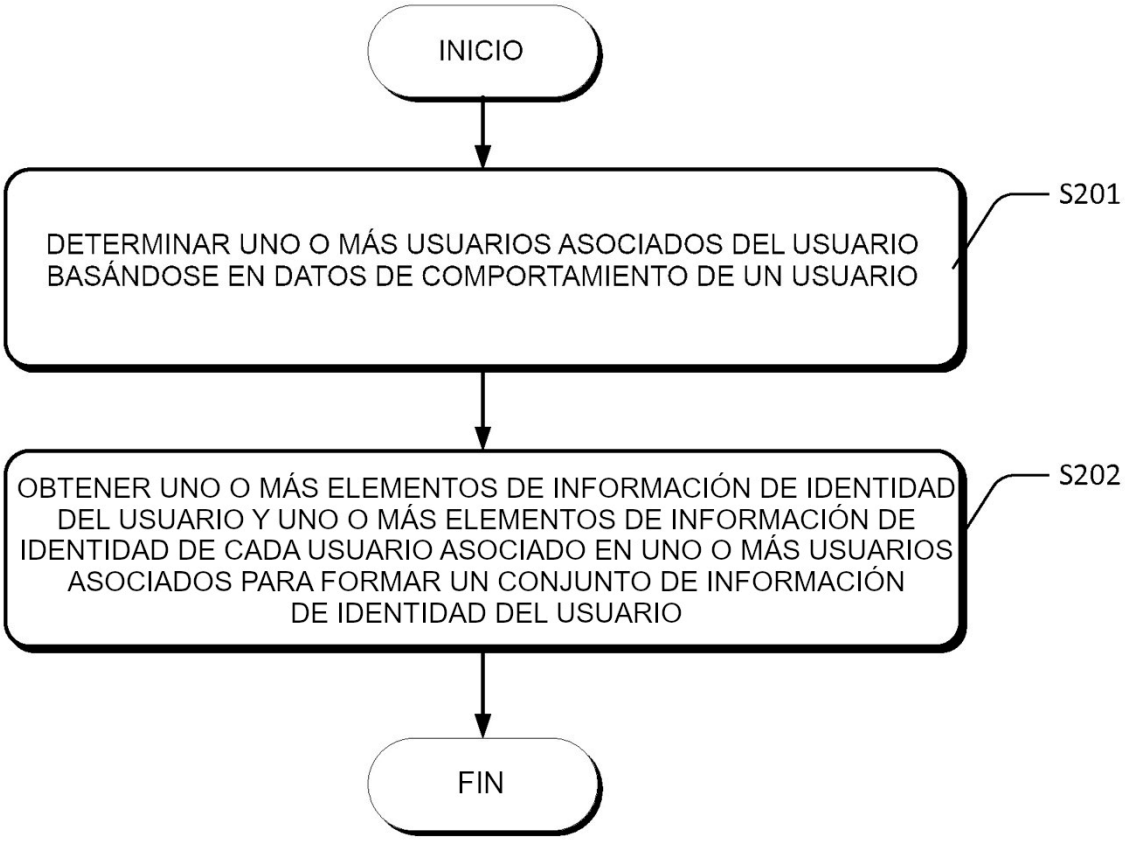
INICIO
DETERMINAR UNO O MÁS USUARIOS ASOCIADOS DEL USUARIO BASÁNDOSE EN DATOS DE COMPORTAMIENTO DE UN USUARIO
S201
OBTENER UNO O MÁS ELEMENTOS DE INFORMACIÓN DE IDENTIDAD DEL USUARIO Y UNO O MÁS ELEMENTOS DE INFORMACIÓN DE IDENTIDAD DE CADA USUARIO ASOCIADO EN UNO O MÁS USUARIOS ASOCIADOS PARA FORMAR UN CONJUNTO DE INFORMACIÓN DE IDENTIDAD DEL USUARIO
S202
FIN

