(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 744 441**

(51) Int. CI.:

G06F 21/62 (2013.01)

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(86) Fecha de presentación y número de la solicitud internacional: **02.12.2016 PCT/EP2016/079686**

(87) Fecha y número de publicación internacional: **22.06.2017 WO17102390**

(96) Fecha de presentación y número de la solicitud europea: **02.12.2016 E 16805823 (8)**

(97) Fecha y número de publicación de la concesión europea: **12.06.2019 EP 3380982**

(54) Título: **Manejo de indagaciones genómicas**

(30) Prioridad:

16.12.2015 PT 2015109034

(45) Fecha de publicación y mención en BOPI de la traducción de la patente:
25.02.2020

(73) Titular/es:

CBRA GENOMICS, S.A. (100.0%)
Biocant, Parque Tecnológico de Cantanhede, Núcleo 04 Lote 3
3060-197 Cantanhede, PT

(72) Inventor/es:

ALVES DE CARVALHO, ANDRÉ DIAS;
LAMEIRAS SOUSA, HELDER;
DE CASTRO ARANTES-OLIVEIRA, NUNO MANUEL;
DE SOUSA SOARES, BRUNO FLÁVIO NOGUEIRA;
PEDROSA PINTO, ANA SOFIA y
PEREIRA LOPES, PEDRO JORGE

(74) Agente/Representante:

ISERN JARA, Jorge

DESCRIPCIÓN

Manejo de indagaciones genómicas

La presente divulgación se refiere al manejo de indagaciones genómicas, en particular aunque no exclusivamente el manejo de indagaciones genómicas presentadas por un médico junto con un paciente.

Antecedentes

La medicina personalizada basada en el análisis del genoma de un paciente se muestra muy prometedora para aumentar la eficacia de los tratamientos y permitir nuevos tratamientos que antes no eran posibles. Actualmente, un proceso típico implica la presentación de una muestra que contiene ADN de un paciente a un laboratorio genómico, donde el genoma del paciente es total o parcialmente secuenciado para responder a una pregunta específica, facilitando que un médico tome decisiones de diagnóstico o tratamiento. Dichas indagaciones implican buscar ciertas características o marcadores en el genoma, como mutaciones y secuencias repetidas de ADN en ciertos genes, números de cromosomas anormales, la presencia o ausencia de ciertos genes, duplicación de genes, entre otros.

En el estado actual de la técnica, la secuenciación del genoma debe realizarse cada vez que se solicita una prueba genética debido a cuestiones de privacidad y anonimato. Además, la formulación de un resultado de la indagación genómica requiere un conocimiento especializado importante que muchos médicos no poseen. Incluso cuando los médicos tienen un conocimiento especializado relevante, la elaboración de respuestas a una indagación genómica requiere de genetistas especializados, por lo general un recurso escaso. La necesidad de secuenciar todo el genoma o parte de él cada vez que se debe evaluar una condición/enfermedad, y el nivel de especialización requerido tanto para realizar el análisis como para interpretar los resultados significa que obtener respuestas a las indagaciones genómicas requiere un proceso que consume mucho tiempo y costoso lo que limita el acceso a un medicamento personalizado.

Resumen

Para abordar las deficiencias inherentes en el estado actual de la técnica, sería deseable proporcionar un marco para procesar automáticamente las indagaciones genómicas de una manera que requiera menos tiempo, sin dejar de abordar las inquietudes relacionadas con la privacidad y el anonimato de los datos confidenciales del genoma.

En un primer aspecto, se proporciona un método para procesar una indagación genómica para producir un reporte. Un primer código secreto, un segundo código secreto y una solicitud de indagación se reciben a través de una red de comunicaciones, por ejemplo, en un servidor, durante una primera sesión de comunicaciones. Un valor de representante asociado con la solicitud de indagación se almacena en una base de datos. La solicitud de indagación también se puede almacenar en la base de datos.

El primer código secreto se utiliza para determinar una clave del genoma, que permite el acceso a los datos del genoma, asociado con el primer código secreto, almacenado en la base de datos. El primer código secreto puede pertenecer a un paciente y, por ejemplo, puede generarse a partir de un identificador físico que pertenece al paciente, por ejemplo, cuando el paciente inserta la identificador física en un ordenador cliente conectado a través de la red de comunicaciones. Esto puede implicar la generación del primer código secreto a partir de los datos en el identificador físico, por ejemplo, utilizando una función unidireccional. Por lo tanto, cuando el primer código secreto pertenece a un paciente, el genoma se asocia con el paciente a través del primer código secreto, o más generalmente con el propietario del primer código secreto. La asociación entre la clave del genoma y los datos del genoma puede deberse a la forma en que los datos del genoma se almacenaron en la base de datos en asociación con la clave del genoma, por ejemplo, como se describe a continuación.

El uso del primer código secreto para determinar la clave del genoma puede comprender evaluar una función, por ejemplo, una función unidireccional, combinar una clave de genoma candidata en la base de datos con el primer código secreto y comparar el resultado con una clave de verificación del genoma asociada con el primer código secreto. Si hay una coincidencia, se ha encontrado la clave del genoma asociada; de lo contrario, el proceso se repite con otra clave candidata del genoma hasta que se encuentra una coincidencia (por supuesto, la evaluación puede hacerse primero de todas las claves del genoma, y luego buscar una coincidencia). La clave de verificación del genoma puede asociarse con el primer código secreto al almacenarse en un perfil de usuario al que se puede acceder con credenciales, incluido el primer código secreto. Si bien se puede acceder al perfil de usuario utilizando el primer código secreto, el primer código secreto no se almacena con el perfil de usuario, para garantizar que no se pueda acceder a los datos del genoma solo con el perfil de usuario sin recibir el primer código secreto. Como se usa en este documento, la credencial generalmente puede incluir los códigos secretos descritos y otra información como nombres de usuario y/o contraseñas para proporcionar dos o más credenciales de factor. Sin embargo, en algunas realizaciones, las credenciales pueden consistir únicamente en el código secreto, por ejemplo, el primer código secreto, y la referencia a "credenciales" debe interpretarse como que incluye el caso de las credenciales de un solo factor.

Los valores de representantes y una clave de indagación se asocian utilizando el segundo código secreto, de modo que la clave de indagación solo se puede encontrar con el valor de representante utilizando tanto el valor de representante como el segundo código secreto. El segundo código secreto puede ser la propiedad de un médico que trata con el paciente y se envía la solicitud de indagación con el paciente. Por ejemplo, el segundo código secreto puede generarse a partir de los datos en un identificador físico que pertenece al médico y puede generarse en el ordenador cliente a partir de los datos, por ejemplo, utilizando una función unidireccional. De esa manera, un médico y un paciente pueden enviarnos una solicitud de indagación juntos insertando su identificador física en el ordenador cliente para enviar la solicitud de indagación.

El valor de representante y la clave de indagación pueden asociarse calculando una clave de verificación de indagación como una función, por ejemplo, una función unidireccional, combinando el valor de representante, la clave de indagación y el segundo código secreto y almacenando la clave de verificación de indagación en la base de datos. La clave de verificación de la indagación se puede almacenar en la base de datos en asociación con el segundo código secreto y el valor de representante. Por ejemplo, la clave de verificación de la indagación y el valor del representante se pueden almacenar en un perfil de usuario accesible con credenciales, incluido el segundo código secreto. Si bien puede accederse al perfil de usuario utilizando el segundo código secreto, el segundo código secreto no se almacena en el perfil de usuario para evitar el acceso a la indagación sin recibir el segundo código secreto.

Se apreciará que las funciones respectivas utilizadas para calcular las diferentes claves de verificación (función de verificación del genoma que combina una clave del genoma y el primer código secreto; función de verificación de la indagación que combina una clave de indagación, un valor de representante y el segundo código secreto; verificación adicional de la indagación la función que combina una clave de indagación, un valor de representante y el primer código secreto) diferirá en las entradas que tomen para generar la clave de verificación correspondiente, pero de lo contrario puede ser la misma, es decir, implementar la misma operación, por ejemplo la misma función unidireccional, o una o más de las funciones respectivas pueden implementar cada una operación respectiva diferente para generar cada tipo respectivo de clave de verificación.

Una vez que se han encontrado y/o generado las claves de genoma y de indagación, se almacena una asociación entre las claves de genoma y de indagación en la base de datos y se eliminan el primer y segundo código secreto, por ejemplo, en respuesta a la asociación de las claves de genoma e indagación o al final de la primera sesión de comunicaciones. La asociación puede ser directa y/o explícita, o puede ser indirecta, por ejemplo, a través de la indagación almacenada u otra entrada de base de datos almacenada. Dado que las claves de indagación y el genoma solo se pueden encontrar usando el primer código secreto, una vez que se eliminan los códigos secretos primero y segundo, la asociación entre el genoma y las claves de indagación y el paciente y/o el médico no puede establecerse rastreando desde el genoma y las claves de indagación, salvaguardando así el anonimato de los datos asociados con estas claves. Por ejemplo, cuando se encuentran las claves del genoma/indagación utilizando un cálculo que involucra uno de los códigos secretos para que coincida con las claves de verificación, sin el código secreto presente, la base de datos contiene conjuntos no relacionados de claves del genoma/indagación (acceso a la base de datos) por un lado y claves de verificación por otro lado. Un par de claves de verificación y acceso a la base de datos solo se pueden hacer coincidir en presencia del código secreto, manteniendo un usuario vinculado en la base de datos a la clave de verificación anónimo a la luz de la clave de acceso a la base de datos y, por lo tanto, manteniendo los datos asociados con la clave de acceso a la base de datos. anónimo. El anonimato puede mejorarse aún más mediante el uso de funciones unidireccionales como se describe anteriormente.

Para procesar la indagación genómica, los datos del genoma se identifican mediante la clave del genoma y la indagación asociada con la solicitud de indagación (asociada con una clave de indagación) se aplica a los datos del genoma identificado para generar un reporte. El reporte se almacena en la base de datos en asociación con la clave de indagación. De esta manera, se puede acceder al reporte en la base de datos utilizando la clave de indagación. Luego de almacenar el reporte de esta manera, se elimina la asociación entre el genoma y las claves de indagación. De esta manera, el anonimato se mejora aún más, ya que el genoma no se puede rastrear desde el reporte sin recibir nuevamente el primer y segundo código secreto.

De este modo, ventajosamente, mediante el uso de claves de acceso a la base de datos que requieren códigos secretos, que no se guardan en el servidor, se salvaguarda el anonimato del paciente (u otro propietario del primer código secreto y los datos del genoma), evitando una asociación de los datos del genoma y/o reportes con el paciente sin recibir el primer código secreto. Mediante el manejo específico de la creación y eliminación de las diversas asociaciones en la base de datos, se habilita un proceso que permite que los datos del genoma se obtengan una vez, se almacenen de una manera que resuelva los problemas de privacidad y anonimato, y se utiliza varias veces para responder a varias indagaciones genómicas. Por lo tanto, se elimina un importante cuello de botella en la aplicación de la medicina personalizada, como se explicó anteriormente. Además, el uso de dos códigos secretos de la manera descrita anteriormente garantiza que el propietario del segundo código secreto, por ejemplo un médico, no pueda ejecutar una indagación genómica sin el consentimiento del propietario del primer código secreto, pero puede recuperar el reporte resultante en ausencia del propietario del primer código secreto, por ejemplo, para prepararse para una consulta con el propietario del primer código secreto. Por lo tanto, la forma descrita de manejar las indagaciones genómicas permite, por ejemplo, que un médico obtenga reportes sobre indagaciones genómicas de

una manera eficiente que respete la privacidad y el anonimato del paciente y facilite el acceso a la medicina personalizada para el paciente.

En virtud de asociar la clave de indagación con el valor de representante (a través del segundo código secreto), el valor de representante identifica de forma única cada indagación. Los valores de representantes pueden generarse de cualquier manera adecuada proporcionando valores de representantes únicos, por ejemplo, incrementando un contador o atribuyendo aleatoriamente identificadores únicos, por ejemplo, utilizando identificadores universalmente únicos (véase https://en.wikipedia.org/wiki/Universally_unique_identifier). Los valores de representantes pueden generarse previamente y almacenarse listos para su uso cuando sea necesario, o pueden generarse en respuesta a la recepción de una indagación de genoma.

En una segunda sesión de comunicaciones posterior, en realizaciones relacionadas con la recuperación del reporte generado, el segundo código secreto se recibe de nuevo a través de la red de comunicaciones y se usa con el valor de representante para encontrar la clave de indagación. Posteriormente a la búsqueda de la clave de indagación, se elimina el segundo código secreto, durante o al final de la segunda sesión de comunicación. Mediante la clave de indagación, el reporte se identifica y se envía a través de la red de comunicaciones durante la segunda sesión de comunicaciones.

Encontrar la clave de indagación puede implicar evaluar la función utilizada para calcular la clave de verificación de la indagación para el valor de representante y una clave de indagación candidata en la base de datos y comparar el resultado con la clave de verificación de la indagación para encontrar una coincidencia entre el resultado e indagación de la clave de verificación, como se describe anteriormente para la clave de verificación del genoma.

En realizaciones en las que las claves de verificación se almacenan en asociación con un código secreto, por ejemplo, en un perfil de usuario accesible con credenciales que incluyen el código secreto, la comparación entre los valores de función y las claves de verificación se puede hacer directamente para la clave de verificación relevante asociada con el código secreto relevante. Alternativamente, se podría ejecutar una indagación para todas las combinaciones de acceso a la base de datos y claves de verificación (o todas las claves de verificación y de base de datos que pertenecen al mismo tipo de objeto, por ejemplo, indagación o genoma), con una coincidencia que indique que tanto la clave de verificación como la base de datos la clave de acceso está asociada con el código secreto en cuestión. Sin embargo, otras realizaciones no se basan en las claves de verificación, sino que generan claves de acceso a la base de datos a partir de los códigos secretos respectivos utilizando una función unidireccional correspondiente, por ejemplo, generando una clave genómica desde un primer código secreto utilizando una primera función unidireccional y generando una clave de indagación desde una combinación de un segundo código secreto y un valor de representante utilizando una segunda función unidireccional (por supuesto, la primera y la segunda funciones unidireccionales podrían ser la misma forma de guardar, por ejemplo, combinar la entrada con una cadena que significa el genoma para la primera) función y una cadena que significa indagación para la segunda función unidireccional).

En algunas realizaciones, una pluralidad de valores de representantes se almacena juntos en la base de datos de modo que sean accesibles usando credenciales que incluyen el segundo código secreto. Por ejemplo, los valores de representantes se pueden almacenar en un perfil de usuario accesible con las credenciales. De esta manera, se puede acceder a todos los valores de representantes asociados con las indagaciones generadas por el propietario del segundo código secreto y, por lo tanto, a todas las indagaciones asociadas. Los valores de representantes pueden ser generados -previamente y asociados con el perfil de antemano. Alternativamente, la asociación entre el perfil y los valores de representantes puede generarse en respuesta a la recepción de la solicitud de indagación, independientemente de si el valor de representante en sí mismo se ha generado previamente o se ha generado en respuesta a la solicitud de indagación.

Durante la segunda sesión de comunicaciones, luego, la información resumida de las indagaciones/reportes asociados con los valores de representantes almacenados se envía al dispositivo cliente para permitir que un usuario seleccione un reporte para recuperar. Por ejemplo, la información de resumen para cada reporte puede asociarse con un identificador correspondiente que se envía desde el ordenador cliente a través de la red de comunicaciones en respuesta a la selección de un reporte/información de resumen, mientras que una asociación entre este identificador y el valor de representante (o clave de indagación) correspondiente al reporte se almacena en el servidor para permitir la recuperación del reporte, por ejemplo, como se describe anteriormente. En el servidor, un valor de representante correspondiente al identificador se recupera y se usa para encontrar la clave de indagación correspondiente como se describe anteriormente, que luego se usa para recuperar el reporte correspondiente. El reporte recuperado se envía al cliente donde el propietario del segundo código secreto puede revisarlo.

En algunas realizaciones, cuando el primer código secreto se usa para acceder al genoma correspondiente, la información de contacto asociada con el propietario del primer código secreto se recupera y se usa para enviar un mensaje que indica que el primer código secreto se ha utilizado para acceder al genoma. De esa manera, el propietario del primer código secreto, por ejemplo, un paciente, recibirá una notificación cada vez que el servidor reciba el primer código secreto, brindándole mayor protección contra el uso no autorizado del primer código secreto. En algunas realizaciones, la información de contacto se almacena en asociación con la clave de verificación del genoma (cuando

corresponda), por ejemplo, en un perfil de usuario accesible con credenciales que incluyen el primer código secreto, en donde también se almacena la clave de verificación del genoma.

