(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 857 803**

(51) Int. CI.:

H04L 29/06 (2006.01)
G07F 17/32 (2006.01)

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(86) Fecha de presentación y número de la solicitud internacional: **15.03.2016 PCT/EP2016/055537**

(87) Fecha y número de publicación internacional: **29.09.2016 WO16150760**

(96) Fecha de presentación y número de la solicitud europea: **15.03.2016 E 16711199 (6)**

(97) Fecha y número de publicación de la concesión europea: **30.12.2020 EP 3275153**

(54) Título: **Transferencia de datos verificable a través de una red**

(30) Prioridad:

25.03.2015 EP 15160904

(45) Fecha de publicación y mención en BOPI de la traducción de la patente:
29.09.2021

(73) Titular/es:

IALM. DANSK VARE- OG NDUSTRILOTTERI (100.0%)
Rosbæksvej 5
2100 Copenhagen O, DK

(72) Inventor/es:

HOLST, ANDERS KRISTOFFER

(74) Agente/Representante:

ELZABURU, S.L.P

DESCRIPCIÓN

Transferencia de datos verificable a través de una red

La presente invención se refiere a métodos y sistemas para llevar a cabo una transferencia de datos verificable a través de una red. Los presentes métodos y sistemas se pueden usar en todas las ocasiones en las que un dispositivo operado por el usuario se comunica con una base de datos segura y el usuario no puede acceder temporalmente a la información relevante en el momento de la comunicación con la base de datos segura y de esta forma el usuario puede desear adquirir o comprobar la información no accedida en un momento posterior. Los métodos y sistemas se usan preferentemente cuando se llevan a cabo loterías en línea con participación del usuario, por ejemplo, billetes para rascar. La lotería tiene la característica particular de que a) todos los billetes de lotería emitidos son posibles billetes ganadores, y b) que todavía existe la posibilidad de ganar hasta que el último campo permitido del billete de rascar haya sido rascado por el usuario. En principio los métodos y el sistema se pueden usar también para otros fines, como la banca en línea, las compras, o transacciones en línea similares que pueden requerir una revisión en un momento posterior cuando la comunicación con la base de datos segura ha concluido.

Antecedentes de la invención

Las loterías en línea se derivan en su mayoría de las loterías previas en las que se usan billetes de lotería físicos. Las loterías en línea tienen la ventaja, aparte de la mayor accesibilidad por el usuario (es decir, no hay necesidad de visitar un quiosco de lotería o similar), de que es posible implementar características de seguridad adicionales en la lotería. Estas características de seguridad adicionales permitirán una mayor participación del usuario en la lotería, lo que aumentará la emoción total de la lotería y la experiencia del usuario.

Los billetes de lotería estándar para rascar, tanto los billetes virtuales en línea como los billetes físicos, normalmente incluyen una serie de campos oscurecidos que deben ser rascados por el usuario para revelar los símbolos digitales que se pueden combinar para resultar en una ganancia o una pérdida. Mientras que los símbolos digitales de los billetes de lotería de rascar físicos están oscurecidos por una capa polimérica que se puede retirar para revelar los símbolos digitales, los billetes en línea usan métodos de visualización por ordenador para ocultar y revelar los símbolos digitales. Normalmente, en caso de que un usuario revele tres símbolos digitales idénticos, el usuario ganará un premio, tal como una cantidad de dinero, de lo contrario el usuario habrá perdido el dinero pagado por el billete. En la mayoría de las loterías, sin embargo, el rascado de los campos es un mero truco, destinado a crear emoción y entretenimiento para el usuario, ya que cada billete de lotería normalmente tiene un identificador único, tal como un número de ID, que se usa para el propósito de determinar un billete de lotería ganador en el organizador de lotería. El uso de números de ID en lugar de los campos rascables reales por parte del organizador elimina la posibilidad de cometer fraude por la manipulación de los campos rascables del billete y hace más fácil al organizador de lotería la publicación de los resultados de la lotería.

De esta forma, en las loterías de rascar mencionadas anteriormente, los billetes ganadores y perdedores están predeterminados. De esta forma, en una lotería en línea, el billete de lotería completo que incluye los símbolos digitales de todos los campos rascables se puede enviar al usuario, ya que el organizador de lotería puede inmediatamente, incluso sin que el billete de lotería sea rascado, determinar si el billete es o no un billete ganador o perdedor simplemente comprobando el número de ID del billete de lotería. La presente invención, por el contrario, se refiere a un tipo diferente de lotería de rascar en línea en la que todos los billetes de lotería tienen la posibilidad de ser un billete ganador, dependiendo de las elecciones del usuario. De esta forma, no todos los campos tienen que ser rascados y dependiendo de los campos que el usuario rasque, el resultado puede ser una ganancia o una pérdida. En tal tipo de lotería el organizador no puede determinar el resultado simplemente usando solo el número de ID ya que la entrada del usuario es decisiva en el resultado. Por esta razón, el billete de lotería completo que incluye los símbolos digitales no rascados no puede ser transferido al usuario ya que permitiría a un usuario fraudulento la posibilidad de tener acceso a los símbolos digitales debajo de los campos no rascados del billete de la lotería en línea antes de rascar cualquiera de los campos y de esta forma el usuario fraudulento rascaría sólo los campos que dan el premio más alto cada vez.

Para evitar tal comportamiento fraudulento se pretende transferir al usuario, además de un número de ID del billete de lotería y el número de campos disponibles, sólo los símbolos digitales de los campos que el usuario ha indicado que se rasquen. De esta forma, el usuario puede no ver nunca el billete de lotería completo, o sólo puede ver el billete de lotería completo después de que se rasque el último campo disponible. Esto permite al organizador de la lotería estar sustancialmente a salvo de comportamientos fraudulentos por parte del usuario, sin embargo, otros comportamientos fraudulentos seguirán siendo posibles. En particular, tal comportamiento fraudulento puede ser que la base de datos segura del organizador de lotería sea pirateada o manipulada de otro modo tal que el usuario siempre perderá, o que un tercero pueda interceptar y modificar la comunicación entre la base de datos segura y el usuario, un llamado "ataque de intermediario". Es de esta forma un objeto de la presente invención proporcionar tecnologías para permitir al usuario sentirse seguro y confiado de que la lotería se lleva a cabo apropiadamente. Además, pueden existir leyes y regulaciones que requieren al organizador de la lotería que asegure que no ha tenido lugar ningún comportamiento fraudulento y la presente invención además ofrece la ventaja de satisfacer tales necesidades.

Existe una gran cantidad de técnicas anteriores en el presente campo técnico. El documento EP 722 353 B1 se refiere a un sistema de comprobación de ganancias para usar con un sistema de apuestas informatizada. El usuario puede usar el sistema para comprobar si se encuentra una configuración ganadora o no en el billete de lotería del usuario.

El documento EP 956 117 B1 se refiere a un sistema de lotería en donde los billetes instantáneos con un resultado predeterminado se pueden emitir en un ordenador de juego. El ordenador de juego no requiere una conexión en línea con el ordenador central después de la compra del billete para ver el resultado.

El documento EP 999 883 B1 se refiere a una lotería informatizada en la que se genera una animación para presentar al ganador de la lotería.

El documento EP 1 355 705 B1 se refiere a un sistema para comprar billetes de lotería a través de Internet. Un servidor aloja al menos un grupo virtual de compradores de billetes de lotería. El servidor entonces comunica los resultados de las compras de billetes de lotería a los compradores sobre la base de la información de grupo.

El documento EP 1 556 840 B1 se refiere a un sistema de telelotería que incluye un laberinto dispuesto para la distribución de los sorteos de premios.

El documento EP 2 346 005 A2 se refiere a un método para llevar a cabo una lotería en donde el participante en la lotería rellena los campos de datos del billete de lotería con los valores recibidos durante una lotería preliminar en la que el/ella ha participado, participación en la lotería preliminar que habilita a los participantes de la lotería a aumentar o disminuir el valor nominal del billete de lotería.

WO 03/042897 A1 se refiere a un método de administración de una lotería que incluye los pasos de deducir un coste de la jugada elegida del saldo de dicha cuenta de usuario, y si se verifica que la jugada elegida es una ganadora, abonar una cantidad de dinero ganadora para la jugada elegida a la cuenta de usuario.

El documento WO 03/091923 A1 se refiere a una tarjeta de lotería de marketing en una forma de un puzle de mosaico, en donde el estado ganador o perdedor de la tarjeta de lotería de marketing se verifica superponiendo la tarjeta de lotería de marketing en una mesa de confirmación de bingo proporcionada en línea o fuera de línea.

El documento US 8,109,828 B2 se refiere a un sistema para jugar un juego de azar. Un resultado parcial del juego de azar se revela a un jugador en una parte del juego fuera de línea. La parte restante del resultado se revela al jugador en una parte del juego online. Los juegos pueden ser, por ejemplo, un juego de máquinas tragaperras, un juego de bingo, un juego de ruleta.

El documento US 8.393.949 B2 se refiere a un método implementado por ordenador para llevar a cabo un juego de azar. El juego incluye un juego basado en un billete y un juego basado en ordenador. El billete incluye un código para revelar el resultado del juego basado en el billete y acceder al juego basado en ordenador.

El documento US 8,398,484 B2 se refiere a un juego de lotería en línea instantánea. El sistema comprende un servidor, que puede tener un primer generador de números aleatorios que puede generar el número de lotería en línea instantánea y un segundo generador de números aleatorios que genera una pluralidad de combinaciones de juego. El número de lotería en línea instantánea y la pluralidad de combinaciones de juego se pueden proporcionar al jugador en el momento de la compra del billete de lotería en línea instantánea.

El documento US 2004/0254019 A1 se refiere a un juego de azar en línea. El juego se basa en un mapa que tiene múltiples ramas, donde se selecciona una ruta deseada pinchando en la rama. Cada rama disponible que se selecciona resulta en un valor de premio que se incrementa, disminuye, o un token que se otorga para su uso posterior en el juego.

