(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 786 551**

(51) Int. CI.:

B42D 25/305 (2014.01)
G06Q 10/10 (2012.01)
B42D 25/24 (2014.01)
G06K 9/00 (2006.01)
G06T 1/00 (2006.01)
G06T 11/60 (2006.01)
H04N 1/32 (2006.01)
G06Q 50/26 (2012.01)

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(86) Fecha de presentación y número de la solicitud internacional: **20.09.2016 PCT/EP2016/072259**

(87) Fecha y número de publicación internacional: **30.03.2017 WO17050739**

(96) Fecha de presentación y número de la solicitud europea: **20.09.2016 E 16767283 (1)**

(97) Fecha y número de publicación de la concesión europea: **29.01.2020 EP 3352993**

(54) Título: **Marcado remoto de pasaporte y documento de seguridad**

(30) Prioridad:

24.09.2015 EP 15186661

(45) Fecha de publicación y mención en BOPI de la traducción de la patente:
13.10.2020

(73) Titular/es:

SICPA HOLDING SA (100.0%)
Av. de Florissant, 41
1008 Prilly, CH

(72) Inventor/es:

TALWERDI, MEHDI

(74) Agente/Representante:

TORO GORDILLO, Ignacio

DESCRIPCIÓN

Marcado remoto de pasaporte y documento de seguridad

Campo técnico

La presente invención se refiere a sistemas, entidades y métodos para marcado remoto de pasaporte y documentos de seguridad. Más específicamente, la presente invención se refiere a marcado de pasaportes como un documento de seguridad ilustrativo con correspondientes sellos, etiquetas, visado y similares.

Antecedentes

En la mayoría de países es común que se comprueben a individuos en puntos de control fronterizos cuando entran o salen del país. Diversas reglas y leyes regulan si se permite a individuos entrar o si se deniega la entrada (o salida). Un medio común es la emisión de visados que conceden al individuo acceso a un país para un periodo de tiempo limitado (por ejemplo, 30 o 90 días, etc.) o sin limitaciones. Normalmente, el individuo presenta su pasaporte en el punto de control fronterizo cuando entra al país y un funcionario comprueba el estado del visado. Si se puede permitir la entrada, se aplica un sello físico o etiqueta al pasaporte que indica la entrada (posiblemente en conjunto con una ubicación y fecha de entrada) o representa el propio visado. Tras dejar el país, se aplica una marca adicional al pasaporte, de modo que el pasaporte puede comprobarse para determinar si se permite que un individuo permanezca en algún país, si un tiempo admisible ha expirado o si se han agotado un número de entradas o reentradas admisibles a un país.

El inconveniente con sellos y etiquetas, o en general una marca, aplicada a pasaportes y otros documentos de seguridad es que la ubicación y calidad de la marca en el documento pueden variar en gran medida. Específicamente, puede aplicarse un sello (sello de caucho) con mala calidad de modo que legibilidad de la marca se ve afectada negativamente o la marca interfiere con marcas ya existentes de modo que su respectiva legibilidad se ve afectada. Adicionalmente, la posición de correspondientes marcas (por ejemplo, sello de entrada y sello de salida) puede no estar bien definida de modo que funcionarios tienen que hojear todo el pasaporte para buscar un sello de entrada y para buscar una ubicación adecuada de un sello de salida. Esto lleva tiempo y el oficial en el punto de control es capaz únicamente de procesar un número limitado de individuos por tiempo dado. Adicionalmente, los documentos de seguridad, tales como pasaportes, tienen únicamente un espacio limitado disponible para marcas, de modo que un uso ineficiente de marcas del espacio disponible puede requerir la emisión de un nuevo pasaporte antes de que pueda aplicarse un visado adicional.