Se apreciará que las funciones respectivas utilizadas para calcular las diferentes claves de verificación (función de verificación del genoma que combina una clave del genoma y el primer código secreto; función de verificación de la indagación que combina una clave de indagación, un valor de representante y el segundo código secreto; verificación adicional de la indagación la función que combina una clave de indagación, un valor de representante y el primer código secreto) diferirá en las entradas que tomen para generar la clave de verificación correspondiente, pero de lo contrario puede ser la misma, es decir, implementar la misma operación, por ejemplo, la misma función unidireccional, o una o más de las funciones respectivas pueden implementar cada una una operación respectiva diferente para generar cada tipo respectivo de clave de verificación.

En un segundo aspecto, se proporciona un método para poblar una base de datos genómica que opcionalmente puede ser adicional o una alternativa al primer aspecto. Un primer código secreto se recibe a través de una red de comunicaciones durante una sesión de comunicaciones y se utiliza con una clave del genoma para generar una clave de verificación del genoma, lo que permite el acceso a los datos del genoma una vez que se almacena en la base de datos. La clave de verificación del genoma se genera de tal manera que la clave del genoma se puede encontrar con la clave de verificación del genoma utilizando solo el primer código secreto y la clave de verificación del genoma. El primer código secreto se elimina después de generar la clave de verificación del genoma, por ejemplo, al final de la sesión de comunicación o inmediatamente una vez que se ha generado la clave. La clave de verificación del genoma se puede almacenar en un perfil de usuario accesible mediante credenciales que pueden incluir el primer código secreto. De esta manera, el propietario del primer código secreto no se puede rastrear desde la clave del genoma, como se explicó anteriormente. La clave del genoma se puede enviar al propietario del primer código secreto para enviarla a un proveedor del genoma designado por el propietario del primer código secreto (o puede enviarse directamente al proveedor del genoma) para permitir que el genoma secuenciado, una vez recibido del genoma proveedor, que se hará accesible a través de la clave del genoma al tiempo que protege el anonimato del propietario del primer código secreto. Esto puede implicar cargar el genoma en la base de datos y almacenarlo en asociación con la clave del genoma. Alternativamente, el proveedor del genoma puede almacenar el genoma en su extremo de modo que sea accesible con la clave del genoma, siempre que no asocien los detalles del propietario del primer código secreto con la clave del genoma. Se puede acceder al genoma en el proveedor del genoma utilizando la clave del genoma cuando sea necesario.

En algunas realizaciones, la clave del genoma puede generarse a partir del primer código secreto utilizando una función unidireccional que está almacenada (o identificada) por el perfil del usuario (permitiendo la recuperación pasando el código secreto a través de la función unidireccional como se explicó anteriormente) en lugar de generando y almacenando una clave de verificación.

El genoma se recibe junto con la clave del genoma y se almacena en la base de datos en asociación con la clave del genoma. A partir de este punto, el genoma puede identificarse para su recuperación utilizando el primer código secreto para encontrar la clave del genoma, como se describió anteriormente. En los aspectos primero y segundo y sus realizaciones, los datos clínicos asociados con el propietario del genoma pueden almacenarse en la base de datos en asociación con la clave del genoma. Esto permite la recuperación de los datos clínicos de una manera similar a la descrita anteriormente. Además, al establecer una asociación entre los datos del genoma y los datos clínicos correspondientes a través de la clave del genoma, se pueden analizar las correlaciones entre los datos clínicos y los datos del genoma, respetando la privacidad y el anonimato del propietario del genoma. Por supuesto, se entenderá que los datos genómicos y clínicos pueden asociarse de otra manera que no sea la clave genómica, por ejemplo, mediante una clave separada común a los datos genómicos y clínicos, o de cualquier otra forma.

Del mismo modo, como se mencionó anteriormente, el primer código secreto puede estar asociado con el paciente y el segundo código secreto puede estar asociado con un médico. El primer y el segundo código secreto pueden haber sido derivados de un identificador físico respectivo en el ordenador cliente, por ejemplo, usando una función unidireccional aplicada a los datos en la identificador en el ordenador cliente. El primer y el segundo código secreto se transmiten a través de la red de comunicaciones y se utilizan como se describe anteriormente. Típicamente, en particular en realizaciones en las que el primer y segundo código secreto pertenecen, respectivamente, a un paciente y un médico, el primer y segundo código secreto no son los mismos. Sin embargo, en algunas realizaciones, el primer y el segundo código secreto pueden ser el mismo código secreto, de modo que el propietario del código secreto puede cargar su genoma en la base de datos y enviar y recuperar indagaciones genómicas, utilizando el código secreto descrito anteriormente. Por ejemplo, un paciente puede administrar todo el proceso descrito anteriormente sin la asistencia de un médico. Incluso cuando el primer y el segundo código secreto no son los mismos, el propietario del primero y el segundo código secreto puede ser la misma persona, por ejemplo, el paciente. En este caso, el propietario, por ejemplo, el paciente, manejaría todo el proceso, aunque utilizando dos códigos secretos y, por ejemplo, dos identificadores físicos correspondientes.

En algunas realizaciones, el acceso a los reportes generados asociados con las claves de indagación respectivas utilizando el primer código secreto está habilitado. Específicamente, las claves de verificación de indagación adicionales respectivas se pueden calcular utilizando las claves de indagación y los valores de representantes

asociados, esta vez junto con el primer código secreto en lugar del segundo código secreto. Estos valores de verificación de la indagación se almacenan en un perfil de usuario asociado con el propietario del primer código secreto (o se puede acceder a ellos utilizando credenciales que comprenden el primer código secreto), junto con la información de resumen de la indagación asociada y otra información como el estado de la indagación. Esto proporciona al propietario del primer código secreto la opción de llevar a cabo algunas o todas las acciones que el propietario del segundo código secreto puede llevar a cabo. Por ejemplo, el propietario del primer código secreto, como un paciente, puede, de esta manera, tener acceso independiente a los reportes generados, para que puedan estar disponibles para un tercero, por ejemplo, un médico que no sea el propietario del segundo código secreto si el dueño del primer código secreto desea obtener una segunda opinión.

En realizaciones en las que las claves se generan a partir de los códigos secretos utilizando una función unidireccional para su posterior recuperación, se pueden generar otras claves a partir del primer código secreto, correspondientes a las claves generadas desde el segundo código secreto y que proporcionan acceso a indagaciones o agrupaciones de claves de indagación.

En cualquiera de los aspectos y realizaciones anteriores, la aplicación de una función unidireccional a una entrada puede comprender concatenar la entrada con una cadena aleatoria y operar el resultado con una función unidireccional. Independientemente de si la entrada se combina con una cadena o no, la función unidireccional puede ser una función *hash* criptográfica, por ejemplo, SHA-256. La cadena puede ser numérica, alfanumérica o solo caracteres y puede ser específica y única para la función unidireccional en cuestión, es decir, una primera cadena para la primera función unidireccional, una segunda cadena para la segunda función unidireccional y pronto. Más en general, se entenderá que una función unidireccional tal como se usa aquí es una función para la cual es difícil o en la práctica imposible encontrar la entrada dada la salida y se apreciará que muchas de estas funciones son bien conocidas en la técnica.

Además, en cualquiera de los aspectos y realizaciones anteriores, la indagación genómica puede comprender instrucciones para buscar ciertos números de cromosomas, rangos de coordenadas cromosómicas, nombres de genes, números de acceso, palabras clave o términos que describen datos de genomas de bases de datos especializadas, como, por ejemplo, Genbank , Uniprot, EBI o NCBI, números de identificación de variantes, referencias bibliográficas, predicción de patogenicidad de variantes, predicción de efectos funcionales de proteínas. Además, cualquiera o más de los anteriores pueden estar asociados con una enfermedad, afección o fármaco como, entre otros, cardiomiopatía, diabetes, trombofilia, terapia del cáncer colorrectal, enfermedad de Alzheimer, glaucoma, artritis reumatoide, fibrosis quística, hemocromatosis, sordera pediátrica, en áreas tales como, entre otras, cardiología, endocrinología, hematología, gastroenterología, neurología, oftalmología, reumatología, neumología, medicina interna o pediatría.

Para evitar dudas, cuando se hace referencia a asociaciones entre diferentes elementos en la base de datos, por ejemplo claves como el genoma y la clave de indagación, estas asociaciones pueden ser explícitas y directas, almacenando por ejemplo ambas claves como un registro de la base de datos, o puede ser indirecto, por ejemplo, mediante asociaciones con uno o más elementos comunes, desde los cuales los elementos en cuestión pueden asociarse entre sí, al que se le asigna un elemento, se puede encontrar el otro elemento.

Breve descripción de los dibujos

Se describen ahora realizaciones específicas a modo de ejemplo, con referencia a los dibujos adjuntos, en los cuales:

La Figura 1 ilustra un sistema cliente/servidor para implementar los procesos descritos a continuación;

La Figura 2 ilustra una base de datos que tiene una parte privada y una parte anónima;

La Figura 3a ilustra la información almacenada en un perfil de paciente en la parte privada de la base de datos;

La Figura 3b ilustra información almacenada en un perfil de médico en la parte privada de la base de datos;

La Figura 4a ilustra un proceso para asociar indirectamente un perfil de paciente con una clave de genoma por medio de un primer código secreto que es propiedad de un paciente;

La Figura 4b ilustra un proceso para encontrar una clave de genoma usando una clave de verificación de genoma y un primer código secreto que es propiedad de un paciente;

La Figura 5a ilustra un proceso para asociar indirectamente un perfil de médico y una clave de indagación a través de un segundo código secreto propiedad de un médico;

La Figura 5b ilustra un proceso para encontrar una clave de indagación utilizando una clave de verificación de indagación y un segundo código secreto propiedad de un médico;

La Figura 6 ilustra un proceso para procesar una indagación genómica;

La Figura 7 ilustra un proceso para proporcionar resúmenes de reportes para permitir la selección de un reporte a recuperar y para proporcionar el reporte seleccionado;

La Figura 8 ilustra un proceso para poblar una base de datos de genoma;

Las Figuras 9a-9d ilustran un proceso para procesar una indagación genómica en realizaciones que usan funciones unidireccionales para la generación e identificación de claves combinadas; y

Las Figuras 10a-10h ilustran un proceso para proporcionar resúmenes de reportes e reportes seleccionados en realizaciones que utilizan funciones unidireccionales para la generación e identificación de claves combinadas.

Descripción específica

Con referencia a la Figura 1, un ordenador 130 cliente, típicamente ubicado en la consulta de un médico, comprende un lector 140 para leer los identificadores 110, 120 físicos además del hardware de ordenador convencional, tal como una infraestructura de procesamiento apropiada, dispositivos de entrada y un monitor. Los identificadores físicos pertenecen, respectivamente, a un paciente y un médico, y cada uno lleva una firma digital, por ejemplo, una cadena aleatoria, única para el propietario. Los respectivos primeros y segundos códigos 410, 420 secretos pueden generarse a partir de las firmas digitales, como se describe a continuación. El ordenador 130 cliente está en comunicación con un servidor 160 configurado para procesar indagaciones genómicas, como se describe a continuación, a través de una red 180 de comunicaciones, por ejemplo, Internet. Las comunicaciones a través de la red 180 de comunicaciones pueden ser a través de canales seguros y encriptados, por ejemplo, utilizando SSL u otros protocolos. El servidor 160 implementa o tiene acceso a una base de datos de genoma que contiene datos del genoma para su procesamiento, como se describirá a continuación. El ordenador 130 cliente y/o el servidor 160 están en comunicación con un servidor 170 de proveedor de genoma para proporcionar datos de genoma al servidor 160.

Con referencia a la Figura 2, una base de datos almacenada en el servidor 160 contiene datos para permitir el procesamiento de indagaciones sobre los genomas de los pacientes, presentados por los pacientes junto con su médico, y comprende una parte 200 privada y una parte 205 anónima. La parte 200 privada comprende un perfil 210 de paciente para cada paciente que comprende un nombre 215 de usuario de paciente, credenciales 220 de paciente y datos de perfil que se describen a continuación. La parte 200 privada comprende adicionalmente un perfil 225 del médico para cada médico que comprende un nombre 230 de usuario de médico, credenciales 235 de médico y datos de perfil descritos a continuación. La parte 205 anónima comprende una clave 240 de genoma almacenada en asociación con los datos 245 de genoma y los datos de perfil que se describen a continuación. La parte 205 anónima comprende adicionalmente una clave 250 de indagación almacenada en asociación con una solicitud 255 de indagación, una indagación 260 y un reporte 265 para cada indagación almacenada. Un enlace 270 temporal entre la clave 240 de genoma y la clave 250 de indagación se almacena en la parte 205 anónima de la base de datos para permitir que una indagación 260 sea procesada por el servidor 160 como se describe a continuación. No se almacenan enlaces entre las partes 200, 205 privadas y anónimas de la base de datos, pero los perfiles 210, 225 en la parte 200 privada de la base de datos contienen información que les permite asociarse con claves (y, por lo tanto, con los datos correspondientes) en la parte 205 anónima en presencia de un código secreto respectivo recibido del paciente o médico, según sea el caso, como se describe en detalle a continuación. La parte 205 anónima no contiene información que pueda vincularse a los perfiles en la parte 200 privada, para garantizar el anonimato.

Con referencia a la Figura 3a, el perfil 210 del paciente para cada paciente comprende información 300 personal del paciente, detalles 305 de contacto del paciente, una clave 310 de verificación del genoma, las credenciales 220 del paciente que comprenden una contraseña 315, una clave 320 del paciente y una clave 325 de verificación del paciente, y para cada indagación un valor 330 representante, una clave 335 de verificación de indagación del paciente, una información 340 de resumen de indagación y un estado 345 de reporte, todo lo cual se describirá con detalle a continuación. La información relacionada con la indagación solo necesita almacenarse en realizaciones en las que el acceso a los reportes esté habilitado para pacientes y médicos.

Con referencia a la Figura 3b, el perfil 225 del médico para cada médico comprende información 350 personal del médico, detalles 355 de contacto del médico, credenciales 235 del médico que comprenden una contraseña 360, una clave 365 del médico y una clave 370 de verificación del médico, y para cada indagación un valor 330 representante, una clave 375 de verificación de indagación del médico, un paciente 377 para indagación, una información 380 de resumen de indagación y un estado 385 de reporte que se describirán con detalle a continuación. Se observará que la clave del médico y de verificación del médico (así como la clave del paciente y de verificación del paciente mencionadas anteriormente con referencia a la Figura 3a) se almacenan en el perfil para permitir que el primer (segundo) código secreto sea verificado como parte de las credenciales utilizadas durante el proceso de inicio de sesión. Será evidente que se pueden emplear muchas otras técnicas que también evitan el almacenamiento de los códigos secretos en los perfiles y que, en algunas realizaciones, los códigos secretos se pueden omitir de las credenciales utilizadas para iniciar sesión en el perfil y solo se pueden usar para hacer la asociación entre las claves de verificación en los perfiles y las claves de base de datos correspondientes en la parte anónima de la base de datos.

Como se mencionó anteriormente, no se almacenan enlaces en la base de datos entre las partes privadas y anónimas, pero se pueden hacer asociaciones entre ellas utilizando códigos secretos pertenecientes al paciente o al médico. Con referencia a la Figura 4a, ahora se describe un proceso para asociar el perfil 210 del paciente y la clave 240 del genoma. En la etapa 401, el servidor 160 genera la clave 240 del genoma. En algunas realizaciones, el servidor 160 genera la clave 240 del genoma aplicando una función unidireccional a un primer código 410 secreto que es propiedad del paciente y que se describe más adelante en combinación con un valor aleatorio para generar una clave segura, y posteriormente aplica una función unidireccional a una combinación del primer código secreto y posteriormente aplica una función unidireccional a una combinación del primer código 410 secreto y la clave segura para generar la clave 240 de genoma. Específicamente, en algunas realizaciones, el valor aleatorio es una cadena alfanumérica de 64 caracteres. Sin embargo, en algunas realizaciones, la clave del genoma se puede calcular previamente y se puede omitir la etapa 401.

En la etapa 402, el servidor 160 usa el primer código 410 secreto y la clave 240 de genoma para generar la clave 310 de verificación del genoma. En algunas realizaciones, el servidor 160 genera la clave 310 de verificación del genoma aplicando una función unidireccional a la clave 240 de genoma y el primer código 410 secreto concatenados entre sí. En la etapa 403, el servidor 160 almacena la clave 310 de verificación del genoma en el perfil 210 del paciente de la parte 200 privada de la base de datos, y almacena la clave 240 de genoma en la porción 205 anónima de la base de datos (a menos que la clave del genoma esté precalculada y ya esté almacenada).