El documento US 2005/0098951 A1 se refiere a un método de juego de cartas. El método comprende barajar la baraja, hacer al menos una apuesta, repartir cada una de las cartas de juego en una disposición y revelar una cara de cada una de las cartas de juego, totalizar un número de puntos asociados con las cartas de juego repartidas y pagar cualquier apuesta ganadora según la apuesta y las probabilidades asociadas con la apuesta ganadora.

El documento US 2012/0323708 A1 se refiere a una interfaz de usuario para comprar y canjear billetes de lotería, en donde la instalación de lotería sólo tiene acceso de escritura a una base de datos de números de lotería ganadores, en donde el servicio de venta de lotería sólo tiene acceso de lectura a la base de datos de números de lotería ganadores, en donde los proveedores del servicio de venta de lotería solo tienen acceso de escritura a una base de datos de números de lotería comprados, en donde la instalación de lotería sólo tiene acceso de lectura a la base de datos de números de lotería comprados.

El documento US 2014/0315614 A1 se refiere a un sistema de rascar de lotería en línea. El usuario tiene un dispositivo de pantalla táctil inalámbrica para interconectar de forma interactiva con la al menos una aplicación de rascador de lotería en línea programable digital para mostrar un billete para rascar digital.

El documento WO 2009/038629 A2 se refiere a un dispositivo para registrar un nombre de dominio, que comprende una tarjeta para rascar que incluye un identificador oculto por una sustancia opaca, el identificador se adapta a un sistema para registrar nombres de dominio, estando adaptada la sustancia opaca para ser retirada al menos parcialmente de la tarjeta con el fin de exponer el identificador a un usuario.

El documento US 6.572.471 B1 se refiere a una máquina tragaperras que tiene una pantalla de visualización de vídeo controlada para mostrar una imagen de juego dividida en una matriz de elementos o zonas seleccionables de jugador. La pantalla de vídeo es preferiblemente de la variedad sensible al tacto. El jugador puede seleccionar uno de los elementos de la matriz, causando de ese modo que la imagen en el elemento cambie para revelar si un valor de premio está asociado o no con esa zona.

El documento US 8.133.104 B2 se refiere a un sistema de juego de póquer en línea que comprende una partida de póquer en vivo o grabada. El terminal de jugador muestra imágenes de la partida en vivo o grabada que se transmite para ser vista por un jugador en línea. El terminal de jugador también incluye un teclado, que habilita al jugador en línea a seleccionar uno o más jugadores para ganar, y seleccionar un valor para cada selección. Así, aunque el jugador en línea no puede tomar decisiones sobre la partida, el jugador en línea puede participar haciendo selecciones, de la misma manera que uno haría selecciones en un hipódromo. El jugador en línea puede hacer múltiples selecciones de juego que no están disponibles para el jugador sentado en la mesa.

El documento US 8.641.522 B2 se refiere a un sistema de juego en el que se asignan a los jugadores dispositivos de juego individuales que comprenden tableros de juego electrónicos. La pasarela confirma la identidad de cada jugador de modo que un jugador sólo pueda acceder a su dispositivo de juego asignado y dedicado.

El documento US 8.016.662 B1 se refiere a un sistema de juego en el que se definen uno o más parámetros para un juego y los parámetros se comunican en un archivo de parámetros a un tercero de confianza.

El documento US 2007/0082722 A1 se refiere a un juego de cartas. El juego comprende apostar, repartir al menos trece cartas de juego, retener cualquier carta de juego, reemplazar cada carta no retenida por una carta de juego repartida boca arriba, comparar las trece cartas con las combinaciones ganadoras predeterminadas para determinar si existe una combinación de cartas ganadora.

El documento US 2014/0045568 A1 se refiere a un sistema de verificación de billetes de lotería. Un primer sistema de servidores almacena un archivo de validación que tiene registros de validación para los billetes de lotería. Un segundo sistema de servidores almacena un archivo de verificación que tiene registros de verificación para los billetes de lotería proporcionados a los jugadores y se hace accesible a los jugadores antes del canje del billete de lotería, en donde un jugador introduce un código proporcionado en el billete de lotería que está vinculado al registro de verificación específico para el billete de lotería y se proporciona con el estado ganador o perdedor del billete de lotería.

El documento US 6,273,817 B1 se refiere a un billete de lotería resistente a la manipulación para evitar el pago de billetes inválidos que comprende: un cuerpo de billete, una pluralidad de campos de juego que pueden ser elegidos por un jugador de lotería, al menos un símbolo digital ganador para el billete colocado en un campo de juego, un material para rascar que cubre los campos de juego para ocultar los contenidos de los campos de juego, un código de seguridad legible impreso en cada uno de los campos de juego. Los códigos de seguridad del billete pueden ser leídos para asegurar que el número apropiado de campos de juego es revelado y el billete de lotería es válido.

El documento US 7,980,937 B2 se refiere a un sistema de billetes de lotería instantánea que tiene un archivo de validación de billetes. La seguridad del archivo de validación es proporcionada por un sistema de auditoría. Los datos de auditoría, basados en los datos de los billetes que se usan para imprimir los billetes de lotería instantánea, se pueden comparar con la formación en el archivo de validación para confirmar la integridad del archivo de validación. Los datos de auditoría pueden incluir todos o una parte de los registros que deberían estar en el archivo de validación o partes seleccionadas de datos en los registros tales como los valores de canje de billetes.

El documento WO 2009/156874 A1 se refiere a un método de control de validez en una lotería basado en el principio de que un jugador rasca campos cubiertos en un billete para descubrir información oculta como letras, números, etc. El billete comprende un número de campos rascables, mayor que el número de campos que realmente se rascan. Cuando un jugador, cuando rasca el billete, detecta una pérdida final, los campos rascables restantes también se pueden rascar para comprobar así sus posibilidades originales de ganar.

Compendio de la invención

Al menos el objeto anterior o al menos uno de los numerosos objetos adicionales que se desprenderán de la siguiente descripción de la presente invención, se obtiene según un primer aspecto de la presente invención mediante un método para llevar a cabo una transferencia verificable de datos a través de una red, el método que comprende los pasos de:

a1) proporcionar una base de datos segura, una base de datos pública, y uno o más dispositivos operados por el usuario, estando todos conectados a la red,

a2) proporcionar un servidor principal (12) para controlar dicha base de datos segura (14),

a3) generar un lote de conjuntos de datos en la base de datos segura, cada uno de los conjuntos de datos que comprende un identificador que identifica de forma única el conjunto de datos dentro del lote y una matriz indexada de símbolos digitales en donde cada símbolo digital se elige de un grupo de símbolos digitales,

a4) generar una versión encriptada del lote y una clave de desencriptado en la base de datos segura,

b) transferir la versión encriptada de la base de datos segura a la base de datos pública, generar un recibo en la base de datos pública y transferir el recibo de la base de datos pública a la base de datos segura,

c) seleccionar uno de los conjuntos de datos del lote y retirar el conjunto de datos seleccionado del lote, la selección de uno de los conjuntos de datos es hecha por el dispositivo operado por el usuario o alternativamente de forma aleatoria por la base de datos segura,

d) transferir el identificador del conjunto de datos seleccionado y un valor correspondiente al número total de símbolos digitales en la matriz indexada de símbolos digitales del conjunto de datos seleccionado desde la base de datos segura a un dispositivo operado por el usuario,

e) transferir un índice seleccionado por el usuario asociado con la matriz indexada de símbolos digitales del conjunto de datos seleccionado desde el dispositivo operado por el usuario a la base de datos segura y transferir el símbolo digital asociado con el índice seleccionado por el usuario de la matriz indexada de símbolos digitales del conjunto de datos seleccionado desde la base de datos segura al dispositivo operado por el usuario,

f) repetir el paso e) un número predeterminado de veces, en donde el número total de símbolos digitales transferidos desde la base de datos segura al dispositivo operado por el usuario es menor que el valor que corresponde al número total de símbolos digitales en la matriz indexada de símbolos digitales del conjunto de datos seleccionado,

g) repetir los pasos c)-f) hasta que se hayan eliminado todos los conjuntos de datos del lote, y

h) transferir la clave de desencriptado desde la base de datos segura a la base de datos pública, reproduciendo el lote de conjuntos de datos en la base de datos pública usando la versión encriptada y la clave de encriptado, y permitir al dispositivo operado por el usuario acceder al conjunto de datos seleccionado en la base de datos pública usando el identificador.

La red a través de la que se realiza la comunicación de datos es normalmente una red de área amplia que puede ser vulnerable en algún punto a ataques externos de personas fraudulentas. Aunque, como se ha dicho en la introducción, el presente método se puede usar en diversas circunstancias donde se requiere una transferencia de datos verificable, se usa normalmente con el propósito de llevar a cabo un juego de lotería en línea o juegos similares o actividades de juego tales como el bingo en línea, el póquer en línea u otros juegos de azar similares.

Se entiende que la base de datos segura comprende un ordenador o servidor que tiene una unidad de procesamiento, una memoria y capacidades para comunicarse de forma segura a través de la red, preferiblemente a través de un servidor separado, un cortafuegos o similar con el fin de restringir las posibilidades de una intrusión por cualquier persona fraudulenta. La base de datos pública puede ser de una construcción de hardware similar a la de la base de datos segura, sin embargo, debe ser accesible al público, o al menos los usuarios. Preferiblemente, la base de datos pública está supervisada por un notario público. Los usuarios son capaces de acceder tanto a la base de datos segura como a la base de datos pública a través de la red usando hardware electrónico que puede ser bien conocido per se. Se entiende de ese modo que el acceso se puede establecer a través de servidores web o similares con el fin de evitar ataques fraudulentos a las bases de datos seguras y públicas. El dispositivo operado por el usuario normalmente incluye una pantalla para visualizar los datos y un dispositivo de entrada para seleccionar los datos a visualizar. Se entiende que tanto la base de datos segura como la base de datos pública pueden estar ubicadas en uno o más servidores operados por un tercero.