Al mismo tiempo, sistemas electrónicos para emitir y autenticar documentos de seguridad, tales como pasaportes, tarjetas de identidad, visado, permisos de conducir y similares, son una práctica común en la actualidad en la mayoría de países en todo el mundo. Tales sistemas normalmente comprenden repositorios de datos centrales que se conectan por medio de protocolos cerrados y bien protegidos y enlaces de datos al equipo y terminales en el campo. El equipo de campo normalmente comprende terminales de datos, escáneres, impresoras y similares.

Normalmente, personal autorizado emplea tales sistemas en, por ejemplo, puntos de control fronterizos (inmigración), instalaciones de oficinas de la autoridad, aeropuertos y puntos de control móviles como parte de patrullas policiales comunes. Específicamente, personal autorizado puede comprobar un documento de seguridad de un propietario en el campo consultado datos personales tomados del documento de seguridad por medio de acceso a los repositorios de datos centrales especiales mencionados.

El sistema puede proporcionar un resultado de análisis a un terminal en el campo de modo que el personal puede tomar una acción apropiada, por ejemplo, dejar a la persona comprobada pasar un punto de control de seguridad, arrestar a la persona comprobada, proporcionar un certificado a la persona comprobada, aplicar un sello o marca al documento de seguridad presentado. Por ejemplo, un oficial puede consultar al sistema si un pasaporte y visado presentado es original y en consecuencia recuperar información si debería aplicarse o no una marca al pasaporte y el individuo puede pasar el punto de control y entrar en el país.

La publicación US7.314.162 divulga un método y sistema para notificar uso de documento de identidad almacenando en una base de datos y notificar a un propietario de documento de identidad casos en los que el permiso de conducir de la persona, pasaporte u otros documentos de identificación emitidos por el gobierno se presentan como una forma de identificación, facilitando de este modo notificación temprana de robo de identidad.

Además, la publicación US 7.503.488 divulga un método de evaluación del riesgo de fraude antes de emitir un permiso de conducir a un solicitante sobre la base de la relativa incidencia de fraude asociada históricamente con la combinación particular de documentos de identificación complementarios (por ejemplo, certificado de nacimiento, pasaporte, tarjeta de estudiante, etc.) presentados por el solicitante en su solicitud de permiso de conducir.

Por lo tanto, es un objeto de la presente invención proporcionar un sistema para el marcado remoto de pasaporte y documento de seguridad que hace uso eficiente de la infraestructura existente, es decir equipo en el campo,

repositorios y procesamiento de datos centrales y redes que conectan los mismos. Es específicamente un objeto de la presente invención proporcionar una solución a la aplicación problemática y no satisfactoria de marcas a pasaportes y documentos de seguridad.

El documento de patente WO 2013/067092 A1 divulga un sistema para imprimir remotamente un documento de valor tal como un cupón o un comprobante.

Sumario

Los problemas anteriormente mencionados e inconvenientes de los conceptos convencionales se resuelven mediante la materia objeto de las reivindicaciones independientes. Realizaciones preferidas adicionales se describen en las reivindicaciones dependientes.

De acuerdo con una realización de la presente invención, se proporciona un sistema de acuerdo con la reivindicación 1.

De acuerdo con una realización de la presente invención, se proporciona un método de acuerdo con la reivindicación 12.

En general, en las realizaciones la red puede ser o bien por cable o inalámbrica o una combinación de las mismas. Además, los datos pueden acompañarse por datos de voz, biométricos o análisis biológico tal como muestra de sangre, ADN o perfil de observación, etc. El módulo de analítica puede adaptarse adicionalmente para hacer coincidir un registro de datos con datos históricos en el repositorio o datos acerca de los datos (metadatos).