Con referencia a la Figura 4b, se describe ahora un proceso para encontrar la clave 240 del genoma usando la clave 310 de verificación del genoma y el primer código 410 secreto. En la etapa 404, el servidor 160 selecciona una primera clave 240 de genoma almacenada en la parte 205 anónima de la base de datos, y luego, en la etapa 405 utilizando el primer código 410 secreto y la clave de genoma seleccionada 240, el servidor 160 genera una clave 310 de verificación de genoma. En la etapa 406, el servidor 160 compara la clave de verificación del genoma generada de la etapa 405 con la clave 310 de verificación del genoma almacenada en el perfil 210 del paciente. Luego, en la etapa 407, el servidor 160 verifica si las dos claves de verificación coinciden. Si la clave de verificación del genoma generada en la etapa 405 no coincide con la clave 310 de verificación del genoma almacenada en el perfil 210 del paciente, el servidor 160 selecciona la siguiente clave 240 de genoma en la base de datos en la etapa 408 y vuelve al paso 405 para repetir el proceso para la siguiente clave 240 de genoma. Si la clave de verificación del genoma generada en la etapa 405 coincide con la clave 310 de verificación del genoma almacenada en el perfil 210 del paciente, el servidor 160 devuelve la clave 240 de genoma como la clave del genoma asociada en la etapa 409. De esta manera, los datos 245 del genoma almacenados en asociación con la clave 240 de genoma pueden identificarse utilizando la clave 310 de verificación del genoma correspondiente y el primer código 410 secreto.

Con referencia a la Figura 5a, ahora se describe un proceso para asociar el perfil 225 del médico y la clave 250 de indagación. En la etapa 501, el servidor 160 genera la clave 250 de indagación y el valor 330 representante. En algunas realizaciones, el servidor 160 genera la clave 250 de indagación aplicando una función unidireccional al segundo código 420 secreto en combinación con un valor aleatorio para generar una clave segura, y posteriormente aplica una función unidireccional a una combinación del segundo código 420 secreto y la clave segura para generar la clave 250 de indagación. Específicamente, en algunas realizaciones, el valor aleatorio es una cadena alfanumérica de 64 caracteres. Sin embargo, en algunas realizaciones, la clave del genoma se puede calcular previamente y la etapa 501 se puede omitir.

En la etapa 502, el servidor 160 genera la clave 375 de verificación de indagación del médico usando una combinación del segundo código 420 secreto, la clave 250 de indagación y el valor 330 representante. En algunas realizaciones, el servidor 160 genera la clave 375 de verificación de indagación del médico aplicando una función unidireccional a la clave 250 de indagación y al segundo código 420 secreto. En la etapa 503, el servidor 160 almacena la clave 375 de verificación de indagación del médico y el valor 330 representante en el perfil 225 del médico en la parte 200 privada de la base de datos, y almacena la clave 250 de indagación en la parte 205 anónima de la base de datos.

Con referencia a la Figura 5b, ahora se describe un proceso para encontrar una clave 250 de indagación utilizando la clave 375 de verificación de indagación del médico y el segundo código 420 secreto. En la etapa 504, el servidor 160 selecciona una primera clave 250 de indagación almacenada en la parte 205 anónima de la base de datos. Luego, en la etapa 505 utilizando una combinación del segundo código 420 secreto, la clave 250 de indagación y un valor 330 representante seleccionado, el servidor 160 genera una clave de verificación de indagación. En la etapa 506, el servidor 160 compara la clave de verificación de indagación de médico generada de la etapa 505 con la clave 375 de verificación de indagación del médico almacenada en el perfil 225 de médico. Luego, en la etapa 507, el servidor comprueba si las dos claves de verificación coinciden. Si la clave de verificación de indagación del médico generada en la etapa 505 no coincide con la clave 375 de verificación de indagación del médico almacenada en el perfil 225 de médico, el servidor 160 selecciona la siguiente clave 250 de indagación en la etapa 508 y luego vuelve al paso 505 para repetir el proceso para la siguiente clave 250 de indagación. Si la clave 375 de verificación de indagación del médico generada en la etapa 505 coincide con la clave 375 de verificación de indagación del médico almacenada en el perfil 225 del médico, el servidor 160 devuelve la clave 250 de indagación en la etapa 509.

La descripción anterior hace referencia a la combinación de ciertos elementos (por ejemplo, un código secreto y una clave) o una combinación de elementos. En algunas realizaciones, los elementos son cadenas y su combinación comprende la concatenación de las cadenas. En algunas realizaciones, la combinación de elementos comprende además la aplicación de una función unidireccional a las cadenas concatenadas. Por ejemplo, la función unidireccional es un *hash* criptográfico en algunas realizaciones, por ejemplo SHA1, 2 o 3. En algunas realizaciones, la concatenación de cadenas puede reemplazarse con otras combinaciones de los elementos antes de aplicar una función unidireccional a la combinación.

En algunas realizaciones donde el acceso a las indagaciones 260 y/o las solicitudes 255 asociadas con las claves 250 de indagación respectivas se deben proporcionar a los pacientes independientemente de su médico, los datos relacionados con la indagación se agregan al perfil 210 del paciente, como se describió anteriormente con referencia a la Figura 3a. por ejemplo, utilizando los procesos descritos anteriormente con referencia a las Figuras 5a y 5b para producir una clave 335 de verificación de indagación del paciente para el mismo valor 330 representante y clave de indagación (es decir, omitiendo la etapa 501) usando el primer código 410 secreto en lugar del segundo código 420 secreto y almacenando la clave 335 de verificación de la indagación del paciente y el valor 330 representante en el perfil 210 del paciente. La clave 335 de verificación de la indagación del paciente, junto con el valor 330 representante y el primer código 410 secreto se pueden usar para encontrar la clave 250 de indagación como se describe anteriormente para el clave 375 de verificación de indagación del médico y segundo código 420 secreto con referencia a la Figura 5b.

Con referencia a la Figura 6, ahora se describe un proceso durante una primera sesión de comunicaciones entre el ordenador 130 cliente y el servidor 160 para producir el reporte 265. El estado de la base de datos del genoma durante este proceso se describe a continuación con referencia a las Figuras 9a-d. Durante la primera sesión de comunicaciones entre el ordenador 130 cliente y el servidor 160, tanto el paciente como el médico insertan su identificador 110, 120 en el lector 140, ya sea simultáneamente o en secuencia para enviar una solicitud de indagación para el procesamiento de una indagación 260 genómica.

El paciente y el médico inician sesión en el ordenador 130 cliente con su nombre de usuario y contraseña respectivos como credenciales e insertan sus identificadores en el lector 140 en el ordenador 130 cliente. En la etapa 601, el ordenador 130 cliente lee una firma digital del paciente desde el identificador 110 de paciente y aplica una función unidireccional a la firma digital del paciente para generar el primer código 410 secreto. En la etapa 602, el ordenador 130 cliente lee de forma concurrente o secuencial una firma digital del médico desde el identificador 120 de médico y aplica una función unidireccional a la firma digital del médico para generar el segundo código 420 secreto. Se entenderá que en la etapa 601 y la etapa 602, el ordenador 130 cliente puede recibir el identificador 110 de paciente y el identificador 120 de médico en cualquier orden, y que el ordenador 130 cliente puede leer la firma digital del paciente y la firma digital del médico en cualquier orden. En la etapa 603, el ordenador 130 cliente genera la indagación 260 asociada con la solicitud 255 de indagación. En la etapa 604, el ordenador 130 cliente envía las credenciales de paciente y médico, incluyendo el primer código 410 secreto, el segundo código 420 secreto, y la solicitud 255 de indagación que comprende la indagación 260, a través de la red 180 de comunicaciones al servidor 160.

En la etapa 605, el servidor 160 recibe la solicitud 255 de indagación y la indagación 260, así como las credenciales 220 del paciente y las credenciales 235 del médico y verifica cada conjunto de credenciales con el perfil 210, 225 respectivo. En la etapa 606, el servidor 160 genera la clave 250 de indagación y la clave 375 de verificación de indagación del médico como se describió anteriormente (con referencia a la Figura 5a).

En la etapa 607, el servidor 160 almacena la solicitud 255 de indagación y la indagación 260 en asociación con la clave 250 de indagación en la parte 205 anónima de la base de datos y, en la etapa 608, el servidor 160 almacena la información 380 de resumen de la indagación, la indagación del nombre 377 del paciente y la clave 375 de verificación de indagación del médico en asociación con el valor 330 representante en el perfil 225 del médico en la parte 200 privada de la base de datos. Se entenderá que una clave 335 de verificación de indagación del paciente puede generarse de la misma manera que la clave 375 de verificación de indagación del médico y almacenarse en asociación con el valor 330 representante en el perfil 210 del paciente en la parte 200 privada de la base de datos para permitir el acceso a la indagación/reporte por parte del paciente, como se describe anteriormente.

En la etapa 609, el servidor identifica la clave 240 de genoma asociada con el primer código 410 secreto usando el primer código 410 secreto y la clave 310 de verificación de genoma como se describió anteriormente (con referencia a la Figura 4b). Luego, en la etapa 610, el servidor 160 crea un enlace 270 temporal en la parte 205 anónima de la base de datos que asocia la clave 240 del genoma y la clave 250 de indagación para permitir el procesamiento de la indagación en el genoma. Posteriormente, el primer y segundo código 410, 420 secretos ya no son necesarios y, en la etapa 611, el servidor 160 borra el primer código 410 secreto, el segundo código 420 secreto, las credenciales 220 del paciente y las credenciales 235 del médico para que los datos en privado y las partes 200, 205 anónimas ya no se pueden asociar, lo que garantiza el anonimato. La eliminación puede ocurrir inmediatamente cuando los códigos secretos ya no son necesarios, o al final de la primera sesión de comunicaciones.

En un momento posterior (por ejemplo, una vez que la indagación llega a la parte superior de una cola de procesamiento), en la etapa 612, el servidor 160 ejecuta la indagación y para ello encuentra los datos 245 del genoma

utilizando el enlace 270 temporal entre la clave 250 de indagación y la clave 240 de genoma para identificar la clave 240 de genoma y, por tanto, los datos 245 de genoma almacenados en asociación con ella. Luego, en la etapa 613, el servidor 160 aplica la indagación 260 asociada con la solicitud 255 de indagación a los datos 245 del genoma encontrados para generar un reporte 265 y en la etapa 614, almacena el reporte 265 en asociación con la clave 250 de indagación.

En la etapa 615, el servidor 160 elimina el enlace 270 temporal entre la clave 240 de genoma y la clave 250 de indagación, de modo que el reporte 265 puede recuperarse sin riesgo para el anonimato del paciente a partir de una identificación del genoma. En esta etapa, todos los datos que pueden haber representado un riesgo de privacidad se han eliminado del servidor 160 y el reporte 265 está listo para su recopilación.

Después de una o más de las primeras sesiones de comunicaciones como se describió anteriormente, la base de datos del servidor 160 comprende una o más claves 250 de indagación e reportes 265 en la parte 205 anónima de la base de datos y una o más claves 250 de indagación, valores 330 representantes y claves 375 de verificación de indagación en el perfil 225 del médico. Por lo tanto, el uno o más reportes 265 están listos para la recolección como se describirá ahora.

Con referencia a la Figura 7, ahora se describe un proceso que permite a un médico recuperar un resumen de sus reportes 265 utilizando su identificador 120. En la etapa 701, durante una segunda sesión de comunicaciones entre el ordenador 130 cliente y el servidor 160, el médico proporciona sus credenciales 235, incluyendo su identificador 120 al ordenador 130 cliente y el ordenador 130 cliente lee la firma digital del médico del identificador 120 del médico y aplica una función unidireccional a la firma digital del médico para generar el segundo código 420 secreto. En la etapa 702, el ordenador 130 cliente envía las credenciales 235 que incluyen el segundo código 420 secreto a través de la red 180 de comunicaciones al servidor 160, junto con una solicitud para recuperar información 380 de resumen de indagación.

En la etapa 703, el servidor 160 recibe las credenciales 235 que incluyen el segundo código 420 secreto y las verifica con el respectivo perfil 225 del médico asociado con el nombre 230 de usuario del médico. Luego, en la etapa 704, el servidor 160 envía la información 380 resumida asociada con cada indagación 260 en el perfil 225 del médico al ordenador 130 cliente.

En la etapa 705, el ordenador 130 cliente recibe la información 380 de resumen de indagación para cada indagación en el perfil desde el servidor 160 a través de la red 180 de comunicaciones. La información 380 de resumen de indagación comprende información para que el médico la use para identificar sus solicitudes 255 de indagación y/o los respectivos reportes 265 asociados. La información 380 de resumen de indagación, en algunas realizaciones, comprende el nombre del paciente, el nombre de la indagación genómica, el estado actual de la solicitud de indagación que indica si la solicitud 255 de indagación está pendiente o finalizada, y el pedido de solicitud de indagación y las fechas de entrega. Para cada solicitud 255 de indagación procesada, la información 380 de resumen de la indagación para cada indagación puede ser utilizada por el médico para seleccionar uno correspondiente de los reportes 265 para su recuperación.

Habiendo seleccionado un reporte 265 para recuperar, el médico ahora puede recuperar el reporte 265 seleccionado. En la etapa 706, el médico realiza una selección, seleccionando uno o más reportes 265 de la información 380 de resumen de indagación para recuperación utilizando el ordenador 130 cliente, por ejemplo, seleccionando un elemento de información resumida en una pantalla de visualización en el ordenador 130 cliente.

En la etapa 707, el ordenador 130 cliente envía a través de la red 180 de telecomunicaciones al servidor 160 la selección, que es recibida por el servidor 160 en la etapa 708.

En la etapa 709, el servidor 160 identifica el valor 330 representante correspondiente a la selección para identificar la clave 250 de indagación correspondiente usando el segundo código 420 secreto como se describió anteriormente con referencia a la Figura 5b. Con la clave 250 de indagación correcta identificada, en la etapa 710, el servidor 160 encuentra el reporte 265 correspondiente utilizando la asociación 930. Como ya no es necesario, en la etapa 711, el servidor 160 borra el segundo código 420 secreto para salvaguardar la privacidad. En algunas realizaciones, el servidor 160 borra el segundo código 420 secreto al final de la segunda o tercera sesión de comunicaciones. Finalmente, en la etapa 712, el servidor 160 envía el reporte 265 identificando al ordenador 130 cliente a través de la red 180 de comunicaciones, y en la etapa 713, el ordenador 130 cliente recibe el reporte 265.

Si bien el sistema actual ha sido diseñado teniendo en cuenta el anonimato y la privacidad, a veces puede ser necesario o deseable contactar al paciente (el propietario del genoma). Un ejemplo de esto ocurre en realizaciones en las que se envía un mensaje al paciente, por ejemplo, por correo electrónico, cada vez que se procesa el primer código 410 secreto para acceder a un genoma. Para este fin, los detalles 305 de contacto se almacenan en el perfil 210 del paciente y pueden comprender uno o más de una dirección de correo electrónico, un número de teléfono o cualquier otro medio para comunicarse con el propietario del primer código 410 secreto. Con esta información, el servidor 160 envía a través de la red 180 de comunicaciones un mensaje al paciente en respuesta a la recepción del primer código 410 secreto. El mensaje puede comprender uno o más de una notificación por correo electrónico, una notificación por

teléfono móvil, un correo de voz, un mensaje SMS o cualquier otro medio de notificación al propietario del primer código 410 secreto. De esta manera, el mal uso del primer código 410 secreto es más fácil de detectar y, al mismo tiempo, garantiza el anonimato, ya que los detalles 305 de contacto están asociados con el perfil 210 del paciente, que no se pueden asociar con el genoma o clave del genoma en ausencia del primer código 410 secreto.

La descripción anterior se ha centrado en el envío de indagaciones genómicas y la recuperación de reportes 265 generados, accediendo a una base de datos que ya contiene datos 245 de genoma para el paciente. Con referencia a la Figura 8, ahora se describe un proceso para agregar datos 245 de genoma para un paciente a la base de datos. En resumen, el paciente (o el médico en nombre del paciente) comisiona el genoma del paciente para que sea secuenciado por un proveedor de secuenciación del genoma. El paciente/médico también encarga al operador del servidor 160 que aloje los datos 245 del genoma en la base de datos, y que se ponga en contacto con el proveedor de secuenciación del genoma para obtener los datos 245 del genoma y asociarlos con la clave 240 de genoma en la base de datos. Se entenderá que, en algunas circunstancias, el operador y el proveedor de secuenciación del genoma pueden ser una y la misma entidad o pueden estar controlados por la misma entidad.