El lote de conjuntos de datos normalmente corresponde a un número de billetes de lotería, al menos más de cero billetes de lotería, en donde cada conjunto de datos corresponde a un billete de lotería “virtual”, y en lo sucesivo se usará la expresión "conjunto de datos" para representar un billete de lotería. El identificador es normalmente un número de ID que hace que cada conjunto de datos sea identificable dentro del lote. La matriz indexada de símbolos digitales se corresponde con los campos rascables de un billete de lotería para rascar, en donde los símbolos digitales están ocultos al usuario hasta que el usuario quiera revelar el campo de datos. La matriz indexada de símbolos digitales se visualizará en la pantalla del dispositivo operado por el usuario como por ejemplo una matriz, y al menos una parte de los símbolos digitales se revelará y se visualizará para el usuario tras solicitarlo el usuario a medida que el juego de lotería avanza. Los símbolos digitales se eligen de un grupo de símbolos digitales y cada símbolo digital puede, según las reglas del juego, tener un "valor" predeterminado para determinar posteriormente el premio en dinero que puede ganar el usuario. Se entiende, además, que el sistema puede constituir un símbolo digital en blanco o vacío, que no obstante debe ser transmitido al usuario de forma muy similar a un símbolo digital que tenga un "valor".

Antes de que se active el lote, es decir, antes de que los usuarios puedan comprar y/o recibir conjuntos de datos del lote, el lote se encripta en su totalidad y se transmite a la base de datos pública sin transferir de ese modo la clave de encriptado. De esta forma los conjuntos de datos del lote no se publicarán en este momento, sino sólo la información de que el lote se ha cargado en la base de datos pública. Después de que la base de datos segura ha recibido un acuse de recibo de la carga con éxito, el lote se puede activar, es decir los usuarios podrán comprar y/o recibir conjuntos de datos del lote.

Cuando el usuario ha comprado un conjunto de datos (o alternativamente ha recibido un conjunto de datos gratuito como parte de un evento comercial, como una ganancia anterior en otra lotería o como un certificado de regalo, etc.), cuya compra se puede hacer y registrar usando una aplicación web de compra en línea estándar, el usuario recibirá un conjunto de datos del lote. El conjunto de datos será entonces eliminado del lote, ya sea separándolo físicamente o alternativamente marcándolo como usado, para prevenir que el mismo conjunto de datos pueda ser vendido a un usuario diferente. Para prevenir que el usuario intente revelar símbolos digitales de la matriz indexada de símbolos digitales sin informar a la base de datos segura y de ese modo poder defraudar la lotería, sólo se transfiere una parte del conjunto de datos al dispositivo operado por el usuario. Inicialmente, sólo se transfieren al usuario el identificador y el número total de símbolos digitales en la matriz indexada de símbolos digitales. De esta manera, el usuario puede identificar su billete de lotería y podrá conocer el número total de campos que se pueden rascar. El usuario también será informado de cuántos símbolos digitales puede revelar según las reglas del juego.

El conjunto de datos puede ser seleccionado por el usuario, por ejemplo, eligiendo un identificador en una lista de identificadores disponibles. Alternativamente, el conjunto de datos es seleccionado aleatoriamente por la base de datos segura entre los conjuntos de datos que quedan en el lote, por ejemplo, usando un generador de números aleatorios estándar. También alternativamente, se puede contemplar una combinación de lo anterior donde se combinan el generador de números aleatorios y la selección del usuario.

En el siguiente paso, el usuario revela secuencialmente un número predeterminado de campos del billete de lotería para rascar en línea visibles en la pantalla del dispositivo operado por el usuario, y en este contexto, un índice que corresponde al campo indicado por el usuario se envía a la base de datos segura y la base de datos segura responde inmediatamente enviando el símbolo digital asociado con el índice de vuelta al usuario para que el dispositivo operado por el usuario lo muestre en su pantalla. Cuando el usuario ha revelado el número predeterminado de campos, según lo prescrito por las reglas del juego y que siempre es un número menor que el número total de campos, el juego termina y dependiendo de los símbolos digitales revelados por el usuario, se puede determinar una ganancia o una pérdida y el premio, por ejemplo una cantidad monetaria o bienes, ganado por el usuario es inmediatamente evidente para el usuario consultando una tabla de premios anexa o similar.

Después de que el lote completo de conjuntos de datos se ha retirado del lote y el número determinado de campos han sido revelados por los usuarios, es decir, todos los billetes de lotería han sido vendidos y usados por los usuarios, o el lote completo puede ser retirado automáticamente después de que ha transcurrido un período de tiempo predeterminado, por ejemplo, 24 horas, desde que se creó el lote, el lote se considera terminado. Con el fin de que los usuarios y opcionalmente una autoridad de inspección de lotería confirmen que no ha tenido lugar ningún fraude, la base de datos segura transmitirá entonces la clave de desencriptado a la base de datos pública de modo que la base de datos pública pueda restaurar el lote completo de conjuntos de datos. El usuario ha almacenado el identificador del conjunto de datos y los campos elegidos por el usuario. De esta manera, el usuario y opcionalmente la autoridad de inspección de lotería pueden comprobar si la lotería se llevó a cabo correctamente o no a través de la base de datos pública.

Según una realización adicional del primer aspecto, el método comprende un paso adicional de proporcionar una base de datos web que constituye la interfaz entre el dispositivo operado por el usuario y la base de datos segura.

Con el fin de permitir que la base de datos segura se ejecute sin problemas, algunas tareas asociadas inevitablemente con el alojamiento de una lotería en línea se pueden ejecutar en uno o más servidores diferentes. Por ejemplo, un servidor web se puede usar para la interconexión con los dispositivos operados por el usuario, y un servidor principal se puede usar para permitir al organizador de la lotería establecer el número de lotes de conjuntos de datos, las propiedades de los conjuntos de datos, el grupo de símbolos digitales, el número predeterminado de campos para ser revelados por el usuario, los premios a ganar por los usuarios, el pago de los billetes de lotería y así sucesivamente.

Según una realización adicional del primer aspecto, la red es Internet.

Preferiblemente, la comunicación de red se realiza a través de Internet que es con mucho la red de comunicación internacional más ampliamente usada.

Según una realización adicional del primer aspecto, el método en el paso e), comprende además transferir el identificador y el índice seleccionado por el usuario asociado con la matriz indexada de símbolos digitales del conjunto de datos seleccionado desde el dispositivo operado por el usuario a la base de datos pública.

Con el fin de que el usuario obtenga una evidencia indiscutible de los campos seleccionados por el usuario para ser revelados, el índice seleccionado por el usuario se puede subir a la base de datos pública. El índice seleccionado

por el usuario puede entonces compararse inmediatamente con el índice recibido por la base de datos segura y en caso de coincidencia, la base de datos segura puede enviar el símbolo digital al usuario. Esto permite una comprobación totalmente automática en la base de datos pública cotejando el conjunto de datos y los índices seleccionados asignados al identificador del usuario. Se entiende que puede transcurrir un cierto período de tiempo antes de que el usuario pueda verificar el conjunto de datos en el servidor público, tal como 24 horas.

Según una realización adicional del primer aspecto, la base de datos pública es independiente y está separada físicamente de cualquiera de los usuarios y de la base de datos segura. La base de datos pública debe estar separada de la base de datos segura y ser supervisada y mantenida por un tercero que sea independiente y no tome parte en las transacciones que se realicen entre los usuarios y el propietario de la base de datos segura. Se entiende además que tanto la base de datos segura como la base de datos pública pueden estar ubicadas en uno o más servidores operados por un tercero.

Según una realización adicional del primer aspecto, el dispositivo operado por el usuario es un ordenador, teléfono inteligente o tableta que ejecuta un software de cliente tal como un cliente web, una aplicación o un programa de terminal.

El dispositivo operado por el usuario puede ser cualquier dispositivo capaz de comunicarse a través de Internet o una red similar por medio de un protocolo estándar tal como Ethernet, WiFi, Bluetooth, 3G, 4G, etc.

Según una realización adicional del primer aspecto, el valor que corresponde al número total de símbolos digitales en la matriz indexada de símbolos digitales es el mismo para todos los conjuntos de datos dentro del lote.

Con el fin de que el juego se lleve a cabo usando las mismas reglas para todos los usuarios, el número de campos rascables del billete de lotería en línea, es decir, el número total de símbolos digitales, puede ser el mismo.

Según una realización adicional del primer aspecto, cada una de las matrices indexadas de símbolos digitales es única dentro del lote. De ese modo cada matriz indexada no debe ser necesariamente única entre los lotes del juego, y de esta forma la misma matriz indexada puede aparecer en el mismo juego pero en un lote diferente.

Además, cada uno de los billetes de lotería del lote puede ser único con el fin de que el juego no sea repetitivo. Al menos el número de ID de cada uno de los billetes de lotería dentro de un lote debe ser único.

Según una realización adicional del primer aspecto, cada uno de los símbolos digitales del grupo de símbolos digitales se usa al menos dos veces en cada una de las matrices indexadas de símbolos digitales, preferiblemente tres veces, más preferiblemente cuatro veces. Además, se puede usar un símbolo "comodín" para representar cualquiera de los símbolos digitales disponibles, y dicho "comodín" sólo se puede usar una vez.

Esto permite que el juego de lotería sea más emocionante ya que el usuario podrá "coleccionar" un cierto símbolo digital durante el juego y de ese modo aumentar el nivel de emoción del juego.

Según una realización adicional del primer aspecto, el método en el paso d) comprende además transferir un identificador de usuario desde la base de datos segura al dispositivo operado por el usuario. De esta manera, el usuario puede ser identificado en la comunicación con la base de datos segura. El identificador de usuario puede ser por ejemplo un nombre de usuario encriptado que garantice que el usuario correcto se está comunicando con la base de datos segura. El identificador de usuario se envía entre el dispositivo operado por el usuario y la base de datos segura en cada momento en que ambos se comunican.