FIG. 2

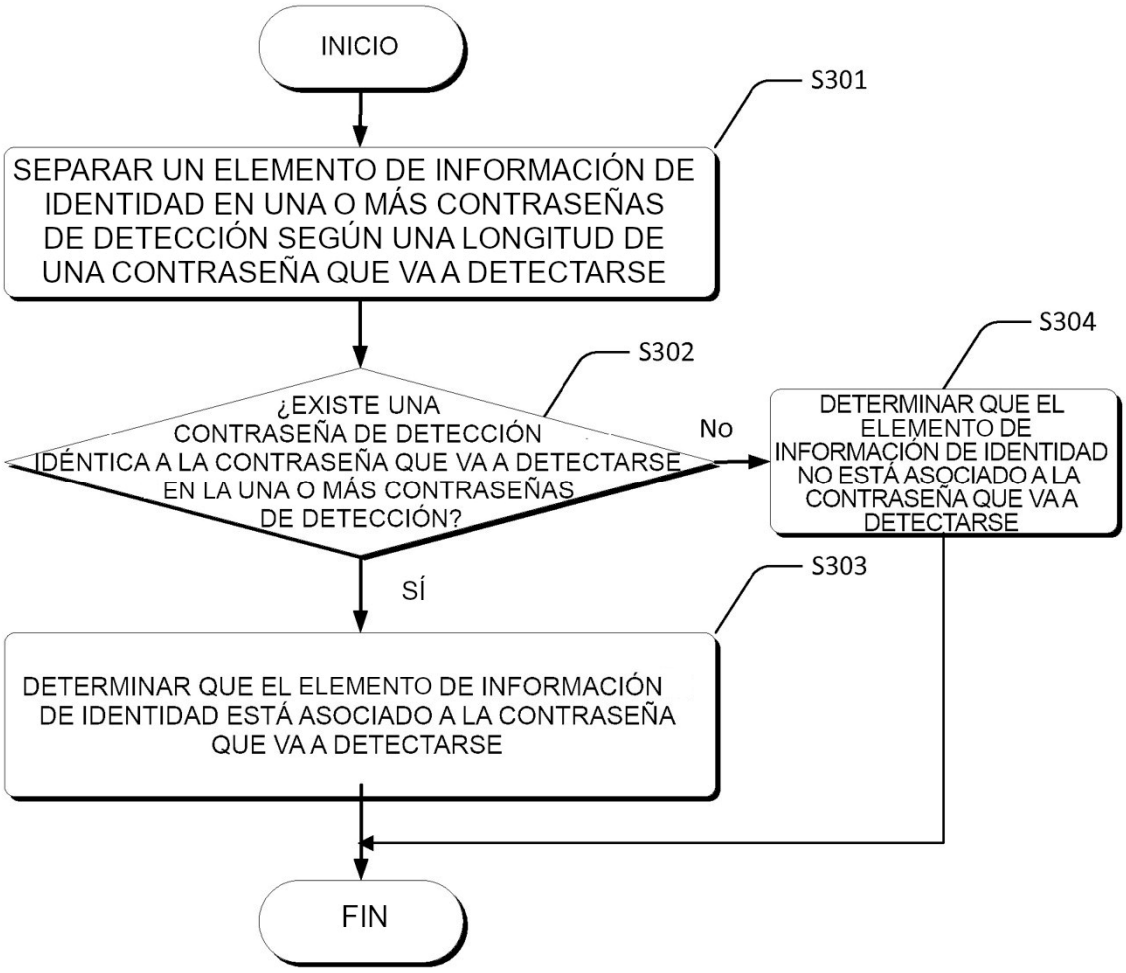
INICIO
S301
SEPARAR UN ELEMENTO DE INFORMACIÓN DE IDENTIDAD EN UNA O MÁS CONTRASEÑAS DE DETECCIÓN SEGÚN UNA LONGITUD DE UNA CONTRASEÑA QUE VA A DETECTARSE
S302
¿EXISTE UNA CONTRASEÑA DE DETECCIÓN IDÉNTICA A LA CONTRASEÑA QUE VA A DETECTARSE EN LA UNA O MÁS CONTRASEÑAS DE DETECCIÓN?
No
S304
DETERMINAR QUE EL ELEMENTO DE INFORMACIÓN DE IDENTIDAD NO ESTÁ ASOCIADO A LA CONTRASEÑA QUE VA A DETECTARSE
SÍ
S303
DETERMINAR QUE EL ELEMENTO DE INFORMACIÓN DE IDENTIDAD ESTÁ ASOCIADO A LA CONTRASEÑA QUE VA A DETECTARSE
FIN