Pasando ahora a la Figura 8, luego, en la etapa 801, durante una sesión de comunicaciones entre el ordenador 130 cliente y el servidor 160 durante el cual las credenciales 220 del paciente y el identificador 110 de paciente son presentados al ordenador 130 cliente, el ordenador 130 cliente lee una firma digital del paciente desde el identificador 110 de paciente y aplica una función unidireccional a la firma 200 digital del paciente para generar el primer código 410 secreto, después de lo cual, en la etapa 802, el ordenador 130 cliente envía las credenciales 220 de paciente, incluyendo el primer código 410 secreto a través de la red 180 de comunicaciones, al servidor 160.

En la etapa 803, el servidor 160 recibe las credenciales 220 de paciente, incluyendo el primer código 410 secreto del ordenador 130 cliente a través de la red 180 de comunicaciones y verifica las credenciales 210 de paciente con respecto al perfil 210 de paciente respectivo.

En la etapa 804, el servidor 160 genera la clave 240 de genoma como se describe anteriormente con referencia a la Figura 4a y la almacena en la parte 205 anónima de la base de datos. En algunas realizaciones, la clave 240 de genoma ya existe dentro de la parte 205 anónima de la base de datos. En la etapa 805, el servidor 160 genera la clave 310 de verificación del genoma utilizando la clave 240 de genoma y el primer código 410 secreto como se describió anteriormente con referencia a la Figura 4a. Luego, en la etapa 806, el servidor 160 almacena la clave 310 de verificación del genoma en el perfil 210 del paciente en la parte 200 privada de la base de datos. Como ya no es necesario, en la etapa 807, el servidor 160 elimina las credenciales 220 del paciente, incluido el primer código 410 secreto, para salvaguardar el anonimato. En algunas realizaciones, el servidor 160 elimina las credenciales 220 de paciente, incluyendo el primer código 410 secreto, al final de la sesión de comunicaciones.

Una vez que se ha generado la clave 240 del genoma en la etapa 804, el servidor 160 envía la clave 240 del genoma a través de la red 180 de comunicaciones al ordenador 130 cliente en la etapa 808, y la clave 240 del genoma se recibe en el ordenador 130 cliente en la etapa 809. El médico/paciente encarga la secuenciación del genoma del paciente enviando a un proveedor 170 de secuenciación del genoma la clave 240 de genoma, una muestra adecuada (por ejemplo, un hisopo bucal, muestra de sangre, etc.) y una solicitud para enviar los datos 245 del genoma secuenciado al operador del servidor 160 junto con la clave 240 de genoma.

En la etapa 810, el proveedor 170 de genoma recibe la clave 240 del genoma junto con la muestra que se va a secuenciar y genera los datos 245 del genoma mediante la secuenciación de la muestra en la etapa 811. El proveedor 170 de genoma realiza la extracción de ADN para el análisis de secuenciación y genera los datos 245 del genoma adecuados para el procesamiento externo. Luego, en la etapa 812, el proveedor 170 de genoma envía al servidor 160 a través de la red 180 de comunicaciones los datos 245 del genoma y la clave 240 correspondiente del genoma.

En la etapa 813, el servidor 160 recibe a través de la red 180 de comunicaciones del proveedor 170 de genoma los datos 245 del genoma y la clave 240 de genoma.

En la etapa 814, el servidor 160 indaga en la base de datos por la clave 240 del genoma y, por lo tanto, identifica dónde almacenar los datos 245 del genoma en la parte 205 anónima de la base de datos. El servidor 160 luego asocia de manera permanente la clave 240 de genoma y los datos 245 del genoma en la parte 205 anónima de la base de datos, lista para su uso como se describe anteriormente.

La descripción anterior se enfoca en detalle en el almacenamiento de los datos 245 del genoma para que sea accesible en la base de datos utilizando la clave secreta del paciente. Cuando los datos 245 del genoma son una secuencia completa del genoma, solo será necesario secuenciarlos una vez, aunque, por supuesto, el proceso se puede repetir para agregar datos adicionales del genoma 245 a la base de datos (en el caso de secuencias parciales, por ejemplo), en cuyo caso, el proceso descrito anteriormente se modifica en la etapa 804 de la Figura 8, en el sentido de que la clave 240 del genoma no se genera por primera vez, pero ya está presente cuando se genera desde el primer código 410 secreto. De la misma manera, este proceso puede ser usado para asociar datos clínicos con la clave 240 de genoma mientras se respeta el anonimato. Cuando los datos clínicos se asocian con los datos 245 del genoma en la base de datos, la base de datos se puede extraer para determinar las correlaciones genotipo-fenotipo sin comprometer

el anonimato y los datos clínicos se pueden usar para mejorar las indagaciones genómicas. Se entenderá, por supuesto, que la asociación entre los datos clínicos y los datos 245 del genoma no tiene que hacerse a través de la clave 240 del genoma, sino que podría realizarse utilizando una clave separada asociada con la clave 240 del genoma o los datos 245 del genoma.

En la realización descrita anteriormente, el proveedor del genoma envía los datos 245 del genoma junto con la clave 240 del genoma para su almacenamiento en el servidor 160 o en una base de datos mantenida por el servidor 160. En otras realizaciones, el proveedor del genoma puede almacenar los datos 245 del genoma al final y hacerlos accesibles, utilizando la clave 240 de genoma, al servidor 160, que, en consecuencia, no almacena los datos 245 del genoma, pero puede acceder al proveedor del genoma cuando sea necesario. Por supuesto, siempre que se pueda acceder a los datos 245 del genoma con la clave 240 de genoma, se pueden almacenar en cualquier otra ubicación, por ejemplo, mantenida por un tercero. Otras variaciones de proceso son igualmente posibles, por ejemplo, el servidor 160 puede enviar la clave del genoma tanto al cliente como al proveedor del genoma o solo al proveedor del genoma (con la muestra enrutada a través del operador del servidor 160 o combinada con la clave del genoma en el proveedor del genoma).

En algunas realizaciones, puede ser deseable permitir que el paciente pueda acceder a su reporte 265 sin el médico, por ejemplo, para discutirlo con un tercero. En algunas realizaciones, esto se implementa utilizando los procesos descritos anteriormente con referencia a las Figuras 5a, 5b y 7, reemplazando el segundo código 420 secreto que pertenece al médico con el primer código 410 secreto que corresponde al paciente, permitir el acceso del paciente además del médico o en su lugar. De manera similar, en algunas realizaciones, la interacción del sistema es solo con el paciente, en cuyo caso el paciente posee el primero y segundo identificadores 110,120 físicos y el primer código 410 secreto y el segundo código 420 secreto, o el primero y segundo identificadores 110,120 y/o los códigos 410, 420 secretos pueden reemplazarse con un solo identificador y un código secreto que combina las funciones descritas anteriormente para los identificadores/códigos secretos separados.

Las realizaciones descritas anteriormente hacen referencia a los perfiles de usuario para el paciente/médico, en los que diversos elementos de datos permiten que las asociaciones entre las partes privadas y anónimas de la base de datos se realicen en presencia del código secreto relevante. El acceso a los perfiles se ha descrito como uno con dos factores, que incluyen un nombre de usuario y una contraseña, así como un código secreto derivado del identificador. Se entenderá que la verificación de un solo factor utilizando solo el código secreto y el nombre de usuario es igualmente posible. Del mismo modo, los perfiles no necesitan contener toda la información descrita anteriormente. Por ejemplo, para implementar la funcionalidad central, sería suficiente si los perfiles incluyeran las claves de verificación y los valores de representantes relevantes. Incluso la inclusión de nombres de usuario en los perfiles podría ser opcional y reemplazarse con una indagación exhaustiva de las claves de verificación relevantes utilizando el código secreto relevante y/o los valores de representantes, según sea el caso.

Las realizaciones descritas anteriormente se basan en la generación de claves de verificación utilizadas en indagaciones de base de datos para identificar claves en la parte anónima de la base de datos. Sin embargo, en otras realizaciones, descritas a continuación, las claves en la parte anónima son generadas por las respectivas funciones unidireccionales respectivas y, por lo tanto, estas realizaciones prescinden del uso de claves de verificación. Algunas de estas realizaciones se describen a continuación. Como se describe, estas realizaciones utilizan credenciales que consisten solo en el código secreto relevante, pero, por supuesto, también se pueden incluir otros factores en las credenciales.

En lo que sigue, se describen realizaciones que usan funciones unidireccionales para la generación e identificación de claves combinadas. Estas realizaciones se describen ahora con referencia a las Figuras 9 y 10, haciendo referencia a las Figuras 6 y 7 para indicar cómo los procesos en estas realizaciones difieren de los descritos anteriormente. La siguiente descripción se realiza en términos de credenciales que incluyen solo los códigos secretos generados por identificadores descritos anteriormente, pero se entenderá que se pueden incluir otros factores.

Con referencia al proceso descrito en la Figura 6, las realizaciones que usan funciones unidireccionales para la generación e identificación de claves combinadas reemplazan las etapas 605 a 609 con el siguiente proceso. El servidor 160 recibe el primer código 410 secreto, el segundo código 420 secreto y la solicitud 255 de indagación. El estado de la información almacenada en la base de datos se ilustra en la Figura 9a. El servidor 160 almacena el primer código 410 secreto, el segundo código 420 secreto y la solicitud 255 de indagación en la base de datos del genoma que contiene una o más claves 240 de genoma asociadas con los datos 245 del genoma respectivo, típicamente uno para cada paciente. Cada clave 240 de genoma y datos 245 de genoma están asociados de forma única con un paciente.

El servidor 160 asocia entonces un valor 330 representante que es único para la solicitud de indagación con la solicitud 255 de indagación mediante una asociación 900 entre el valor 330 representante y la solicitud 255 de indagación, como se ilustra en la Figura 9b. En algunas realizaciones, el valor 330 representante se genera previamente antes de recibir la solicitud 255 de indagación. En algunas realizaciones, el servidor 160 genera o selecciona el valor 330 representante en respuesta a la recepción de la solicitud 255 de indagación asignando identificadores universalmente únicos. Posteriormente, el servidor 160 aplica una primera función 905 unidireccional al primer código 410 secreto

para generar la clave 240 de genoma (ver Figura 9b). Dado que los datos 245 del genoma se asocian únicamente con esta clave 240 de genoma, como se describió anteriormente, los datos 245 del genoma que pertenecen al paciente se encuentran de esta manera utilizando el primer código 410 secreto.

El servidor 160 también aplica una segunda función 910 unidireccional a una combinación del segundo código 420 secreto y el valor 330 representante para generar la clave 250 de indagación y el servidor 160 aplica una tercera función 915 unidireccional al segundo código 420 secreto para generar una clave 920 de agrupación (véase la Figura 9b). El servidor 160 crea una asociación 925 entre la clave 920 de agrupación y el valor 330 representante. De esta manera, la clave 920 de agrupación se asocia de forma única con el médico y, al asociar el valor 330 representante y, por lo tanto, la clave 250 de indagación con la agrupación con la clave 920, el médico puede acceder posteriormente a sus indagaciones, tal como se describe a continuación (véase la Figura 9c). Típicamente, una pluralidad de valores 330 representantes (y, por lo tanto, las solicitudes 255 de indagación del mismo médico, para sus pacientes) estarán asociadas con cada clave 920 de agrupación. El servidor 160 crea el enlace 270 temporal entre la clave 250 de indagación y la clave 240 del genoma y almacena el enlace 270 temporal en la base de datos, de manera que luego se pueda eliminar.

En cuanto a la etapa 611 descrita anteriormente, después de almacenar el enlace 270 temporal, el servidor 160 elimina el primer código 410 secreto y el segundo código 420 secreto después de generar la clave 240 del genoma y la clave 250 de indagación. En algunas realizaciones, el servidor 160 borra el primer código 410 secreto y el segundo código 420 secreto al final de la primera sesión de comunicaciones. Una vez que se eliminan el primer código 410 secreto y el segundo código 420 secreto, ya no es posible rastrear al médico y al paciente, ya que las claves generadas están vinculadas a los códigos secretos mediante funciones unidireccionales.

De manera similar a la etapa 612, para procesar la indagación genómica, el servidor 160 identifica los datos 245 del genoma utilizando la clave 240 del genoma. De este modo, a través del enlace 270 temporal creado entre la clave 250 de indagación y la clave 240 del genoma los datos 245 del genoma se identifican para ejecutar la indagación 260 de la solicitud 255 de indagación en él (ver 9d). De forma similar a las etapas 613 y 615 descritos anteriormente, la indagación 260 se procesa y, una vez que ya no es necesaria, se elimina el enlace 270 temporal.

En cuanto a las realizaciones descritas anteriormente, después de una o más primeras sesiones de comunicaciones, la base de datos del servidor 160 comprende uno o más reportes 265 y una o más claves 240 de indagación asociadas por medio de las asociaciones 930 respectivas en la base de datos. El estado de la información almacenada en la base de datos en realizaciones que utilizan funciones unidireccionales para la generación e identificación de claves combinadas se ilustra en la Figura 10a. La base de datos comprende además la clave 920 de agrupación asociada con el médico y uno o más valores 330 representantes correspondientes a la una o más solicitudes 255 de indagación y los reportes 265 asociados con la clave 920 de agrupación por las asociaciones 925. Por lo tanto, los reportes están listos para su recopilación como se describirá ahora.

Con referencia al proceso descrito en la Figura 7, las realizaciones que usan funciones unidireccionales para la generación e identificación de claves combinadas reemplazan las etapas 703, 704 con el siguiente proceso. Al recibir el segundo código secreto, el servidor 160 aplica la tercera función 915 unidireccional al segundo código 420 secreto para generar la clave 920 de agrupación. El estado de la información almacenada en la base de datos en este punto se ilustra en la Figura 10b. El servidor 160 identifica el uno o más valores 330 representantes asociados con la clave 920 de agrupación por medio de asociaciones 925 y aplica la segunda función 910 unidireccional a una combinación del segundo código 420 secreto y uno o más valores 330 representantes identificados. De esta manera, el servidor 160 genera una o más claves 240 de indagación, cada una asociada con un reporte 265 por medio de la asociación 930 (véase la Figura 10c). Usando las claves 240 de indagación generadas, el servidor 160 identifica la información 380 de resumen de indagación asociada con los respectivos reportes 265 asociados con la respectiva una o más claves 240 de indagación (ver 10d). El servidor 160 luego borra el segundo código 420 secreto (véase la Figura 10e) y envía la información 380 de resumen de la indagación a través de la red 180 de comunicaciones al ordenador 130 cliente.

En el lado del cliente, las etapas 705 a 707 son igualmente aplicables a las realizaciones que utilizan funciones unidireccionales para la generación e identificación de claves combinadas. De manera similar a la etapa 708, el servidor 160 recibe el segundo código 420 secreto y la selección asociada con la información 380 de resumen de la indagación (véase la Figura 10f). Posteriormente, el servidor 160 aplica la tercera función 915 unidireccional al segundo código 420 secreto para generar la clave 920 de agrupación. Usando la clave 920 de agrupación generada, el servidor 160 identifica uno o más valores 330 representantes asociados con la clave 920 de agrupación por medio de las asociaciones 925 (ver Figura 10g).

Para facilitar la recuperación de reportes, en algunas realizaciones, cada reporte 265 identificado en la información 380 de resumen de indagación está asociado con un identificador 940 correspondiente (véase la Figura 10h). El servidor 160 almacena una asociación 945 entre el identificador 940 y el valor 330 representante correspondiente al reporte 265 para permitir la recuperación del reporte 265. El ordenador 130 cliente recibe los identificadores 940 junto con la información 380 de resumen de indagación y envía el identificador 940 correspondiente al servidor 160 a través

de la red 180 de comunicaciones cuando el médico realiza la selección. El servidor 160 puede entonces identificar el valor 330 representante correspondiente al identificador 940 utilizando la asociación 945.

De manera similar a la etapa 709, el servidor 160 identifica el valor 330 representante asociado con la solicitud 255 de indagación seleccionada o el reporte 265, pero luego aplica la segunda función 910 unidireccional a una combinación del segundo código 420 secreto y el valor 330 representante identificado correspondiente a la selección para generar la clave 240 de indagación correspondiente (véase la Figura 10h). Como la clave de indagación 240 generada, por definición, corresponde al reporte 265 seleccionado, el servidor 160 identifica el reporte 265 correspondiente utilizando la asociación 930, similar a la etapa 710 anterior. Como ya no es necesario, el servidor 160 luego borra el segundo código 420 secreto, para salvaguardar la privacidad y envía el reporte 265 correspondiente a la selección al cliente 130 para su revisión por parte del médico, análogo a las etapas 711 y 712 descritos anteriormente.