Según una realización adicional del primer aspecto, la matriz indexada de símbolos digitales comprende entre 4 y 64 símbolos digitales, preferiblemente entre 9 y 32 símbolos digitales, más preferiblemente entre 16 y 25 símbolos digitales.

Tal número de símbolos digitales como se ha descrito anteriormente permitirá un período de tiempo suficiente de entretenimiento de lotería para el usuario así como permitir una multitud de variaciones de los conjuntos de datos individuales.

Según una realización adicional del primer aspecto, cada uno de los conjuntos de datos dentro del lote está asociado con un billete de lotería para rascar virtual. Lo anterior se desprende de la descripción detallada a continuación.

Según una realización adicional del primer aspecto, el método en el paso f) comprende además determinar en la base de datos segura si los símbolos digitales de la matriz indexada de símbolos digitales del conjunto de datos seleccionados asociados con los índices seleccionados por el usuario coinciden con un conjunto de símbolos digitales ganadores predeterminados, siendo elegidos los símbolos digitales ganadores, la matriz indexada de símbolos digitales y el número predeterminado de veces preferentemente de forma que la determinación final no puede tener lugar hasta que se haya alcanzado el número predeterminado de veces.

La determinación anterior de la ganancia o la pérdida se puede realizar cuando el usuario haya revelado el número predeterminado de símbolos digitales y al mismo tiempo se puede presentar al usuario el conjunto de datos

completo como una verificación del resultado. Alternativamente, para prevenir cualquier análisis estadístico de los conjuntos de datos restantes en el lote por el usuario y/o asegurar un beneficio adecuado para el organizador, la determinación se puede hacer después de que se haya terminado el lote completo.

Según una realización adicional del primer aspecto, el número predeterminado de veces se elige de forma que el número total de símbolos digitales transferidos desde la base de datos segura al dispositivo operado por el usuario sea menor que el 50% del valor que corresponde al número total de símbolos digitales en la matriz indexada de símbolos digitales del conjunto de datos seleccionado, preferiblemente el 25%, más preferiblemente el número predeterminado está entre 2 y 5.

Tal número de símbolos digitales como se ha descrito anteriormente permitirá un período de tiempo suficiente de entretenimiento de lotería para el usuario así como permitir una multitud de variaciones de las combinaciones de símbolos digitales ganadores.

Al menos el objeto anterior o al menos uno de los numerosos objetos adicionales que se desprenderán de la siguiente descripción de la presente invención se obtiene, según un segundo aspecto de la presente invención por un sistema para llevar a cabo una transferencia verificable de datos a través de una red, el sistema que comprende una base de datos segura, y un servidor principal para controlar la base de datos segura, estando la base de datos segura conectada a una base de datos pública y a uno o más dispositivos operados por el usuario a través de la red, siendo la base de datos segura capaz de:

a1) generar un lote de conjuntos de datos, cada uno de los conjuntos de datos que comprende un identificador que identifica de forma única el conjunto de datos dentro del lote y una matriz indexada de símbolos digitales en donde cada símbolo digital se elige de un grupo de símbolos digitales,

a2) generar una versión encriptada del lote y una clave de desencriptado en la base de datos segura,

b) enviar la versión encriptada a la base de datos pública y recibir un recibo de la base de datos pública,

c) seleccionar uno de los conjuntos de datos del lote y retirar el conjunto de datos seleccionado del lote, siendo hecha la selección de uno de los conjuntos de datos por el dispositivo operado por el usuario o alternativamente de forma aleatoria por la base de datos segura,

d) enviar el identificador del conjunto de datos seleccionado y un valor que corresponde al número total de símbolos digitales en la matriz indexada de símbolos digitales del conjunto de datos seleccionado a un dispositivo operado por un usuario,

e) recibir un índice seleccionado por el usuario asociado con la matriz indexada de símbolos digitales del conjunto de datos seleccionado desde el dispositivo operado por el usuario y enviar el símbolo digital asociado con el índice seleccionado por el usuario de la matriz indexada de símbolos digitales del conjunto de datos seleccionado al dispositivo operado por el usuario,

f) repetir el paso e) un número predeterminado de veces, en donde el número total de símbolos digitales enviados al dispositivo operado por el usuario es menor que el valor que corresponde al número total de símbolos digitales en la matriz indexada de símbolos digitales del conjunto de datos seleccionado,

g) repetir los pasos c)-f) hasta que todos los conjuntos de datos del lote hayan sido retirados, y

h) enviar la clave de desencriptado desde la base de datos segura a la base de datos pública.

El sistema anterior según el segundo aspecto se puede usar para llevar a cabo el método anterior según el primer aspecto y todas las realizaciones aplicables al método anterior según el primer aspecto serán igualmente aplicables al sistema según el segundo aspecto.

Breve descripción de los dibujos

La FIG. 1 ilustra un sistema de lotería según la presente invención cuando se genera el lote de conjuntos de datos.

La FIG. 2 ilustra un sistema de lotería según la presente invención cuando se transmite una copia encriptada del lote de conjuntos de datos a la base de datos pública.

La FIG. 3 ilustra un sistema de lotería según la presente invención cuando el dispositivo operado por el usuario está haciendo un pago a la base de datos web.

La FIG. 4 ilustra un sistema de lotería según la presente invención cuando el dispositivo operado por el usuario está recibiendo un conjunto de datos de la base de datos web.

La FIG. 5 ilustra un sistema de lotería según la presente invención cuando el dispositivo operado por el usuario está enviando un índice a la base de datos segura.

La FIG. 6 ilustra un sistema de lotería según la presente invención cuando el dispositivo operado por el usuario está recibiendo un símbolo digital de la base de datos segura.

La FIG. 7 ilustra un sistema de lotería según la presente invención cuando el dispositivo operado por el usuario está enviando otro índice a la base de datos segura.

La FIG. 8 ilustra un sistema de lotería según la presente invención cuando el dispositivo operado por el usuario está recibiendo otro símbolo digital de la base de datos segura.

La FIG. 9 ilustra un sistema de lotería según la presente invención cuando el dispositivo operado por el usuario está enviando otro índice más a la base de datos segura.

La FIG. 10 ilustra un sistema de lotería según la presente invención cuando el dispositivo operado por el usuario está recibiendo otro símbolo digital más de la base de datos segura.

La FIG. 11 ilustra un sistema de lotería según la presente invención cuando la base de datos segura determina si el usuario tiene o no derecho a recibir un premio.

La FIG. 12 ilustra un sistema de lotería según la presente invención cuando la clave de encriptado se envía desde la base de datos segura a la base de datos pública.

Descripción detallada de los dibujos

La FIG. 1 es una vista esquemática de un sistema de lotería en línea 10 según la presente invención. El sistema de lotería 10 comprende un servidor principal 12 que es responsable de la tasa de generación de billetes de lotería, los tipos de billetes de lotería disponibles para la compra, los precios de los billetes de lotería y los premios disponibles.

El servidor principal 12 se comunica con una base de datos segura 14 que es responsable de llevar a cabo la lotería. A petición del servidor principal 12, la base de datos segura 14 genera un lote 16 de conjuntos de datos 18, en donde cada conjunto de datos 18 corresponde a un billete de lotería virtual. Cada conjunto de datos 18 comprende una matriz indexada de símbolos digitales 20 y un identificador 22. La matriz indexada de símbolos digitales 20 de cada conjunto de datos 18 dentro del lote 16 es única, y cada identificador 22 identifica de forma única un conjunto de datos 18 dentro del lote 16. Los símbolos digitales 20 de cada matriz indexada de símbolos digitales 20 de cada conjunto de datos 18 se eligen aleatoriamente de un grupo limitado de símbolos digitales. Los símbolos digitales pueden por ejemplo representar una letra, un número, un pictograma o similar.

El sistema de lotería 10 incluye además un servidor web 24, a través del cual el sistema de lotería 10 puede comunicarse a través de Internet con un dispositivo operado por el usuario 26 tal como un ordenador, un teléfono inteligente, una tableta, etc. La base de datos segura 14 es capaz adicionalmente de comunicarse con una base de datos pública 28 que es accesible también por el dispositivo operado por el usuario 26.

Cada juego es iniciado por el usuario, y el sistema de lotería responde a cualquier solicitud enviada por el usuario.

La FIG. 2 es una vista esquemática de un sistema de lotería en línea 10 después de que se haya generado un lote 16 de conjuntos de datos 18. En esta etapa, la base de datos segura 14 está generando una copia encriptada 30 del lote 16 de conjuntos de datos 18. La copia encriptada 30 se envía a la base de datos pública 28, sin embargo, sin enviar ninguna información de desencriptado a la base de datos pública 28. De esta forma, la copia encriptada 30 está a salvo de cualquier alteración por cualquiera de las bases de datos pública 28, la base de datos segura 14 y el dispositivo operado por el usuario 26. Cuando la base de datos pública 28 ha acusado recibo de la copia encriptada 30, los conjuntos de datos 18 del lote 16 se consideran disponibles para la compra por parte de los usuarios.

La FIG. 3 es una vista esquemática del dispositivo operado por el usuario 26 haciendo un pago al servidor web 24. El dispositivo operado por el usuario 26, que es controlado por un usuario que desea participar en la lotería, accede al servidor web 24 a través de Internet y hace un pago correspondiente al precio estipulado de un billete de lotería, por ejemplo usando una transferencia bancaria, tarjeta de crédito, tarjeta de débito, etc. La información del pago se envía al servidor principal 12. Se entiende que un pago en efectivo puede no ser necesario en todos los casos ya que al usuario se le puede permitir participar en el juego de forma gratuita como una campaña de marketing o publicidad o por cualquier otra razón que no implique un pago en efectivo.