FIG. 3

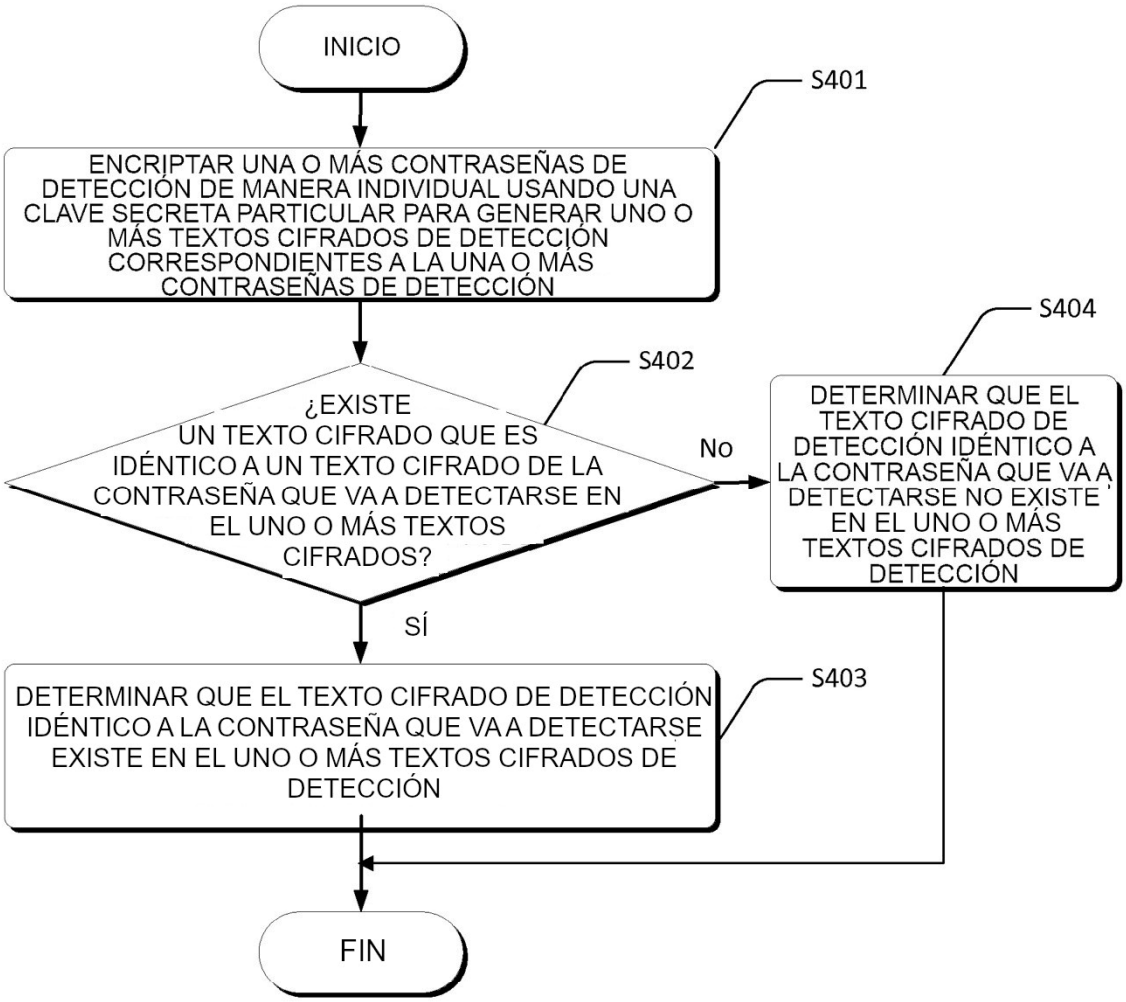
INICIO
S401
ENCRIPTAR UNA O MÁS CONTRASEÑAS DE DETECCIÓN DE MANERA INDIVIDUAL USANDO UNA CLAVE SECRETA PARTICULAR PARA GENERAR UNO O MÁS TEXTOS CIFRADOS DE DETECCIÓN CORRESPONDIENTES A LA UNA O MÁS CONTRASEÑAS DE DETECCIÓN
S402
¿EXISTE UN TEXTO CIFRADO QUE ES IDÉNTICO A UN TEXTO CIFRADO DE LA CONTRASEÑA QUE VA A DETECTARSE EN EL UNO O MÁS TEXTOS CIFRADOS?
No
S404
DETERMINAR QUE EL TEXTO CIFRADO DE DETECCIÓN IDÉNTICO A LA CONTRASEÑA QUE VA A DETECTARSE NO EXISTE EN EL UNO O MÁS TEXTOS CIFRADOS DE DETECCIÓN
SÍ
S403
DETERMINAR QUE EL TEXTO CIFRADO DE DETECCIÓN IDÉNTICO A LA CONTRASEÑA QUE VA A DETECTARSE EXISTE EN EL UNO O MÁS TEXTOS CIFRADOS DE DETECCIÓN
FIN