De manera similar a las realizaciones descritas anteriormente, puede ser deseable proporcionar acceso a los reportes generados al paciente además del médico o en su lugar. Esto se puede lograr generando una clave de agrupación de pacientes desde el primer código 410 secreto y asociando los valores 330 representantes de los reportes de indagación 265 generados para el paciente (usando la primera secreta 410) con esta clave de agrupación de pacientes. Usando los procesos descritos anteriormente, reemplazando la clave 920 de agrupación con una clave de agrupación de pacientes y el segundo código 420 secreto con el primer código 410 secreto, se puede habilitar al paciente para acceder a sus reportes 265.

La descripción anterior de las realizaciones que utilizan funciones unidireccionales para la generación e identificación de claves combinadas se ha centrado en la generación de indagaciones y la recuperación de reportes. Naturalmente, antes de estos procesos, la base de datos debe estar poblada con datos del genoma. El proceso y sus variaciones, descritos anteriormente con referencia a la Figura 8, son igualmente aplicables a estas realizaciones, con la omisión de las etapas 805 y 806 relacionados con la generación de la clave de verificación del genoma y observando que la clave del genoma debe generarse desde el primer código secreto utilizando la primera función unidireccional (es decir, la misma función unidireccional utilizada para generar la clave del genoma para la recuperación/asociación de datos). En otras palabras, la clave del genoma debe generarse para estas realizaciones desde el primer código secreto usando una función unidireccional fija que luego también se usa para la generación de la clave del genoma para la asociación y recuperación, es decir, sin una semilla aleatoria variable como se describió anteriormente en el contexto de la Figura 8. Además, naturalmente, la clave del genoma no puede ser simplemente generada -previamente, sino que debe ser específica para el primer código secreto.

Si bien el sistema actual ha sido diseñado teniendo en cuenta el anonimato y la privacidad, a veces puede ser necesario o deseable contactar al paciente (el propietario del genoma). Un ejemplo de esto ocurre en realizaciones, donde se envía un mensaje al paciente, por ejemplo, por correo electrónico, cada vez que se procesa el primer código 410 secreto para acceder a un genoma. Para reconciliar esto con el mantenimiento de la privacidad y el anonimato, en algunas realizaciones, se utiliza una cuarta función de un solo sentido. Específicamente, en algunas realizaciones, el servidor 160 aplica una cuarta función unidireccional al primer código 410 secreto para generar una clave de contacto en respuesta a la recepción del primer código 410 secreto. La clave de contacto está asociada con la información de contacto contenida en la base de datos para el paciente. Para este fin, la información de contacto se almacena en el perfil 210 del paciente y puede comprender uno o más de una dirección de correo electrónico, un número de teléfono o cualquier otro medio para comunicarse con el propietario del primer código 410 secreto. Con esta información, el servidor 160 envía a través de la red 180 de comunicaciones un mensaje al paciente en respuesta a la recepción del primer código 410 secreto. El mensaje puede comprender uno o más de una notificación por correo electrónico, una notificación de teléfono móvil, un correo de voz, mensaje SMS o cualquier otro medio para notificar al propietario del primer código 410 secreto. De esta manera, el mal uso del primer código 410 secreto es más fácil de detectar, al mismo tiempo que garantiza el anonimato, ya que la información de contacto está asociada con la clave de contacto, que no puede volver al paciente o acceder a los datos almacenados en la base de datos. Se entenderá que la clave de contacto (o una clave similar) se puede usar para asociar información de contacto y/u otros datos personales con el primer código secreto para fines distintos a los descritos anteriormente.

Si bien se han descrito varias formas de realización diferentes, algunas con referencia a las Figuras 2 a 8, otras con referencia principalmente a las Figuras 9 y 10, se apreciará que los diversos procesos pueden combinarse y que las características de cualquiera de los conjuntos de realizaciones se pueden añadir al otro. Por ejemplo, el uso de las claves de verificación descritas anteriormente se puede combinar con el concepto de agrupación de claves y funciones unidireccionales específicas para generar e identificar claves (o cadenas específicas de las funciones), y se puede almacenar en los perfiles de usuario. Por lo tanto, son posibles diversas combinaciones y se describen a continuación. Además, en todas las realizaciones descritas en este documento, la referencia a partes privadas y anónimas de la base de datos puede referirse a partes físicas, por ejemplo, servidores o unidades independientes, o pueden ser lógicas o incluso meramente distinciones conceptuales para propósitos de la descripción, en lugar de partes físicamente distinguibles. Además, se entenderá que las asociaciones en la base de datos a la que se hace referencia en este documento pueden ser explícitas, almacenando un enlace a un elemento de datos con el asociado con él, o implícitas almacenando los elementos de datos asociados juntos, por ejemplo, en la misma fila de la base de datos.

Las realizaciones anteriores se basan en varias funciones unidireccionales para generar varias claves desde el primer código 410 secreto y el segundo código 420 secreto. Las funciones unidireccionales pueden ser de cualquier tipo, siempre que sea imposible en la práctica inferir la entrada a partir de la salida (resistencia a preimagen). La fortaleza de la protección de anonimato proporcionada por las realizaciones anteriores depende de la fortaleza de las funciones unidireccionales utilizadas. En algunas realizaciones, en realizaciones particulares que usan funciones unidireccionales para la generación e identificación de claves combinadas, las diversas funciones unidireccionales usan una función unidireccional común, que se distingue por cadenas respectivas con las cuales las entradas de función se concatenan antes de ser aplicado a la función unidireccional común para generar una salida. Específicamente, en algunas realizaciones se usa una cadena alfanumérica de 64 caracteres. En particular, en el contexto de las realizaciones que utilizan funciones unidireccionales para la generación e identificación de claves combinadas, la cadena para cada función unidireccional se genera aleatoriamente, por ejemplo, pero luego se mantiene constante para asegurar cálculos consistentes de las diversas claves desde la primera y los segundos códigos secretos, según sea el caso.

Habiendo leído la descripción específica anterior de algunas realizaciones de ejemplo, el experto sabrá que es posible usar combinaciones, modificaciones y yuxtaposiciones de las características y realizaciones anteriores que no están limitadas a los ejemplos específicos descritos anteriormente. Por ejemplo, aunque las etapas del proceso se han descrito en un cierto orden, el orden puede variar de una realización a otra en la medida en que la información necesaria esté disponible para cada paso cuando sea necesario. La invención se define por las reivindicaciones adjuntas.

REIVINDICACIONES

1. Un método para procesar una indagación en un genoma para producir un reporte, comprendiendo el método:

recibir un primer código secreto, un segundo código secreto y una solicitud de indagación a través de una red de comunicaciones durante una primera sesión de comunicaciones y almacenar un valor de representante asociado con la solicitud de indagación en una base de datos;

usar el primer código secreto para determinar una clave del genoma que permita el acceso a los datos del genoma almacenados en la base de datos y asociados con el primer código secreto;

asociar el valor de representante y una clave de indagación utilizando el segundo código secreto, de modo que la clave de indagación solo se puede encontrar con el valor de representante utilizando tanto el valor de representante como el segundo código secreto;

almacenar una asociación entre la clave del genoma y la clave de indagación en la base de datos;

eliminar el primer y segundo código secreto después de determinar la clave del genoma y asociar el valor de representante y la clave de indagación durante o al final de la primera sesión de comunicaciones;

identificar el genoma utilizando la clave del genoma y aplicar una indagación asociada con la solicitud de indagación al genoma identificado para generar un reporte;

almacenar el reporte en la base de datos en asociación con la clave de indagación, por lo que se puede acceder al reporte en la base de datos utilizando la clave de indagación; y

posteriormente al almacenamiento del reporte, se elimina la asociación entre el genoma y las claves de indagación.

2. El método de la reivindicación 1, en donde determinar la clave del genoma usando el primer código secreto comprende evaluar una función que combina una clave de genoma candidata en la base de datos con el primer código secreto y comparar el resultado con una clave de verificación del genoma asociada con el primer código secreto para encontrar una coincidencia entre el resultado y la clave de verificación, opcionalmente, en donde la función que combina la clave del genoma candidato con el primer código secreto es una función unidireccional y, opcionalmente, la clave de verificación del genoma se almacena en un perfil de usuario accesible con credenciales que incluyen el primer código secreto.

3. El método de la reivindicación 1 o 2, en donde asociar el valor de representante y la clave de indagación comprende calcular una clave de verificación de indagación como una función que combina el valor de representante, la clave de indagación y el segundo código secreto y almacenar la clave de verificación de indagación en la base de datos, opcionalmente en donde la función que combina el valor de representante, la clave de indagación y el segundo código secreto es una función unidireccional y, de manera opcional, la clave de verificación de la indagación se almacena en un perfil de usuario accesible con credenciales, incluido el segundo código secreto.

4. El método de cualquier reivindicación precedente, que comprende recibir el segundo código secreto a través de una red de comunicaciones durante una segunda sesión de comunicaciones posterior;

usar el segundo código secreto y el valor del representante para determinar la clave de indagación;

eliminar el segundo código secreto posterior a la determinación de la clave de indagación durante o al final de la segunda sesión de comunicaciones;

identificar el reporte usando la clave de indagación;

y enviar el reporte a través de la red de comunicaciones durante la segunda sesión de comunicaciones.

5. El método de la reivindicación 4, que comprende almacenar una pluralidad de valores de representantes en la base de datos de modo que sean accesibles utilizando credenciales que incluyen el segundo código secreto, y que además comprende, durante la segunda sesión de comunicación, recibir una selección de usuario de un reporte para recuperar, en donde el valor de representante utilizado para determinar la clave de indagación corresponde al reporte seleccionado que se recuperará.

6. Un método para poblar una base de datos genómica, comprendiendo el método:

recibir un primer código secreto a través de una red de comunicaciones durante una sesión de comunicaciones;

usar el primer código secreto y una clave del genoma para generar una clave de verificación del genoma asociada con el primer código secreto y la clave del genoma, por lo que la clave del genoma puede combinarse con la clave de verificación del genoma utilizando solo el primer código secreto y la clave de verificación del genoma;

enviar la clave del genoma a través de la red de comunicaciones para permitir que se asocie con un genoma secuenciado por un proveedor del genoma; y

eliminar el primer código secreto posterior a la generación de la clave de verificación del genoma durante o al final de la sesión de comunicaciones,

comprendiendo el método opcionalmente demás

recibir datos del genoma junto con la clave del genoma; y

almacenar los datos del genoma en la base de datos en asociación con la clave del genoma.

7. El método de cualquier reivindicación precedente, en donde el primer código secreto está asociado con un paciente, y

en donde el segundo código secreto está asociado con un médico.

8. Un producto de programa de ordenador que comprende instrucciones codificadas, que, cuando se ejecuta en un procesador, implementa un método de acuerdo con cualquier reivindicación precedente.

9. Un sistema para procesar una indagación en un genoma para producir un reporte, comprendiendo el sistema una base de datos y un procesador, en donde el procesador está configurado para:

recibir un primer código secreto, un segundo código secreto y una solicitud de indagación a través de una red de comunicaciones durante una primera sesión de comunicaciones y almacenar un valor de representante asociado con la solicitud de indagación en una base de datos;

usar el primer código secreto para determinar una clave de genoma que permita el acceso a los datos del genoma almacenados en la base de datos y asociados con el primer código secreto;

asociar el valor de representante y una clave de indagación utilizando el segundo código secreto, de modo que la clave de indagación solo se pueda encontrar con el valor de representante utilizando tanto el valor de representante como el segundo código secreto;

almacenar una asociación entre la clave del genoma y la clave de indagación en la base de datos;

eliminar el primer y segundo código secreto después de determinar la clave del genoma y asociar el valor de representante y la clave de indagación durante o al final de la primera sesión de comunicaciones;

identificar el genoma mediante la clave del genoma y aplicar una indagación asociada con la solicitud de indagación al genoma identificado para generar un reporte;

almacenar el reporte en la base de datos en asociación con la clave de indagación, por lo que se puede acceder al informar en la base de datos utilizando la clave de indagación; y

después de almacenar el reporte, eliminar la asociación entre el genoma y las claves de indagación.

10. El sistema de la reivindicación 9, en donde determinar la clave del genoma usando el primer código secreto comprende evaluar una función que combina una clave de genoma candidata en la base de datos con el primer código secreto y comparar el resultado con una clave de verificación del genoma asociada con el primer código secreto para encontrar una coincidencia entre el resultado y la clave de verificación, opcionalmente, en donde la función de combinar la clave del genoma candidato con el primer código secreto es una función unidireccional y, opcionalmente, la clave de verificación del genoma se almacena en un perfil de usuario accesible con credenciales que incluyen el primer código secreto.

11. El sistema de la reivindicación 9 o 10, en donde asociar el valor de representante y la clave de indagación comprende calcular una clave de verificación de indagación como una función que combina el valor de representante, la clave de indagación y el segundo código secreto y almacenar la clave de verificación de indagación en la base de datos, opcionalmente en donde la función que combina el valor de representante, la clave de indagación y el segundo código secreto es una función unidireccional y, de manera opcional, la clave de verificación de la indagación se almacena en un perfil de usuario accesible con credenciales, incluido el segundo código secreto.

12. El sistema de una cualquiera de las reivindicaciones 9 a 11, en donde el procesador está configurado para:

recibir el segundo código secreto a través de una red de comunicaciones durante una segunda sesión de comunicaciones posterior;

usar el segundo código secreto y el valor de representante para determinar la clave de indagación;

eliminar el segundo código secreto posterior a la determinación de la clave de indagación durante o al final de la segunda sesión de comunicaciones;

identificar el reporte utilizando la clave de indagación; y

enviar el reporte a través de la red de comunicaciones durante la segunda sesión de comunicaciones.

13. El sistema de la reivindicación 12, en donde el procesador está configurado para almacenar una pluralidad de valores de representantes en la base de datos de modo que sean accesibles usando credenciales que incluyen el segundo código secreto y

en donde el procesador está configurado para recibir, durante la segunda sesión de comunicación, una selección de usuario de un reporte que se recuperará, en donde el valor de representante utilizado para determinar la clave de indagación corresponde al reporte seleccionado que se recuperará.

14. Un sistema para poblar una base de datos genómica, comprendiendo el sistema una base de datos y un procesador configurado para:

recibir un primer código secreto a través de una red de comunicaciones durante una sesión de comunicaciones;

usare el primer código secreto y una clave del genoma para generar una clave de verificación del genoma asociada con el primer código secreto y la clave del genoma, por lo que la clave del genoma puede combinarse con la clave de verificación del genoma utilizando solo el primer código secreto y la clave de verificación del genoma;

enviar la clave del genoma a través de la red de comunicaciones para permitir que se asocie con un genoma secuenciado por un proveedor del genoma; y

eliminar el primer código secreto posterior a la generación de la clave de verificación del genoma durante o al final de la sesión de comunicaciones,

estando el procesador opcionalmente configurado para

recibir datos del genoma junto con la clave del genoma; y

almacenar los datos del genoma en la base de datos en asociación con la clave del genoma.

15. El sistema de una cualquiera de las reivindicaciones 9 a 14, en donde el primer código secreto está asociado con un paciente y en donde el segundo código secreto está asociado con un médico.