La FIG. 4 es una vista esquemática del dispositivo operado por el usuario 26 que recibe un conjunto de datos 18' del servidor web 24. Una vez que el servidor principal 12 ha registrado el pago, la base de datos segura 14 transmitirá un conjunto de datos 18' desde el lote 16 de conjuntos de datos 18 al dispositivo operado por el usuario 26 a través del servidor web 24. El conjunto de datos 18' que se enviará al dispositivo operado por el usuario 26 es seleccionado por el usuario en el dispositivo operado por el usuario 26 seleccionando un identificador 22, o aleatoriamente por la base de datos segura 14. El conjunto de datos 18' enviado al dispositivo operado por el usuario sólo contiene el identificador 22 y un número que corresponde al número total de símbolos contenidos en la matriz indexada de símbolos digitales 20. El usuario se encuentra de esta forma con un identificador 22 y una matriz indexada de campos en blanco.

La FIG. 5 es una vista esquemática del dispositivo operado por el usuario 26 que envía un índice 32 a la base de datos segura 14 a través del servidor web 24. El índice 32 está representando uno de los campos en blanco que a su vez representa uno de los símbolos de la matriz indexada de símbolos del conjunto de datos 18' desde el servidor web 24.

La FIG. 6 es una vista esquemática del dispositivo operado por el usuario 26 que recibe un símbolo digital 20 de la base de datos segura 14 a través del servidor web 24. El símbolo digital 20 enviado desde la base de datos segura 14 al dispositivo operado por el usuario 26 es el símbolo digital de la matriz indexada de símbolos del conjunto de datos 18 que corresponde al índice 32 seleccionado por el usuario.

La FIG. 7 es una vista esquemática del dispositivo operado por el usuario 26 que envía un índice adicional 32' a la base de datos segura 14 a través del servidor web 24. El índice 32' está representando otro de los campos en blanco que a su vez representa otro de los símbolos de la matriz de símbolos del conjunto de datos 18' del servidor web 24.

La FIG. 8 es una vista esquemática del dispositivo operado por el usuario 26 que recibe un símbolo digital 20' de la base de datos segura 14 a través del servidor web 24. El símbolo digital 20' enviado desde la base de datos segura 14 al dispositivo operado por el usuario 26 es el símbolo digital de la matriz indexada de símbolos del conjunto de datos 18 que corresponde al índice 32' seleccionado por el usuario.

La FIG. 9 es una vista esquemática del dispositivo operado por el usuario 26 que envía un índice 32'' a la base de datos segura 14 a través del servidor web 24. El índice 32'' está representando otro más de los campos en blanco que a su vez representa otro más de los símbolos de la matriz indexada de símbolos del conjunto de datos 18' del servidor web 24.

La FIG. 10 es una vista esquemática del dispositivo operado por el usuario 26 que recibe un símbolo digital 20'' de la base de datos segura 14 a través del servidor web 24. El símbolo digital 20'' enviado desde la base de datos segura 14 al dispositivo operado por el usuario 26 es el símbolo digital de la matriz indexada de símbolos del conjunto de datos 18 que corresponde al índice 32'' seleccionado por el usuario.

La FIG. 11 es una vista esquemática en la que la base de datos segura 14 determina si el usuario tiene o no derecho a recibir un premio. La base de datos segura compara los símbolos seleccionados por el usuario con una tabla de premios predeterminada, y notifica al servidor principal 12 del estado ganador o perdedor del conjunto de datos usado. Opcionalmente, el conjunto de datos 18 completo puede ser transmitido al dispositivo operado por el usuario a través del servidor web 24 para permitir al usuario hacer una comparación directa. De ese modo, también se revelan al usuario los símbolos no seleccionados 20'''.

La FIG. 12 es una vista esquemática del paso final de la lotería en el que se ha usado el lote 16 completo de conjuntos de datos 18, o después de que haya transcurrido un período de tiempo predeterminado. La clave de encriptado 34 es enviada desde la base de datos segura 14 a la base de datos pública 28 de forma que el lote original 16 puede ser restablecido en la base de datos pública 28. El usuario o un inspector de lotería puede acceder posteriormente a la base de datos pública 28 para verificar la corrección de la lotería comparando el conjunto de datos 18, que incluye tanto los símbolos seleccionados por el usuario 20 20' 20'' como los símbolos no seleccionados por el usuario 20''', con el conjunto de datos 18 y los símbolos 20 20' 20'' 20''' presentados al usuario por la base de datos segura 14.

Aunque el sistema y el método anteriores se han descrito en relación a una realización específica relacionada con una lotería en línea, es decir, una lotería de tarjetas para rascar, la persona experta puede prever que se pueden hacer numerosas modificaciones del sistema y el método anteriores y que puede ser igualmente aplicable a otros, propósitos no relacionados con la lotería, tales como una tienda online, donde el conjunto de datos puede representar un tipo de bienes y los símbolos pueden representar la cantidad de bienes que el usuario está comprando y donde el usuario más tarde puede verificar la disponibilidad original de un cierto tipo de bienes en el vendedor. Alternativamente se puede usar en un sistema bancario en línea donde el conjunto de datos puede representar una cuenta de usuario y los símbolos pueden representar diferentes cantidades monetarias disponibles en la cuenta de usuario, y donde el usuario desea verificar posteriormente el estado de cuenta original en el banco.

Referencias numéricas usadas

10. Sistema de lotería

12. Servidor principal

14. Base de datos segura

16. Lote de conjuntos de datos

18. Conjunto de datos

20. Símbolo digital

22. Identificador

24. Servidor web

26. Dispositivo de control del usuario

28. Base de datos pública

30. Copia encriptada

32. Índice

34. Clave de encriptado

REIVINDICACIONES

1. Un método para llevar a cabo una transferencia verificable de datos a través de una red, dicho método que comprende los pasos de:

a1) proporcionar una base de datos segura (14), una base de datos pública (28), y uno o más dispositivos operados por el usuario (26), estando todos ellos conectados a dicha red,

a2) proporcionar un servidor principal (12) para controlar dicha base de datos segura (14),

a3) generar un lote de conjuntos de datos (16) en dicha base de datos segura (14),

cada uno de dichos conjuntos de datos (18) que comprende un identificador (22) que identifica de forma única dicho conjunto de datos (18) dentro de dicho lote y una matriz indexada de símbolos digitales (20) en donde cada símbolo digital (20) se elige de un grupo de símbolos digitales (20),

a4) generar una versión encriptada de dicho lote y una clave de desencriptado en dicha base de datos segura (14),

b) transferir dicha versión encriptada desde dicha base de datos segura (14) a dicha base de datos pública (28), generar un recibo en dicha base de datos pública (28) y transferir dicho recibo desde dicha base de datos pública (28) a dicha base de datos segura (14),

c) seleccionar uno de dichos conjuntos de datos (18) de dicho lote (16) y retirar dicho conjunto de datos (18) seleccionado de dicho lote (16), siendo hecha dicha selección de uno de dichos conjuntos de datos por dicho dispositivo operado por el usuario (26) o alternativamente de forma aleatoria por dicha base de datos segura,

d) transferir el identificador (22) de dicho conjunto de datos seleccionado y un valor que corresponde al número total de símbolos digitales (20) en dicha matriz indexada de símbolos digitales (20) de dicho conjunto de datos seleccionado desde dicha base de datos segura (14) a un dispositivo operado por el usuario (26),

e) transferir un índice seleccionado por el usuario (32) asociado con dicha matriz indexada de símbolos digitales (20) de dicho conjunto de datos seleccionado desde dicho dispositivo operado por el usuario (26) a dicha base de datos segura (14) y transferir el símbolo digital (20) asociado con dicho índice seleccionado por el usuario (32) de dicha matriz indexada de símbolos digitales (20) de dicho conjunto de datos seleccionado desde dicha base de datos segura (14) a dicho dispositivo operado por el usuario (26),

f) repetir la etapa e) un número predeterminado de veces, en donde el número total de símbolos digitales (20) transferidos desde dicha base de datos segura (14) a dicho dispositivo operado por el usuario (26) es inferior a dicho valor que corresponde al número total de símbolos digitales (20) en dicha matriz indexada de símbolos digitales de dicho conjunto de datos seleccionado (18),

g) repetir los pasos c)-f) hasta que todos los conjuntos de datos de dicho lote han sido retirados, y

h) transferir dicha clave de desencriptado desde dicha base de datos segura a dicha base de datos pública, reproducir dicho lote de conjuntos de datos en dicha base de datos pública usando dicha versión encriptada y dicha clave de encriptado (34), y permitir a dicho dispositivo operado por el usuario (26) acceder a dicho conjunto de datos seleccionado (18) en dicha base de datos pública usando dicho identificador (22).

2. El método según la reivindicación 1, en donde dicho método comprende un paso adicional a5) de proporcionar un servidor web (24) que constituye la interfaz entre dicho dispositivo operado por el usuario (26) y dicha base de datos segura (14).

3. El método según cualquiera de las reivindicaciones anteriores, en donde dicha red es Internet.

4. El método según cualquiera de las reivindicaciones anteriores, en donde dicho método en el paso e), comprende además transferir dicho identificador (22) y dicho índice seleccionado por el usuario (32) asociado con dicha matriz indexada de símbolos digitales (20) de dicho conjunto de datos seleccionado desde dicho dispositivo operado por el usuario (26) a dicha base de datos pública (28).

5. El método según cualquiera de las reivindicaciones anteriores, en donde dicha base de datos pública (28) es independiente y está separada físicamente de cualquiera de dichos usuarios (26) y de dicha base de datos segura (14).

6. El método según cualquiera de las reivindicaciones anteriores, en donde dicho dispositivo operado por el usuario (26) es un ordenador, un teléfono inteligente o una tableta que ejecuta un software de cliente tal como un cliente web, una aplicación o un programa de terminal.

7. El método según cualquiera de las reivindicaciones anteriores, en donde dicho valor que corresponde al número total de símbolos digitales (20) en la matriz indexada de símbolos digitales es el mismo para todos dichos conjuntos de datos (18) dentro de dicho lote (16).