Breve descripción de los dibujos

Realizaciones de la presente invención, que se presentan para un mejor entendimiento los conceptos inventivos, pero que no deben verse como limitantes de la invención, se describirán ahora con referencia a las Figuras, en las que:

La Figura 1A muestra una vista esquemática de un punto de control fronterizo convencional con equipo electrónico para analizar un documento de seguridad;

La Figura 1B muestra una vista esquemática de un documento de seguridad con marcas para el ejemplo de un pasaporte con visados, sellos y etiquetas;

La Figura 2 muestra una vista esquemática de un despliegue de un sistema para el marcado remoto de pasaporte y documento de seguridad de acuerdo con una realización de la presente invención;

La Figura 3 muestra una vista esquemática de una entidad de servidor para el marcado remoto de documento de seguridad de acuerdo con una realización adicional de la presente invención;

La Figura 4 muestra una vista esquemática de una realización de aparato general de una entidad de servidor para el marcado remoto de documento de seguridad; y

La Figura 5 muestra un diagrama de flujo de un método general de realización de operación de la presente invención.

Descripción detallada

La Figura 1A muestra una vista esquemática de un punto de control fronterizo convencional con equipo electrónico para analizar un documento de seguridad. Específicamente, se muestra un punto de control 30 como parte de equipo de seguridad en el campo 1. En general, el término campo se refiere a todas las ubicaciones en las que se distribuyen correspondiente equipo y componentes. Este equipo de campo, por lo tanto, incluye componentes tales como terminales de entrada, terminales de visualización, escáneres, impresoras y similares. En el ejemplo mostrado, el punto de control 30 permite que un oficial de seguridad 19 opere, por ejemplo, un terminal de visualización 11 y un escáner 12. En un escenario habitual, un individuo presentará un documento de seguridad al oficial 19. Por consiguiente, se supone que el individuo es el propietario del documento de seguridad y que se analiza y comprueba la propiedad correcta y/o correspondiente autenticidad del documento de seguridad presentado.

Más específicamente, el individuo presentará el documento de seguridad al oficial 19, quien, a su vez puede emplear el escáner 12 para escanear el documento de seguridad o partes del mismo. Normalmente, el escáner 12 empleará técnicas de procesamiento de datos para extraer información relativa al individuo (o el propietario del documento de seguridad presentado), tal como un nombre, una fecha de nacimiento y/o un número de documento de seguridad o bien en formato biográfico o bien biométrico tal como contenido de RFID, etc. En general, cualquiera de los siguientes artículos de datos pueden representar así llamados datos adicionales relativos al individuo/propietario/titular del documento de seguridad: apellido, nombre de pila, fecha y lugar de nacimiento, país

de nacionalidad, lugar y país de residencia, número de documento, identificación de tipo de documento, fecha de emisión de documento, lugar de emisión de documento, datos biométricos del propietario, datos de imagen o datos gráficos relativos a la cara, huellas dactilares u otras características físicas del propietario de documento y similares.

Una vez que el escáner 12 ha generado tal información relativa al individuo, esta información puede reenviarse a través de un enlace seguro a alguna clase de repositorio central (no mostrado). Este repositorio es probable que sea un servidor y/o recursos de un centro de datos, red privada y/o infraestructura en la nube que se disponen y son capaces de analizar la información recibida con respecto a autenticación. Por ejemplo, el repositorio puede almacenar datos relativos a si el individuo tiene o no el derecho de entrar en un país dado. Suponiendo que el punto de control 30 mostrado se ubica antes de una puerta de salida o está conectado electrónicamente de forma segura (por cable o inalámbricamente) al aeropuerto, el repositorio puede almacenar datos que indican si el individuo ha entrado legítimamente o no al país y está abandonado ahora el país dentro de una duración de visado admisible. Por ejemplo, el repositorio puede informar al oficial 19 a través del terminal de visualización 11 que el individuo que presentó su pasaporte en el punto de control 30 ha permanecido más tiempo en el país que el permitido por su respectivo visado. El oficial 19 puede, por consiguiente, operar una barrera 13 para permitir el arresto del individuo. Naturalmente, el oficial 19 también puede operar la barrera 13 para dejar pasar al individuo si una respuesta desde el repositorio 120 indica que todo está en orden.