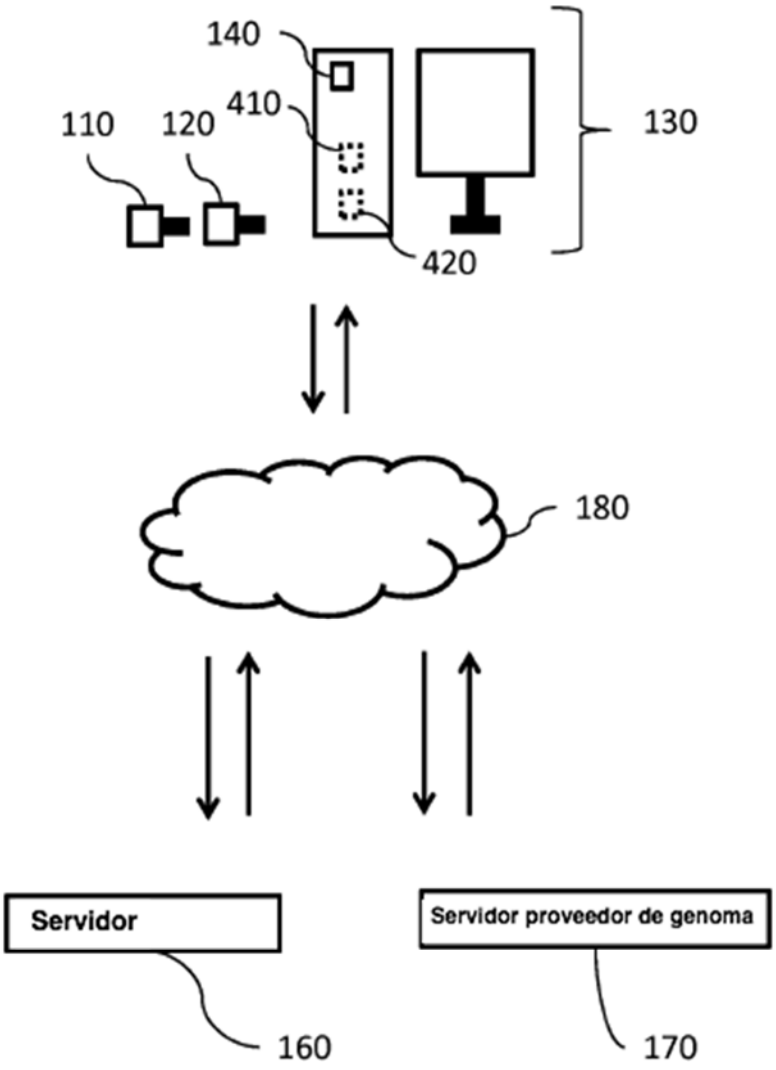
140
410
110
120
130
420
180
Servidor
Servidor proveedor de genoma
160
170

Figura 1

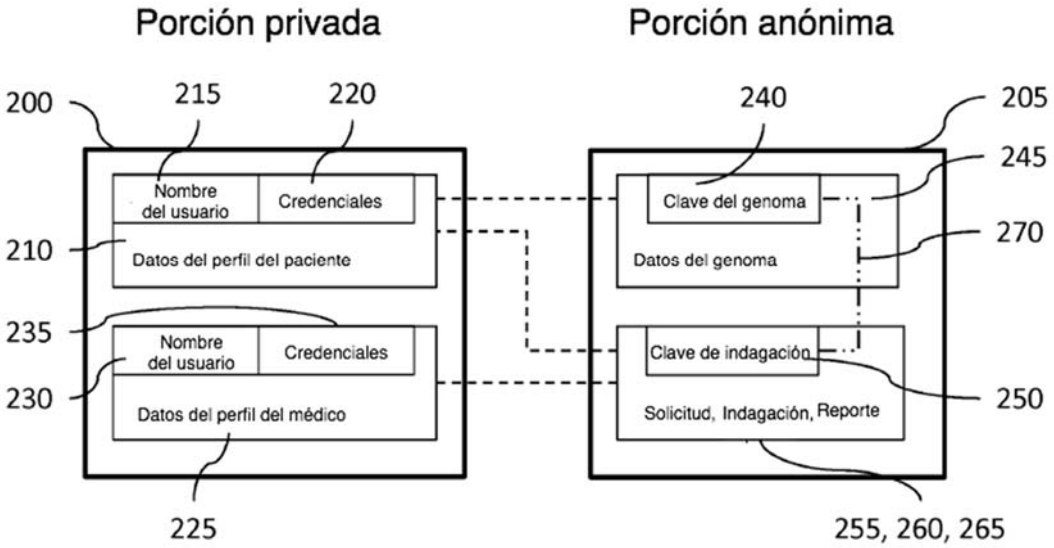
Porción privada
Porción anónima
200
215
220
240
205
245
Nombre del usuario
Credenciales
Clave del genoma
210
Datos del perfil del paciente
270
Datos del genoma
235
Nombre del usuario
Credenciales
Clave de indagación
230
250
Datos del perfil del médico
Solicitud, Indagación, Reporte
225
255, 260, 265
Asociaciones que no son almacenadas en el servidor y pueden ser hechas solo utilizando el código secreto
Enlace temporal hecho solo mientras la indagación está siendo procesada