8. El método según cualquiera de las reivindicaciones anteriores, en donde cada una de dichas matrices indexadas de símbolos digitales (20) es única dentro de dicho lote (16).

9. El método según cualquiera de las reivindicaciones anteriores, en donde cada uno de dichos símbolos digitales (20) de dicho grupo de símbolos digitales se usa al menos dos veces en cada una de dichas matrices indexadas de símbolos digitales, preferiblemente tres veces, más preferiblemente cuatro veces.

10. El método según cualquiera de las reivindicaciones anteriores, en donde dicho método en el paso d) comprende además transferir un identificador de usuario (22) desde dicha base de datos segura (14) a dicho dispositivo operado por el usuario (26).

11. El método según cualquiera de las reivindicaciones anteriores, en donde dicha matriz indexada de símbolos digitales comprende entre 4 y 64 símbolos digitales (20), preferiblemente entre 9 y 32 símbolos digitales (20), más preferiblemente entre 16 y 25 símbolos digitales (20).

12. El método según cualquiera de las reivindicaciones anteriores, en donde cada uno de dichos conjuntos de datos (18) dentro de dicho lote está asociado con un billete de lotería para rascar virtual.

13. El método según la reivindicación 12, en donde dicho método en el paso f) comprende además determinar en dicha base de datos segura (14) si los símbolos digitales (20) de dicha matriz indexada de símbolos digitales (20) de dicho conjunto de datos seleccionado (18) asociado con dichos índices seleccionados por el usuario (32) coinciden con un conjunto de símbolos digitales ganadores predeterminados (20), dichos símbolos digitales ganadores (20), dicha matriz indexada de símbolos digitales (20) y dicho número predeterminado de veces se eligen preferiblemente de forma que la determinación final no puede tener lugar hasta que se ha alcanzado dicho número predeterminado de veces.

14. El método según cualquiera de las reivindicaciones anteriores, en donde, en la etapa g) todos los conjuntos de datos restantes (18) de dicho lote (16) se retiran automáticamente después de un período de tiempo predeterminado.

15. Un sistema para llevar a cabo una transferencia de datos verificable a través de una red, dicho sistema que comprende una base de datos segura (14), y un servidor principal (12) para controlar dicha base de datos segura (14), estando dicha base de datos segura (14) conectada a una base de datos pública (28) y a uno o más dispositivos operados por el usuario (26) a través de dicha red, siendo capaz dicha base de datos segura (14) de:

a1) generar un lote de conjuntos de datos (18), cada uno de dichos conjuntos de datos (18) que comprende un identificador (22) que identifica de forma única dicho conjunto de datos (18) dentro de dicho lote (16) y una matriz indexada de símbolos digitales (20) en donde cada símbolo digital (20) se elige de un grupo de símbolos digitales (20),

a2) generar una versión encriptada de dicho lote (16) y una clave de desencriptado en dicha base de datos segura (14),

b) enviar dicha versión encriptada a dicha base de datos pública (28) y recibir un recibo de dicha base de datos pública (28),

c) seleccionar uno de dichos conjuntos de datos (18) de dicho lote (16) y retirar dicho conjunto de datos seleccionado (18) de dicho lote (16), siendo hecha dicha selección de uno de dichos conjuntos de datos (18) por dicho dispositivo operado por el usuario (26) o alternativamente de forma aleatoria por dicha base de datos segura (14),

d) enviar el identificador (22) de dicho conjunto de datos seleccionado (18) y un valor que corresponde al número total de símbolos digitales (20) en dicha matriz indexada de símbolos digitales de dicho conjunto de datos (18) seleccionado a un dispositivo operado por el usuario (26),

e) recibir un índice seleccionado por el usuario asociado con dicha matriz indexada de símbolos digitales (20) de dicho conjunto de datos seleccionado (18) de dicho dispositivo operado por el usuario (26) y enviar el símbolo digital (20) asociado con dicho índice seleccionado por el usuario (32) de dicha matriz indexada de símbolos digitales de dicho conjunto de datos seleccionado (18) a dicho dispositivo operado por el usuario (26),

f) repetir el paso e) un número predeterminado de veces, en donde el número total de símbolos digitales (20) enviado a dicho dispositivo operado por el usuario (26) es menor que dicho valor que corresponde al número total de símbolos digitales (20) en dicha matriz indexada de símbolos digitales (20) de dicho conjunto de datos seleccionado (18),

g) repetir los pasos c)-f) hasta que se hayan retirado todos los conjuntos de datos (18) de dicho lote (16), y

h) enviar dicha clave de desencriptado desde dicha base de datos segura (14) a dicha base de datos pública (28).

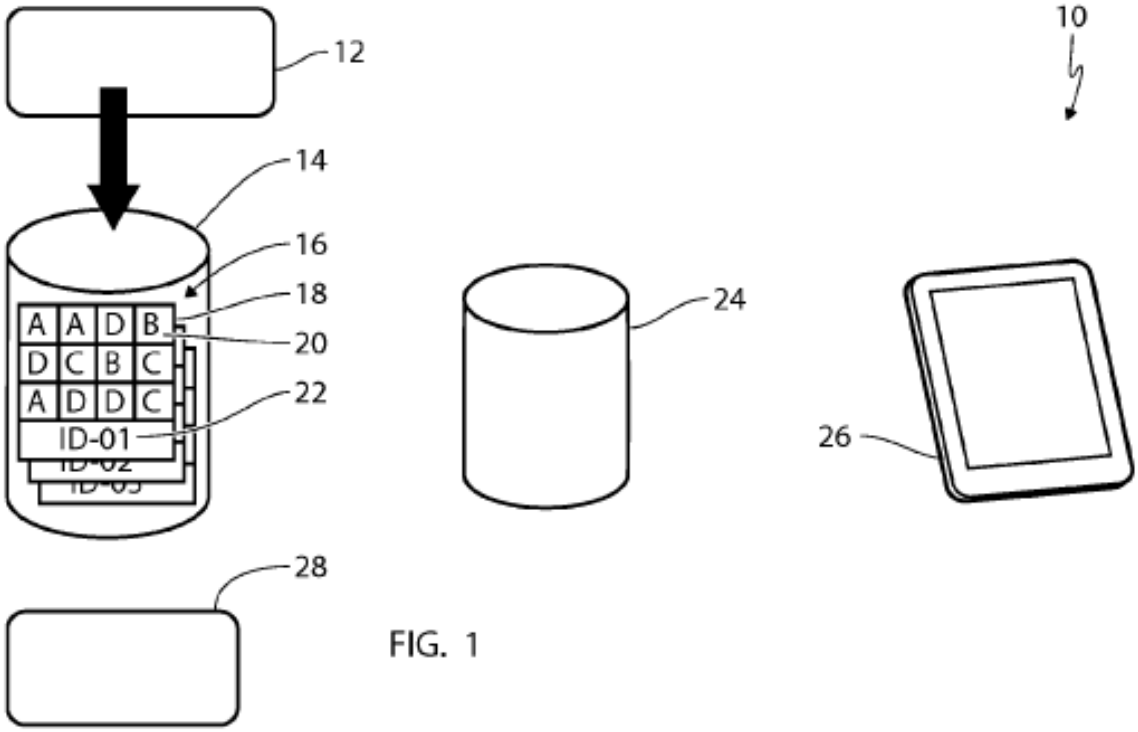
12
14
16
18
20
22
A A D B
D C B C
A D D C
ID-01
24
10
26
28

FIG. 1

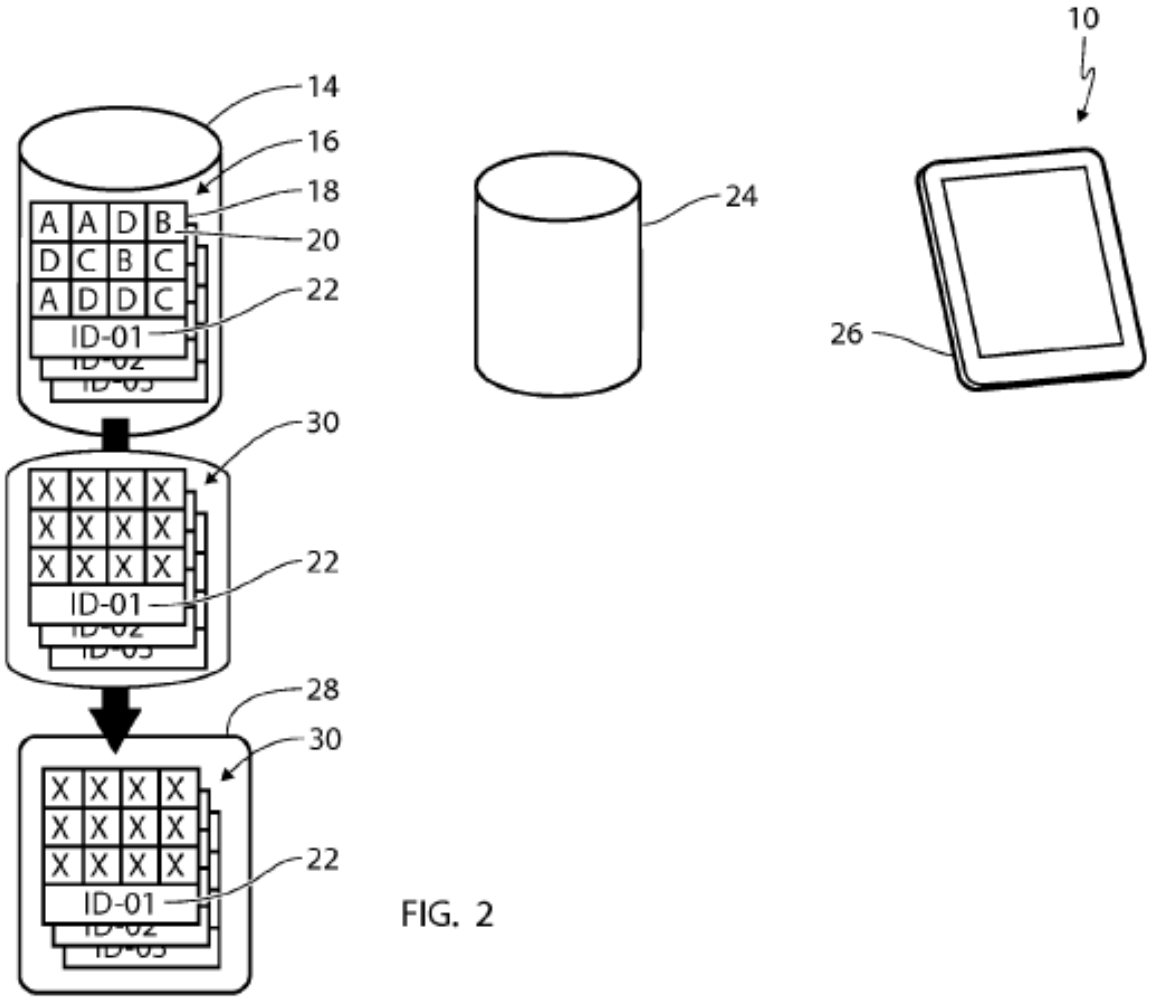
14
16
18
20
22
A A D B
D C B C
A D D C
ID-01
24
10
26
30
X X X X
X X X X
X X X X
ID-01
28
30
22