En general, los sistemas electrónicos convencionales para análisis de documento de seguridad normalmente emplean campo de equipo distribuido 1 y alguna clase de recursos centrales ubicados en una o más ubicaciones centrales para almacenamiento de datos y análisis. El enlace puede implementarse mediante una línea de señal especial especializada o puede ser alguna clase de comunicación segura a través de redes de comunicación existentes, tal como internet (por ejemplo, conexión VPN, túneles, etc.). Estos sistemas convencionales sufren del inconveniente de que es difícil añadir o cambiar los componentes del equipo de campo 10.

La Figura 1B muestra una vista esquemática de un documento de seguridad con marcas para el ejemplo de un pasaporte con visados, sellos y etiquetas. Específicamente, se muestra una libreta abierta de un pasaporte como un ejemplo para un documento de seguridad 40. El pasaporte 40 normalmente puede estar provisto de alguna clase de información de identificación tal como un número de pasaporte 41. El propietario (individuo) del pasaporte puede haber solicitado un visado para un país dado que se concedió y, por consiguiente, aplicó al pasaporte 40 como alguna clase de etiqueta de visado 42. Esta etiqueta de visado puede a su vez comprender correspondiente información de identificación y características de seguridad, tal como fotografías, hologramas y similares.

Como se muestra, el pasaporte 40 tiene marcas aplicadas adicionales en forma de una etiqueta 43 y sellos 44, 45 y 46. Como ya se ha mencionado, la aplicación de sellos y etiquetas puede sufrir diversos inconvenientes. En particular, una etiqueta 43 puede aplicarse de la forma de modo que cubre parte de un sello 44 aplicado anteriormente. De esta manera, la legibilidad del sello 44 puede verse afectada gravemente. De manera similar, un sello 45 puede aplicarse de una forma incorrecta de modo que únicamente aparece una parte del mismo en el pasaporte 40. Un ejemplo adicional pero no final es el sello 46 que se aplicó con mala calidad de modo que también la legibilidad se ve afectada gravemente. Este último puede ser el resultado de muy poca tinta o poca presión de aplicación empleada cuando se aplicó el sello 46 al pasaporte 40. Además, el sello 46 se aplica de nuevo de una forma de modo que la legibilidad de otras marcas de pasaporte puede verse afectada gravemente.

La Figura 2 muestra una vista esquemática de un despliegue de un sistema para el marcado remoto de pasaporte y documento de seguridad de acuerdo con una realización de la presente invención. Se proporciona un correspondiente sistema 20 en alguna clase de ubicación central 2 en el sentido de que puede estar remota de los diversos sitios en el campo 1, en el que se distribuye el equipo para escanear, imprimir, entrada/salida de datos, etc. En general, el sistema 20 proporciona marcado remoto de documento de seguridad y, por lo tanto, comprende una interfaz 21 adaptada para recibir, desde equipo en el campo 1 y a través de una red 110, datos de imagen 111 de un documento de seguridad escaneado. De esta manera, la interfaz 21 puede recibir datos gráficos desde cualquier tipo de escáner y fuente de datos en el campo 1. Los datos gráficos generalmente son de una imagen escaneada del documento de seguridad en el sentido de que el documento de seguridad se escanea para generar una imagen digital en forma de dichos datos gráficos. Por lo tanto, dichos datos gráficos pueden determinar valores de color o brillo de los píxeles a partir de los que puede compilarse la imagen.

El sistema 20 no depende o incluso requiere formatos de datos propietarios y especializados, sino que, en su lugar, es capaz de aceptar y procesar datos de imagen gráficos recibidos a través de cualquier tipo de red, tal como internet, intranet, dispositivos móviles y otros medios de interconexión de red tal como satélites. Como consecuencia, puede emplearse cualquier equipo de escaneo adecuado para escanear un documento de seguridad y generar los respectivos datos de imagen. Dicho equipo de escaneo puede incluir, por lo tanto, escáneres 12 de equipo de campo especializados 10 ya existentes y empleados por el organismo/autoridad correspondiente. Por ejemplo, el equipo de campo 10 puede ser equipo de terceros proporcionado al organismo/autoridad en conexión con un repositorio central especializado como se ha analizado y explicado en mayor detalle en conjunto con la Figura 1. Análogamente, el escaneo equipo también puede incluir componentes individuales o autónomos que no son parte de o dependientes de ningún equipo de campo 10 específico, tal como el escáner 12'. Adicionalmente, se considera cualquier otra fuente de datos para generar y reenviar la imagen o datos digitales de un documento de