Figura 2

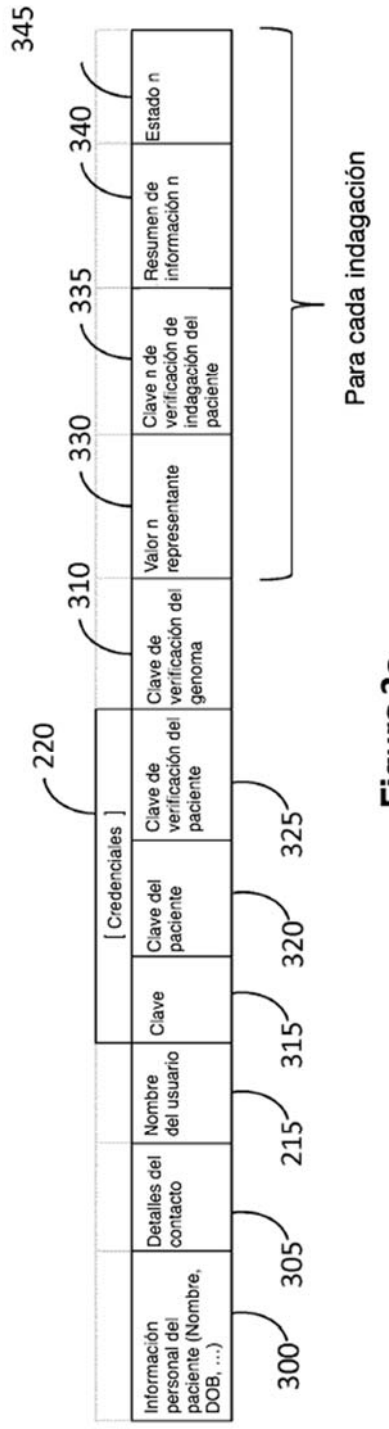

Figura 3a

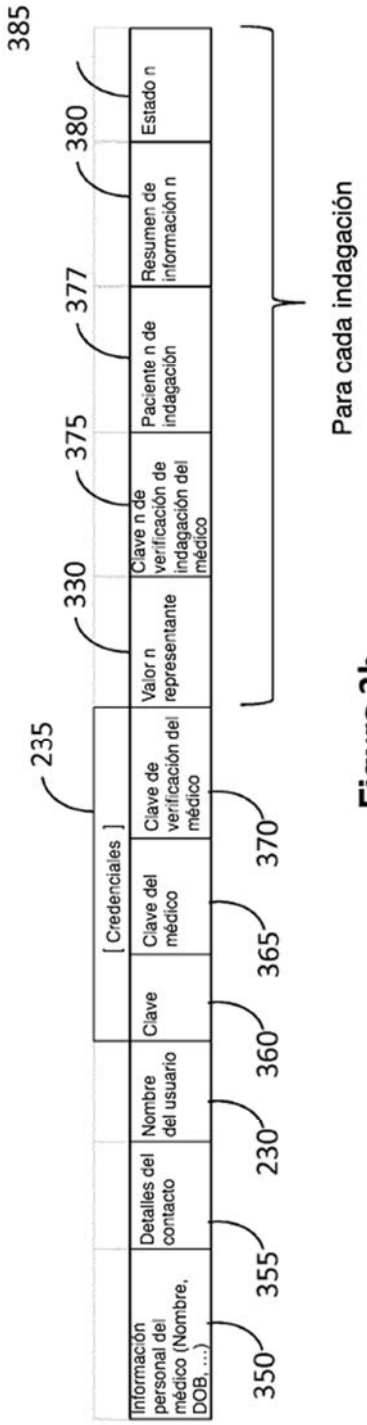

Figura 3b

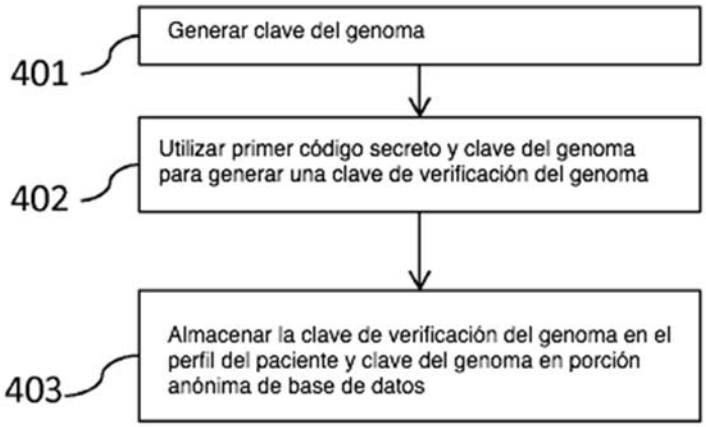

Figura 4a

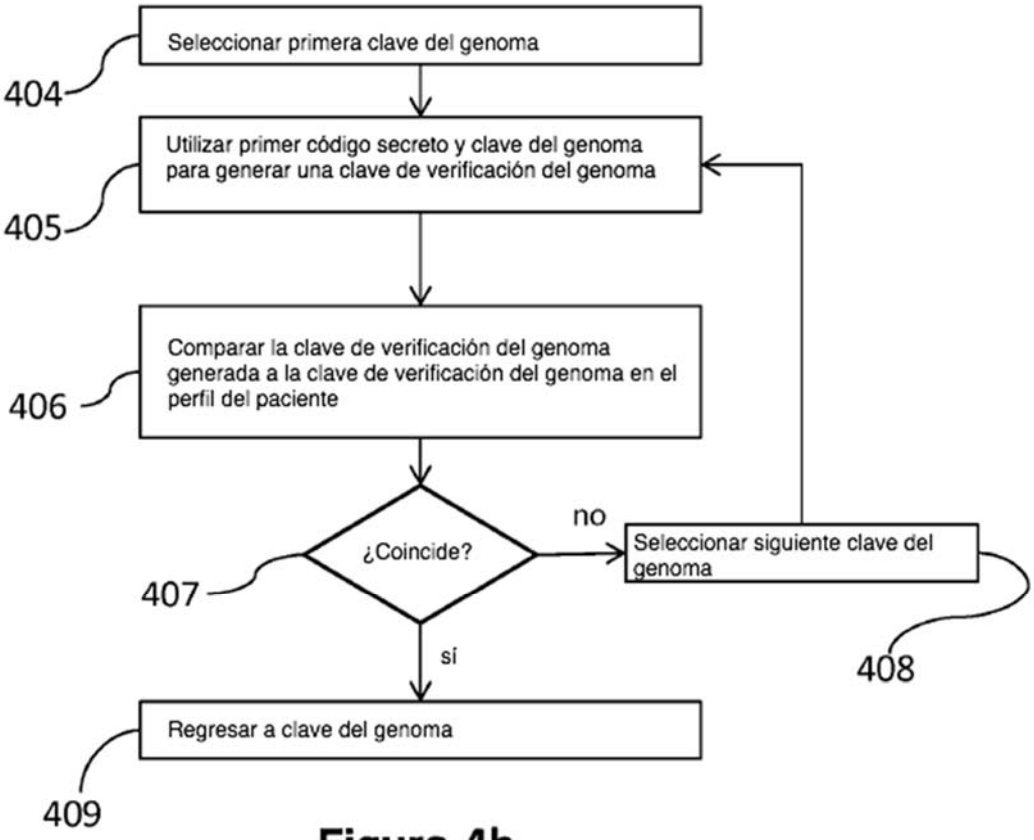

Figura 4b

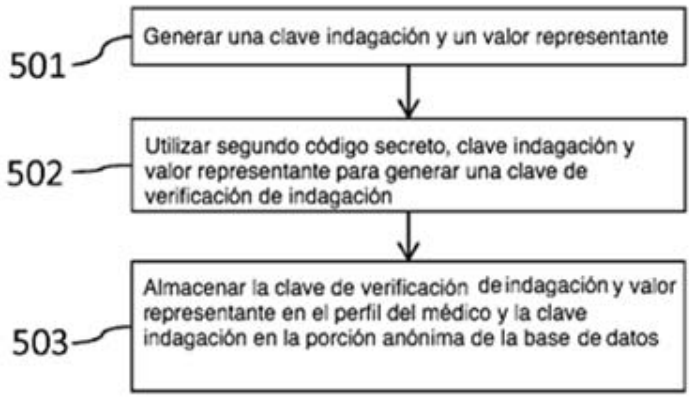

Figura 5a

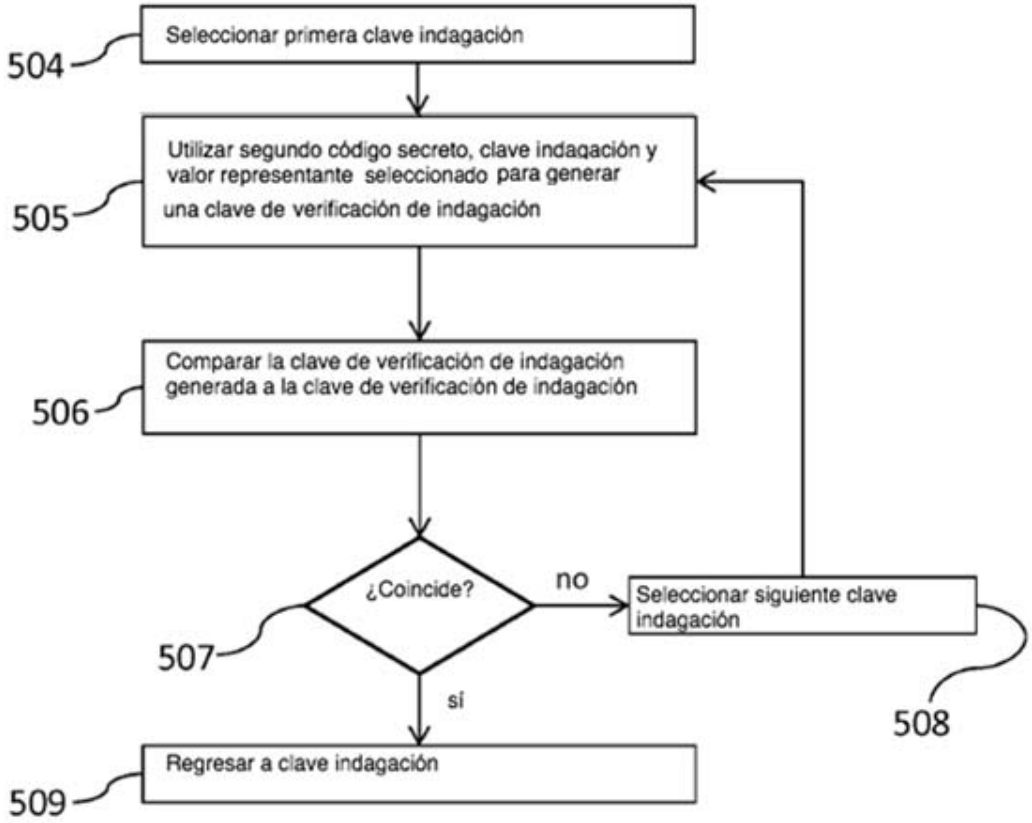

Figura 5b

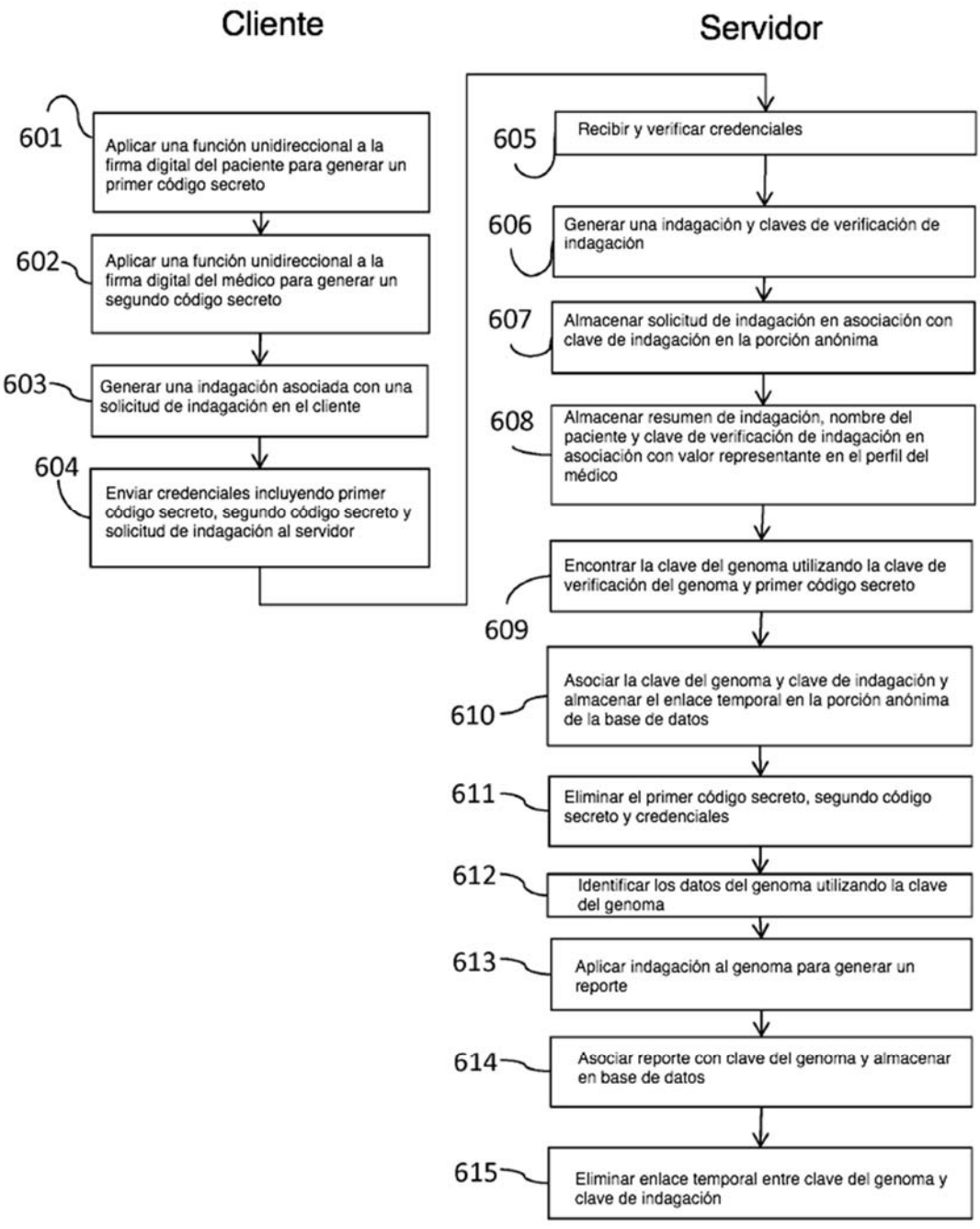
Cliente
Servidor
601
Aplicar una función unidireccional a la firma digital del paciente para generar un primer código secreto
602
Aplicar una función unidireccional a la firma digital del médico para generar un segundo código secreto
603
Generar una indagación asociada con una solicitud de indagación en el cliente
604
Enviar credenciales incluyendo primer código secreto, segundo código secreto y solicitud de indagación al servidor
605
Recibir y verificar credenciales
606
Generar una indagación y claves de verificación de indagación
607
Almacenar solicitud de indagación en asociación con clave de indagación en la porción anónima
608
Almacenar resumen de indagación, nombre del paciente y clave de verificación de indagación en asociación con valor representante en el perfil del médico
609
Encontrar la clave del genoma utilizando la clave de verificación del genoma y primer código secreto
610
Asociar la clave del genoma y clave de indagación y almacenar el enlace temporal en la porción anónima de la base de datos
611
Eliminar el primer código secreto, segundo código secreto y credenciales
612
Identificar los datos del genoma utilizando la clave del genoma
613
Aplicar indagación al genoma para generar un reporte
614
Asociar reporte con clave del genoma y almacenar en base de datos
615
Eliminar enlace temporal entre clave del genoma y clave de indagación

Figura 6

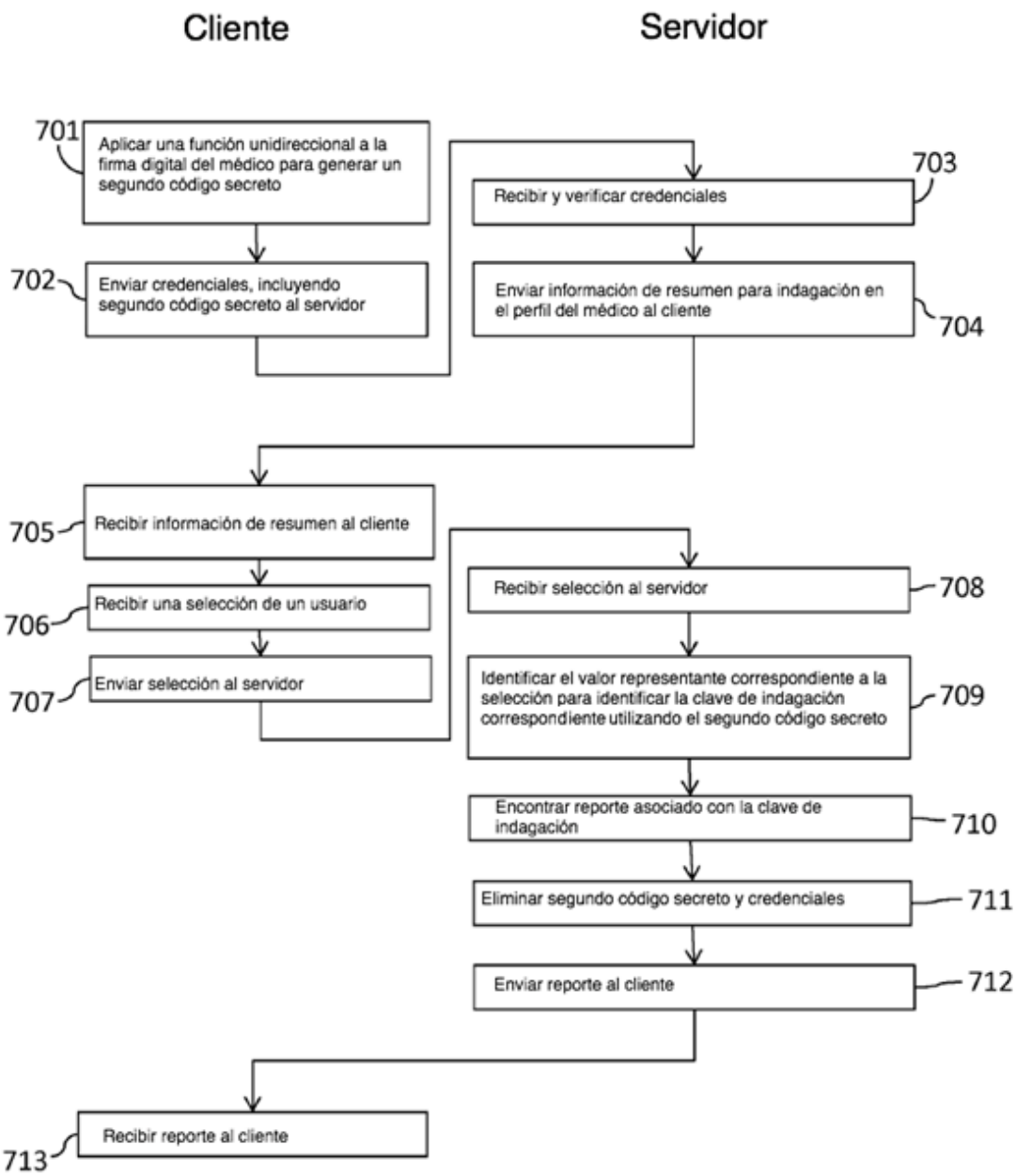
Cliente
Servidor
701
Aplicar una función unidireccional a la firma digital del médico para generar un segundo código secreto
702
Enviar credenciales, incluyendo segundo código secreto al servidor
703
Recibir y verificar credenciales
Enviar información de resumen para indagación en el perfil del médico al cliente
704
705
Recibir información de resumen al cliente
706
Recibir una selección de un usuario
707
Enviar selección al servidor
Recibir selección al servidor
708
Identificar el valor representante correspondiente a la selección para identificar la clave de indagación correspondiente utilizando el segundo código secreto
709
Encontrar reporte asociado con la clave de indagación
710
Eliminar segundo código secreto y credenciales
711
Enviar reporte al cliente
712
713
Recibir reporte al cliente

Figura 7

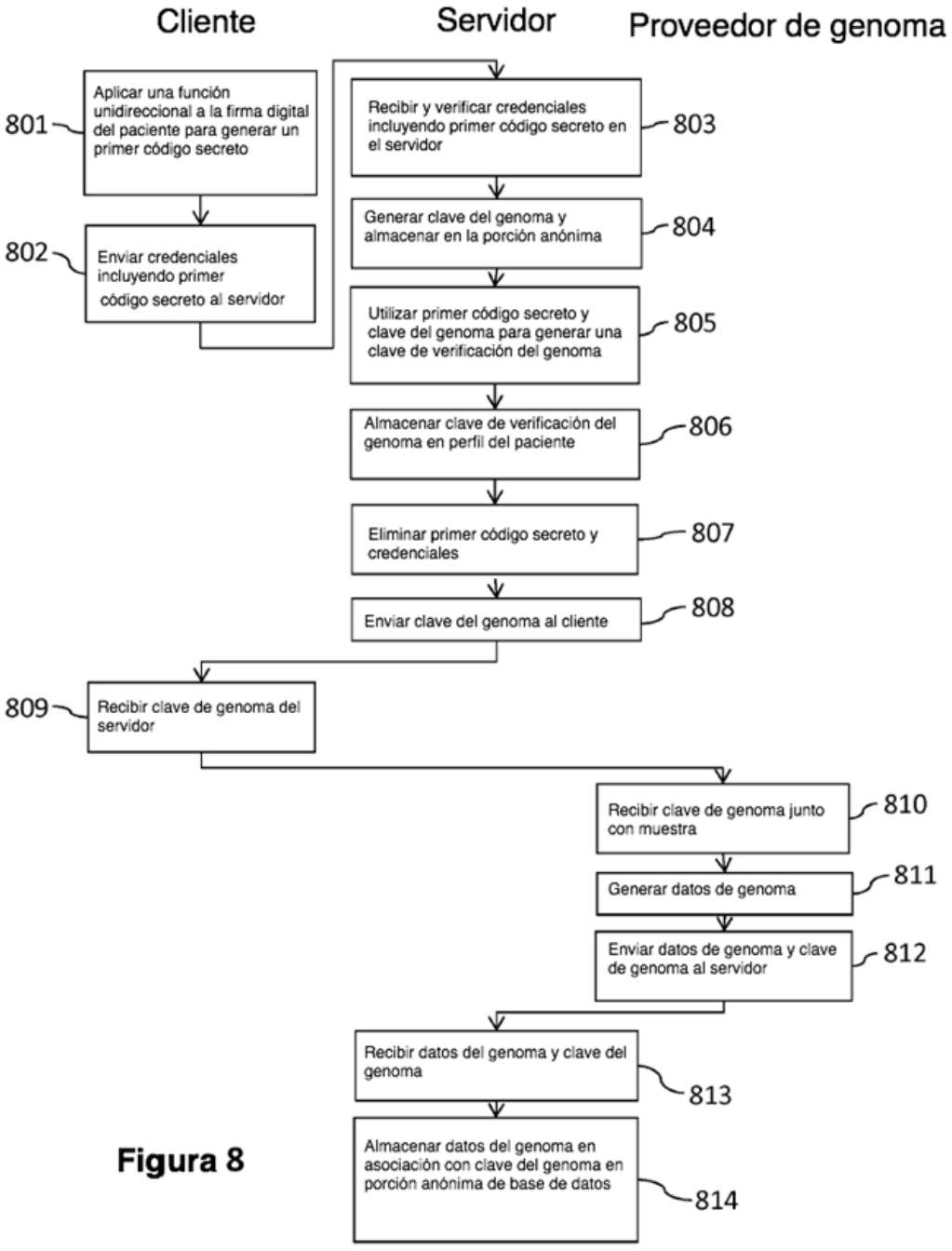
Cliente
Servidor
Proveedor de genoma
Aplicar una función unidireccional a la firma digital del paciente para generar un primer código secreto
801
Enviar credenciales incluyendo primer código secreto al servidor
802
Recibir y verificar credenciales incluyendo primer código secreto en el servidor
803
Generar clave del genoma y almacenar en la porción anónima
804
Utilizar primer código secreto y clave del genoma para generar una clave de verificación del genoma
805
Almacenar clave de verificación del genoma en perfil del paciente
806
Eliminar primer código secreto y credenciales
807
Enviar clave del genoma al cliente
808
Recibir clave de genoma del servidor
809
Recibir clave de genoma junto con muestra
810
Generar datos de genoma
811
Enviar datos de genoma y clave de genoma al servidor
812
Recibir datos del genoma y clave del genoma
813
Almacenar datos del genoma en asociación con clave del genoma en porción anónima de base de datos
814