FIG. 4

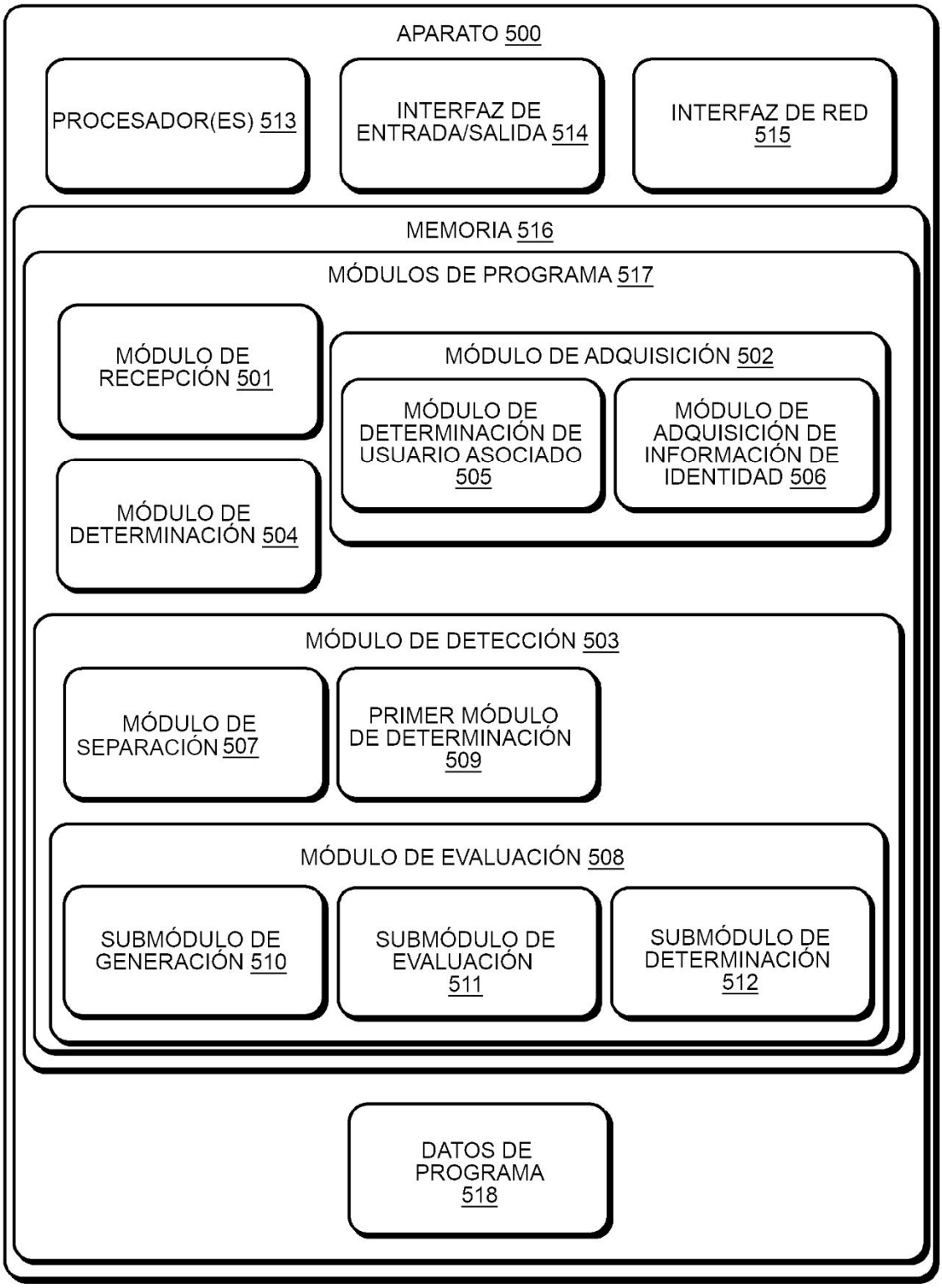
APARATO 500
PROCESADOR(ES) 513
INTERFAZ DE ENTRADA/SALIDA 514
INTERFAZ DE RED 515
MEMORIA 516
MÓDULOS DE PROGRAMA 517
MÓDULO DE RECEPCIÓN 501
MÓDULO DE ADQUISICIÓN 502
MÓDULO DE DETERMINACIÓN DE USUARIO ASOCIADO 505
MÓDULO DE ADQUISICIÓN DE INFORMACIÓN DE IDENTIDAD 506
MÓDULO DE DETERMINACIÓN 504
MÓDULO DE DETECCIÓN 503
MÓDULO DE SEPARACIÓN 507
PRIMER MÓDULO DE DETERMINACIÓN 509
MÓDULO DE EVALUACIÓN 508
SUBMÓDULO DE GENERACIÓN 510
SUBMÓDULO DE EVALUACIÓN 511
SUBMÓDULO DE DETERMINACIÓN 512
DATOS DE PROGRAMA 518

FIG. 5