seguridad escaneado a través de la red 110 a la interfaz 21 del sistema. El sistema 20 comprende además un almacenamiento de datos 22 adaptado para almacenar un registro de datos que comprende los datos de imagen recibidos y datos adicionales en relación con un propietario del documento de seguridad escaneado.

Las realizaciones de la presente invención consideran procesamiento de datos gráficos para superponer imagen de una marca en la imagen del documento de seguridad. En línea con la presente realización, el sistema 20 comprende un módulo de procesamiento de datos gráficos 23 que recupera los datos gráficos de la imagen escaneada del documento de seguridad desde el almacenamiento de datos 22. El módulo de procesamiento gráfico 23 se adapta para superponer una imagen 49 de una marca en la imagen del documento de seguridad. Además, el módulo de procesamiento de datos gráficos 23 se adapta para generar así llamados datos gráficos adicionales de la imagen escaneada del documento de seguridad con la marca. Estos datos gráficos adicionales pueden almacenarse de vuelta al almacenamiento de datos 22 o a otro almacenamiento de datos especializado. En otras palabras, se obtiene un marcado virtual del documento de seguridad. El sistema 20 comprende además un módulo de acceso 24 adaptado para proporcionar acceso a los datos gráficos adicionales que pueden almacenarse en el almacenamiento de datos 22 o en otro almacenamiento de datos especializado. Por medio del módulo de acceso 24, oficiales u otro personal autorizado pueden solicitar la inspección 112 del documento de seguridad virtual.

En general, las realizaciones de la presente invención permiten una aplicación de una marca a un documento de seguridad con una calidad controlada y bien definida siguiendo igualmente requisitos y reglas bien definidos. Específicamente, la marca puede superponerse a la imagen del documento de seguridad en una posición adecuada empleando colores adecuados y/o variaciones de contrastes. Como consecuencia, los datos gráficos adicionales proporcionan una imagen de un documento de seguridad con un marcado que se aplica a la posición correcta en una calidad dada bien definida, que, a su vez, puede resolver los problemas mencionados en conexión con mala calidad de reproducción, mala legibilidad, uso efectivo del espacio disponible, uso efectivo de tiempo de inspección y similares.

La anterior realización de la presente invención puede proporcionar adicionalmente la ventaja de que el equipo usado en el campo 1 puede ser más independiente de cualquier entidad centralizada que es responsable generalmente para analizar datos relativos a documentos de seguridad. El sistema 20 de acuerdo con esta realización puede integrarse en cualquier equipo de campo existente de modo que las funcionalidades básicas, tal como escanear, imprimir, visualizar información y operación mecánica tal como apertura de una puerta y similares, pueden emplearse para trabajar junto con el sistema 20. En particular, el uso de los datos de imagen del documento de seguridad escaneado permite el uso de prácticamente cualquier equipo de escaneo adecuado en el campo y el uso de infraestructura de red de comunicación convencional.