Figura 8

Figura 9a

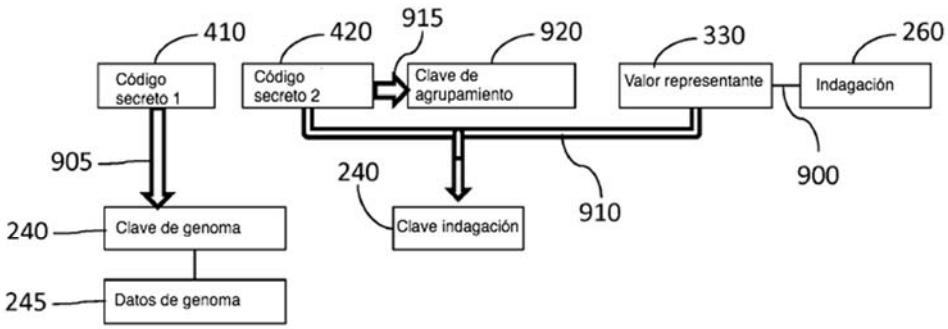

Figura 9b

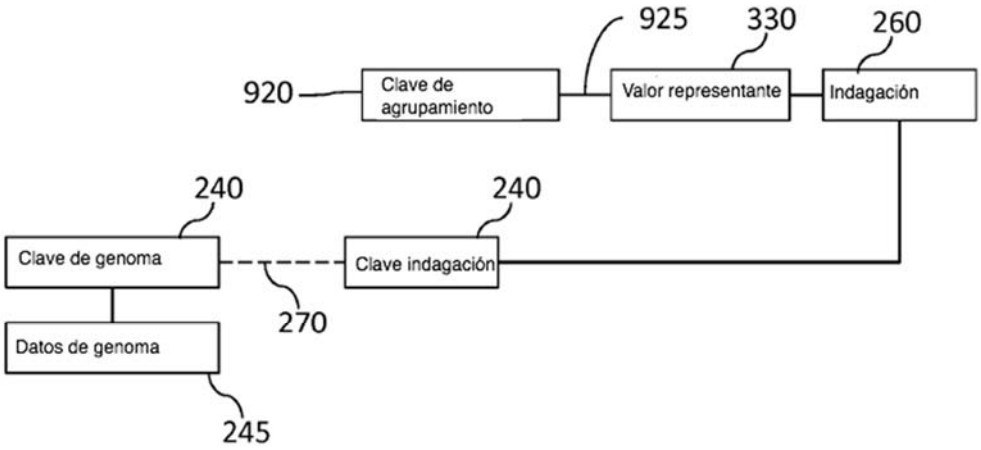

Figura 9c

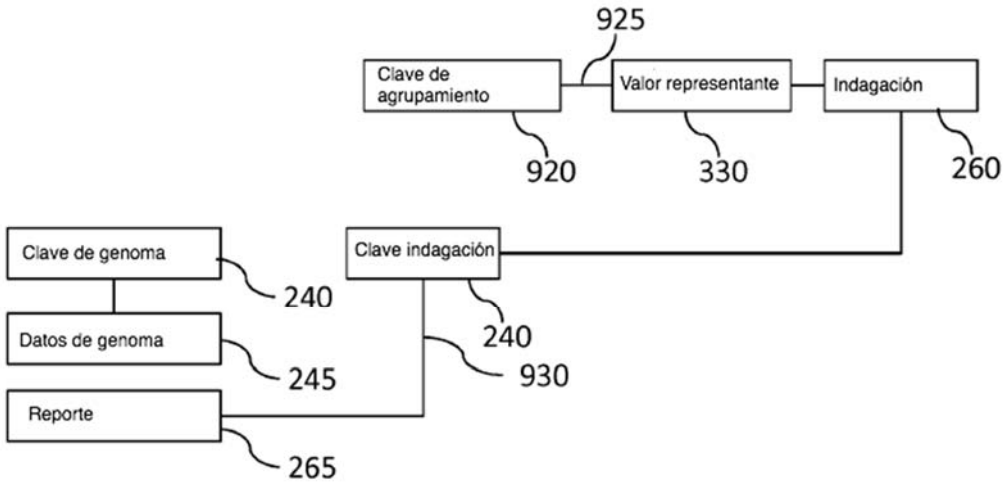

Figura 9d

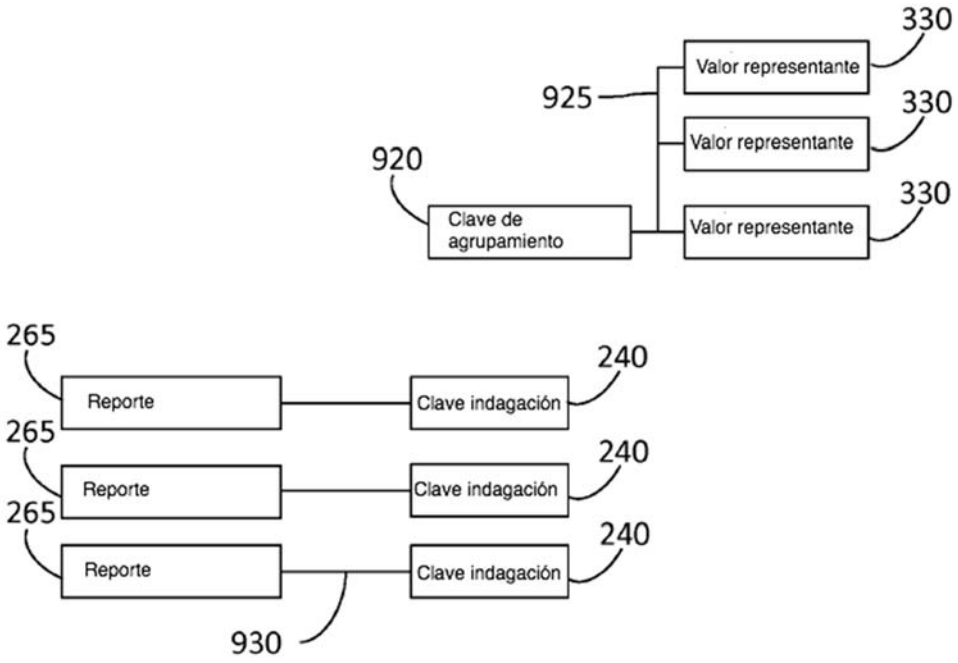

Figura 10a

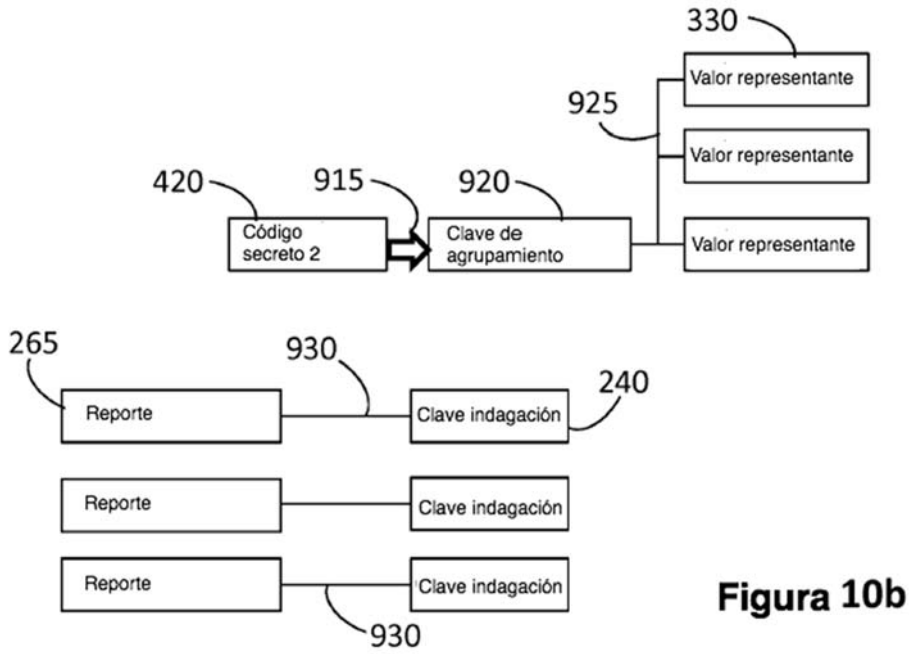

Figura 10b

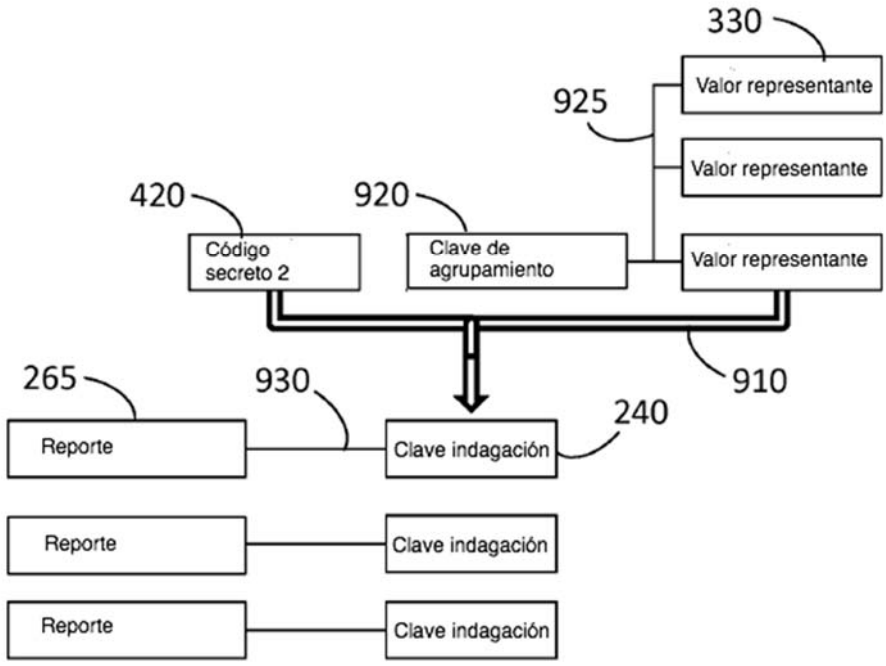

Figura 10c

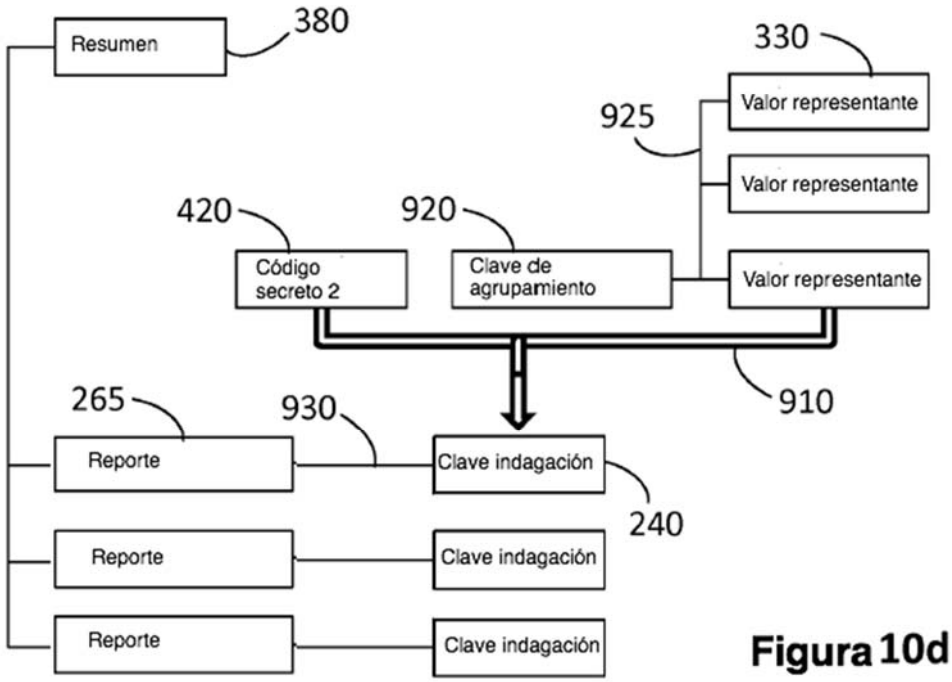

Figura 10d

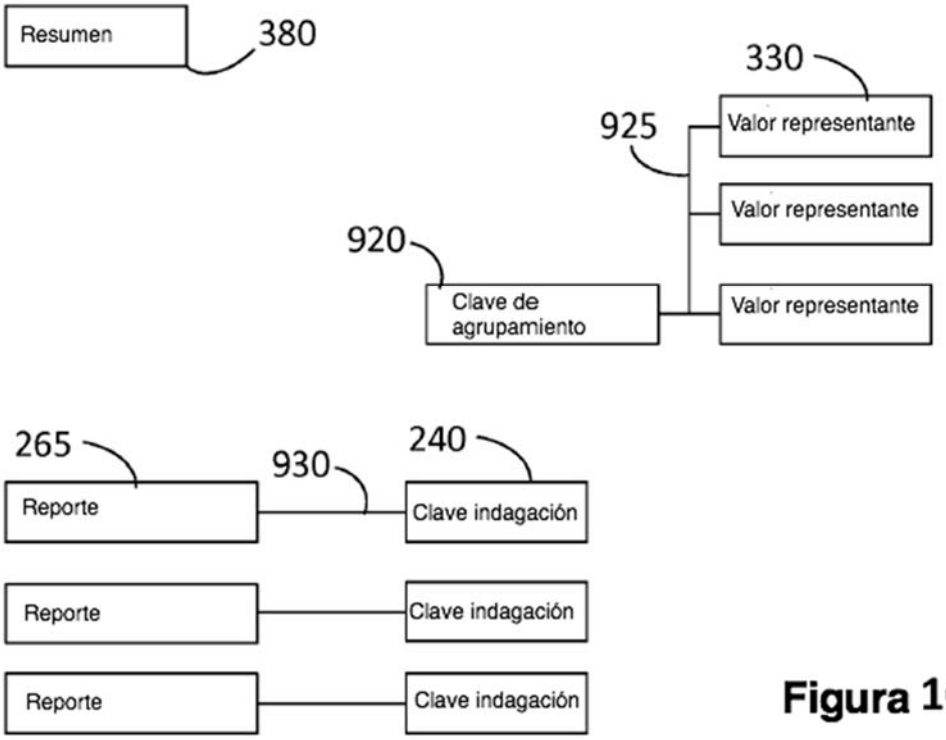

Figura 10e

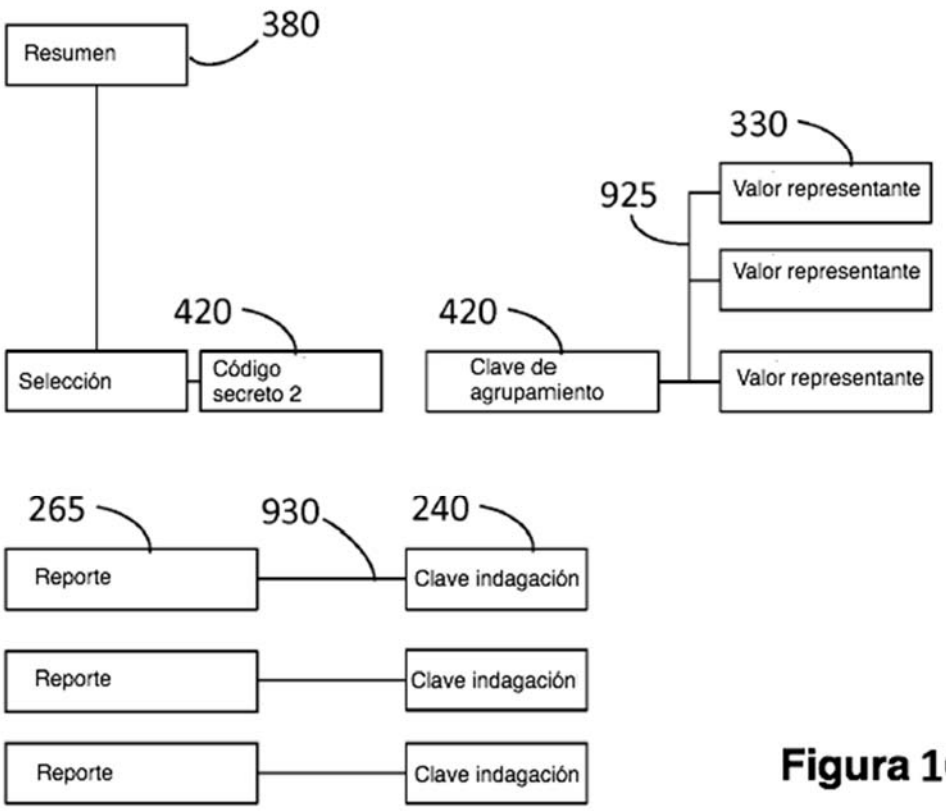

Figura 10f

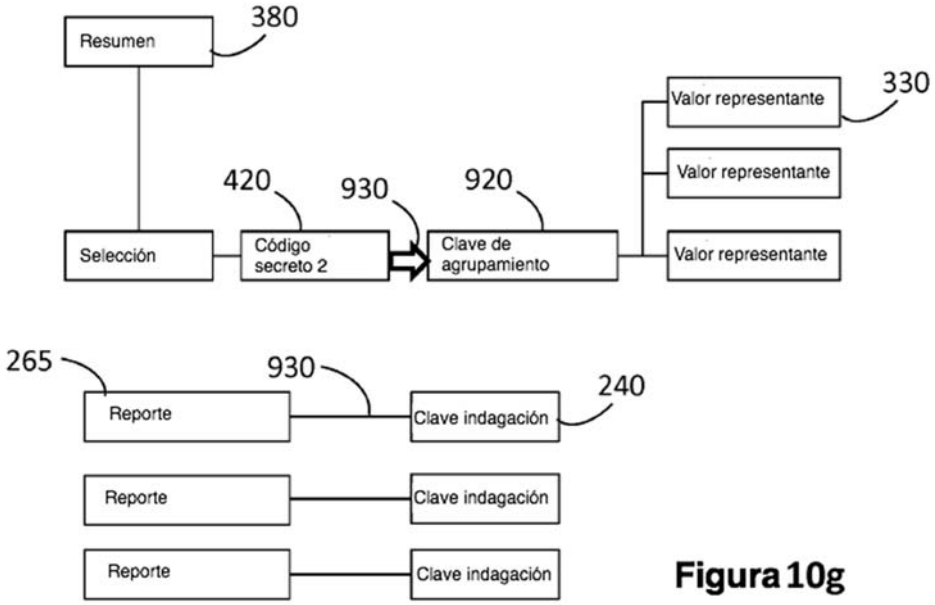

Figura 10g

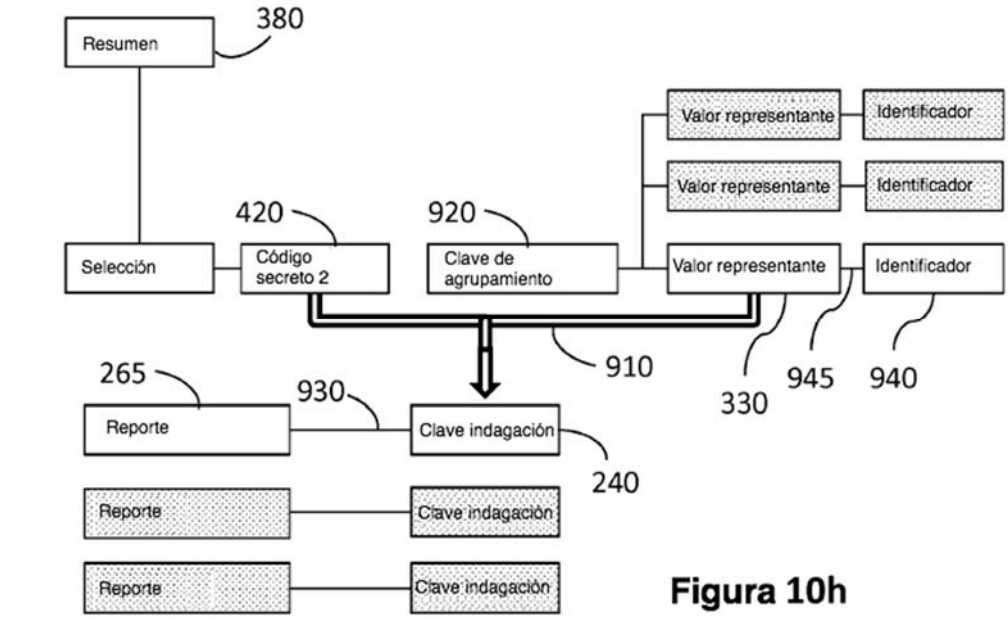

Figura 10h