FIG. 2

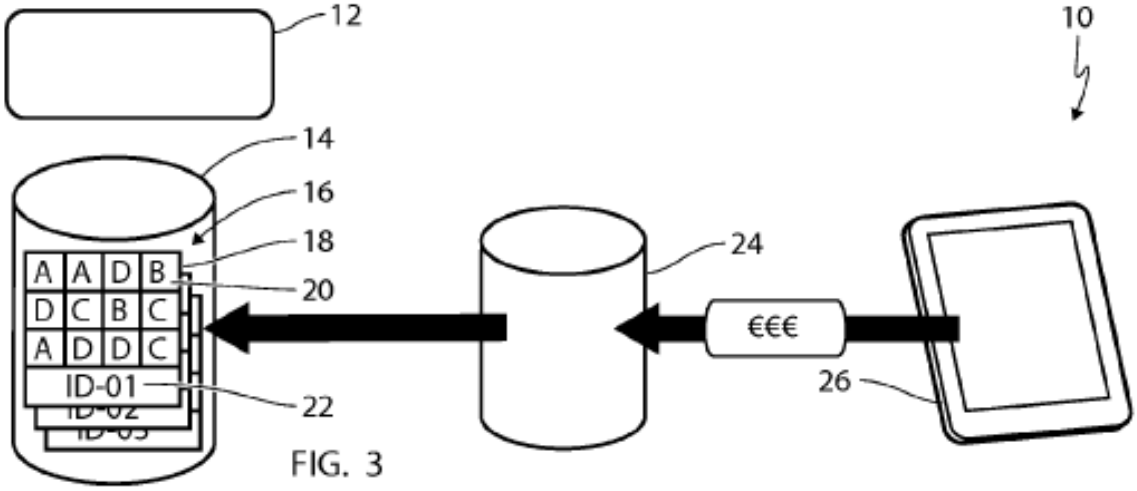

FIG. 3

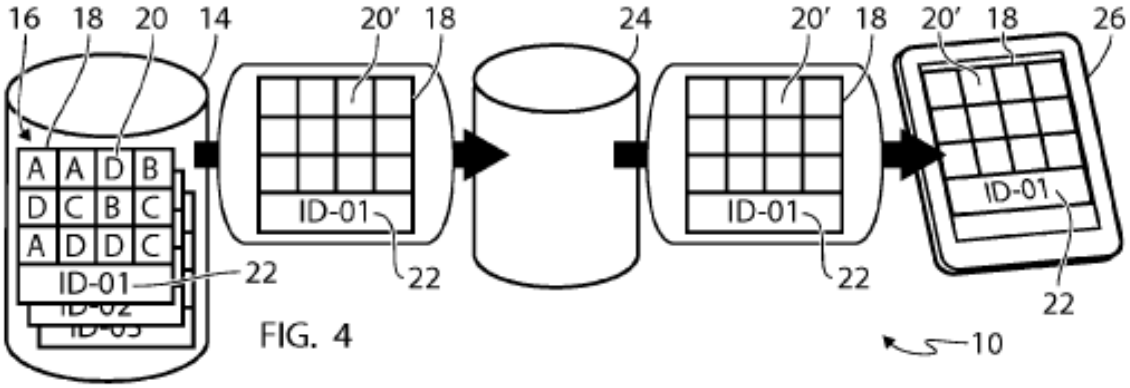

FIG. 4

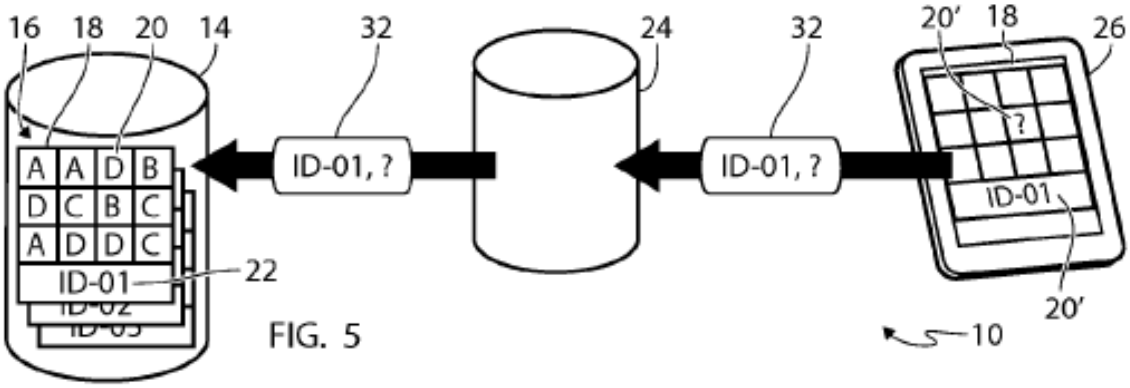

FIG. 5

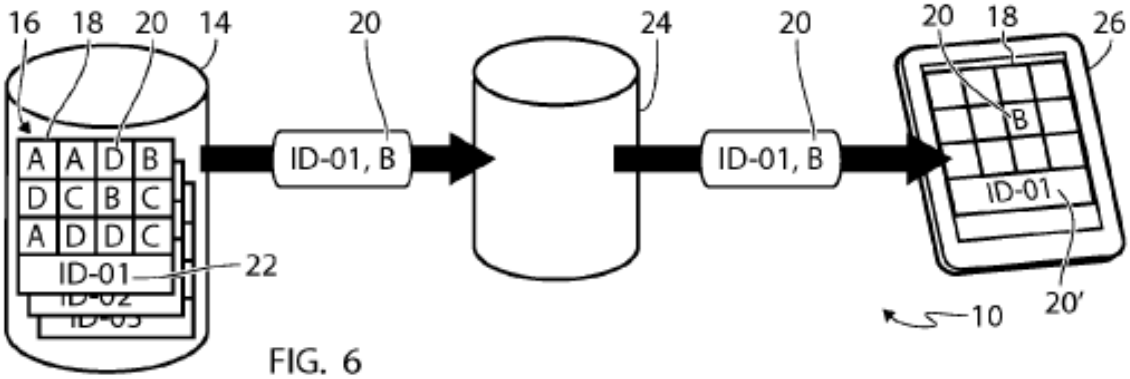

FIG. 6

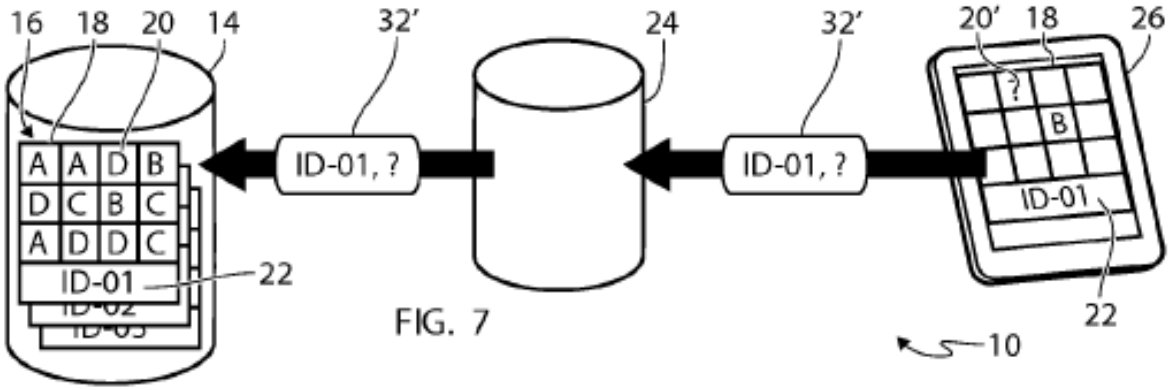

FIG. 7

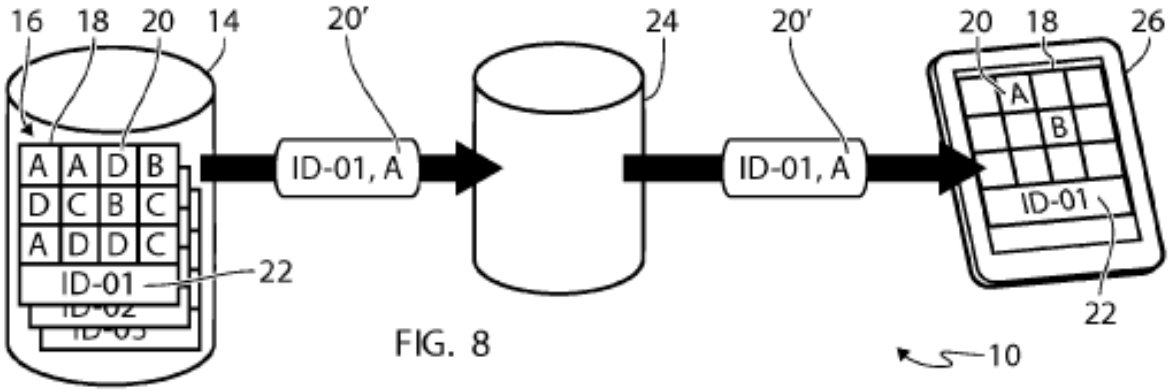

FIG. 8

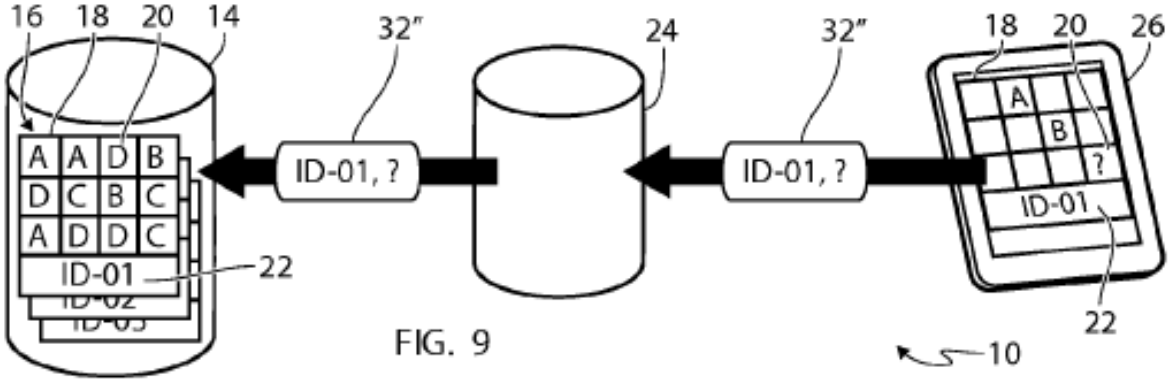