La Figura 3 muestra una vista esquemática de una entidad de servidor para el marcado remoto de documento de seguridad de acuerdo con una realización adicional de la presente invención. En esta realización, las funcionalidades de sistema se integran en una entidad de servidor, es decir en forma de una aplicación ejecutándose en alguna clase de recursos de procesamiento (servidor, hardware especializado, porción de un centro de datos). Similar al sistema como se describe en conjunto con la Figura 2, la entidad de servidor 20' comprende una interfaz 21 adaptada para recibir, desde equipo de campo 10 y a través de una red 110, datos de imagen 111 de un documento de seguridad escaneado. La entidad de servidor 20' comprende además un almacenamiento de datos 22 adaptado para almacenar un registro de datos que comprende dichos datos de imagen recibidos y datos adicionales en relación con un propietario del documento de seguridad escaneado. Además, la entidad de servidor 20' comprende un módulo de procesamiento de datos gráficos 23' adaptado para superponer una imagen de una marca en la imagen del documento de seguridad. El módulo de procesamiento de datos gráficos 23' se adapta adicionalmente para generar datos gráficos adicionales de la imagen escaneada del documento de seguridad con la marca. Estos datos gráficos adicionales pueden almacenarse de vuelta al almacenamiento de datos 22' o a otro almacenamiento de datos externo. Aún además, la entidad de servidor 20' comprende un módulo de acceso 24' adaptado para proporcionar acceso a los datos gráficos adicionales.

En esta realización, la interfaz 21' se implementa como un servidor de aplicación que puede proporcionar control operacional basado en la nube de propiedad privada de un lector, escáner, impresora y/o lector/escáner/impresora integrado, cualquiera que pueda instalarse en el campo. El servidor de aplicación 21' puede proporcionar otras funciones administrativas, aliviando de este modo la carga de integrar cualquier escáner/lector/impresora en sistemas electrónicos de terceros existentes. El almacenamiento de datos 22' puede implementarse como un módulo de colección de datos que se adapta para recopilar y almacenar en una base de datos todos los datos deseados. El tipo de datos que pueden almacenarse puede limitarse o restringirse por legislación nacional (por ejemplo, leyes sobre privacidad). Sin embargo los datos almacenados pueden ser en forma de registros de datos que pueden asociarse con cada uso o usos seleccionados de un documento de seguridad o artículo de valor (pasaporte).

Un registro de datos puede incluir cualquiera de los siguientes: (i) datos de imagen de escaneo del documento de seguridad por el lector/escáner o dispositivo integrado, incluyendo múltiples escaneos en múltiples longitudes de onda de radiación electromagnética, escaneos de ultrasonidos (por ejemplo, de líquidos como parte del documento de seguridad o artículos de seguridad), escaneos de rayos x, escaneos láser, etc.; (ii) identificación de documento

de seguridad tal como un número de pasaporte, imagen o imágenes u otra identificación del pasaporte y sus contenidos, incluyendo posición dentro de un pasaporte dado de cualquier sello oficial anterior (por ejemplo, visado) en ese pasaporte dado; (iii) datos biométricos y/o biográficos del titular o propietario del documento o artículo, tal como huellas dactilares, escaneos oculares, escaneos faciales, escaneos corporales, datos de sensor de calor por infrarrojos, grabaciones audiovisuales, etc.; (iv) fecha, hora y ubicación de cada uso o usos seleccionados del documento/artículo, incluyendo, por ejemplo, siempre que un pasaporte se escanea en una instalación de escaneo de pasaportes tal como un cruce fronterizo (punto de control), centro de transporte tal como en aeropuertos, muelles de barco y estaciones de tren, o en bancos, hoteles, etc., o siempre que un artículo de valor se escanea en una instalación de escaneo; (v) grabaciones de sonido, imagen o vídeo de interacciones entre titulares de documento/artículo y funcionarios (personal) en una instalación de escaneo de pasaportes u otras grabaciones relacionadas con el uso del documento/artículo, metadatos de medios asociados (por ejemplo, número de fotogramas grabados, firmas de frecuencia de voz u otros datos grabados) y métricas calculadas a partir de tales metadatos de medios (por ejemplo, que pueden cifrarse y emplearse para complementar tecnologías antimanipulación existentes); (vi) datos de vídeo que muestran personas usando el pasaporte u otro artículo de valor; (vii) información de viaje asociada con el titular o propietario del artículo de valor, por ejemplo información de llegada o destino, tal como un n.º de vuelo de aerolínea asociado con un pasaporte que se escanea en un aeropuerto u otra instalación de escaneo de pasaportes; (viii) información médica (por ejemplo, estado de salud, exposición anterior a enfermedades comunicables, informes médicos, etc., asociados con un titular de pasaporte, individuo (por ejemplo, refugiado) presente en una instalación de recopilación de datos oficial, o propietario de artículo de valor; (ix) documentación relacionada, tal como un escaneo de formularios de aduanas, escaneos de documentos de identificación secundarios, notas por funcionarios implicados, etc. (x) identidad del oficial responsable implicado en el tratamiento de un pasaporte u otro artículo de valor, tal como en el que el oficial se identifica mediante huella dactilar usando el correspondiente equipo, si está instalado, u otra biométrica por ejemplo; y (xi) contenidos de RFID en los que se instala un chip de RFID en un pasaporte, etiqueta o pegatina (por ejemplo, fijada a un objeto) o artículo de valor y se escanea en la instalación de escaneo (de pasaportes). La base de datos también puede almacenar información relacionada con visado, entrada nacional, salida nacional, formulario de aduanas, sellos de pasaporte u otros sellos oficiales para uso en controlar centralmente (es decir, remotamente) un escáner, lector, impresora y/o dispositivo integrado, cualquiera que pueda estar instalado.