FIG. 9

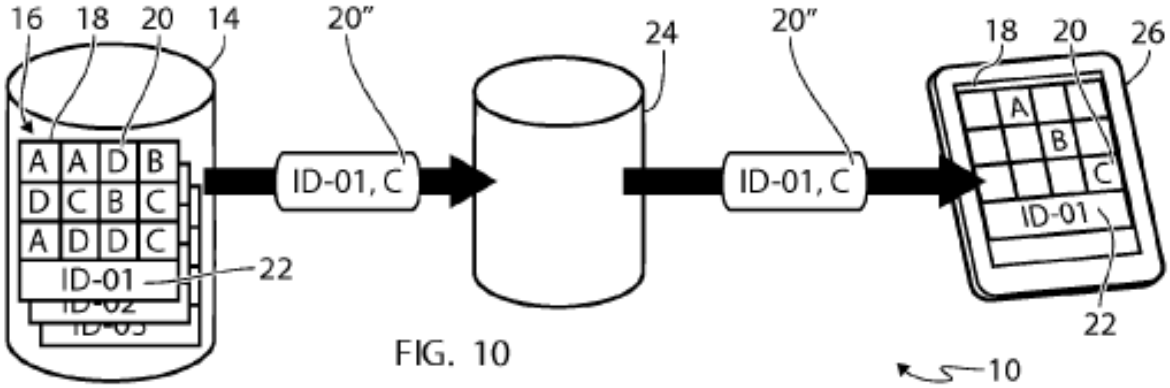

FIG. 10

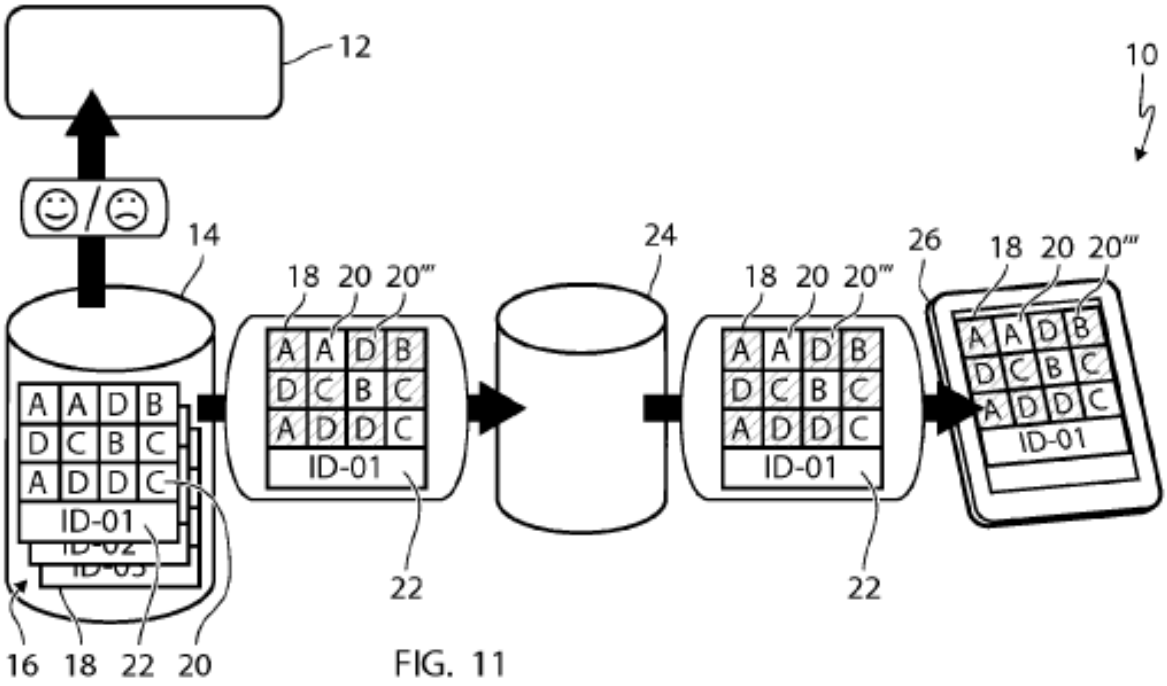
12
10
14
18 20 20''''
24
26
18 20 20''''
A A D B
D C B C
A D D C
ID-01
22
16 18 22 20

FIG. 11

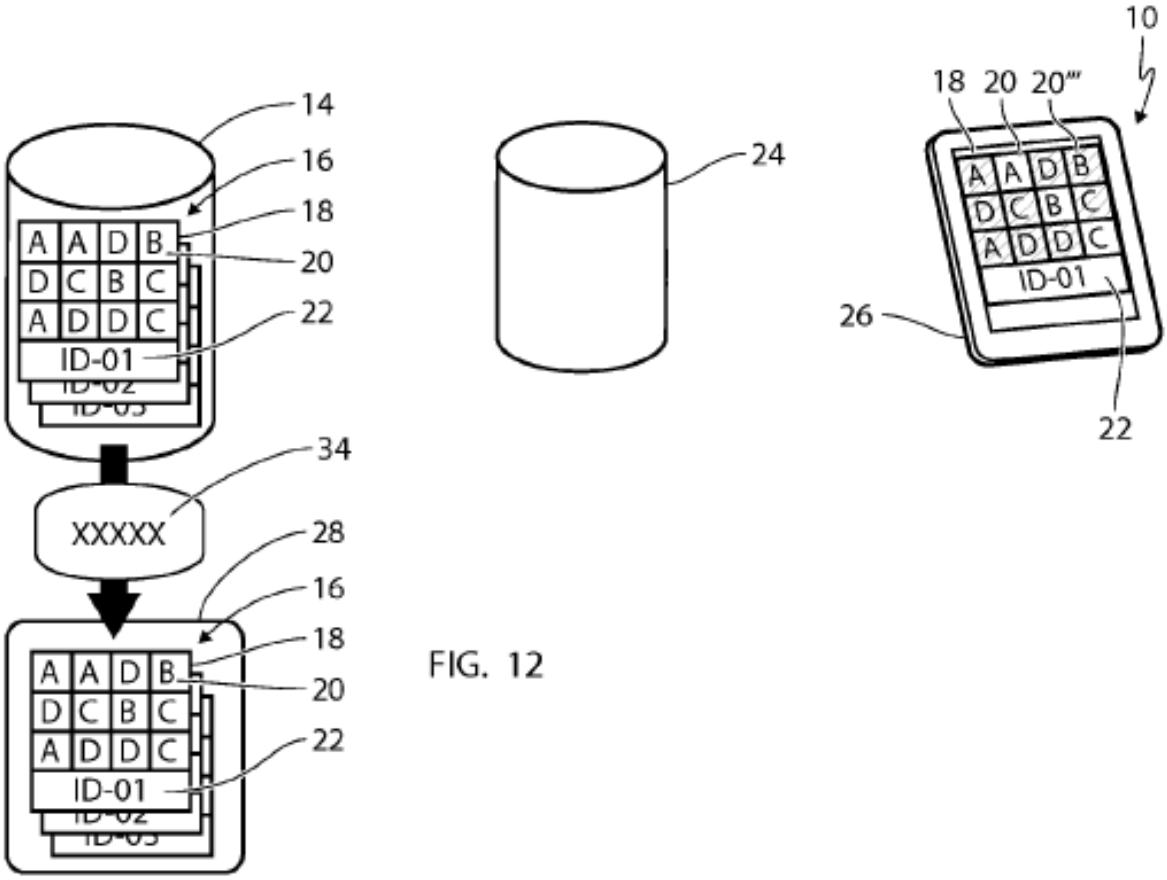
10
14
16
18
20
22
24
18 20 20''''
26
34
XXXXX
28
A A D B
D C B C
A D D C
ID-01

FIG. 12