El servidor 20' puede comprender opcionalmente un módulo de analítica 23A adaptado para analizar los registros de datos almacenados en el almacenamiento de datos 22 y para generar un correspondiente resultado de análisis. Por ejemplo, los datos de imagen recibidos 111 se analizan para características de identidad o seguridad, ya que tales características son elementos comunes de documentos de seguridad modernos. Específicamente, el módulo de analítica 23A puede mirar tales artículos de identidad o seguridad en conexión con los datos adicionales que se almacenan con el correspondiente registro de datos. Por ejemplo, el artículo de identidad puede conducir a la identificación de un individuo específico que es titular de un visado. Los datos adicionales pueden indicar a continuación, siguiendo este ejemplo, una región admisible donde o periodo admisible en el que puede residir el individuo. Si el módulo de analítica 23 encuentra una inconsistencia, puede lanzarse un correspondiente indicador hacia el módulo de acceso 24'. A su vez, el módulo de acceso 24' puede generar y lanzar una notificación basándose en el resultado de análisis tomado en el módulo de analítica 23A. Por medio de la notificación, puede notificarse a un oficial en el campo 1 el resultado de análisis tomado remotamente en la entidad de servidor 20'.

El módulo de analítica 23A puede configurarse específicamente para analizar los datos almacenados en la base de datos para determinar, en tiempo real, uso potencialmente irregular de un pasaporte u otro artículo de valor, tal como dónde se está intentando una entrada en o salida de un país por un titular de pasaporte sin una correspondiente salida o entrada anterior, o dónde un titular de artículo de valor está mostrando patrones de comportamiento destacables tal como nerviosismo. En general, tal análisis puede denominarse como comprobaciones plausibles y/o comprobar cualquier información entrante que se asocia a un evento (por ejemplo, intento de cruce fronterizo) con la conformidad de una o más reglas predeterminadas. Por ejemplo, una regla puede definir que un individuo dado necesita haber entrado en un país y, por consiguiente, haberse registrado, antes de que se observe un intento de abandonar el país. En una realización, el módulo de analítica 23A se adapta para hacer una determinación de si una marca se superpone o no por el módulo de procesamiento gráfico 23'. Además, el módulo de analítica 23A puede adaptarse para hacer una determinación de una ubicación dentro del documento de seguridad de que la marca imagen está superpuesta.

Adicionalmente, el módulo de analítica 23A también puede supervisar bases de datos externas 220, por ejemplo de INTERPOL, Europol, bases de datos nacionales de registros criminales y otras bases de datos para identificar individuos de interés que están intentado usar un pasaporte en una instalación de escaneo de pasaportes u otro artículo de valor en una instalación de escaneo. El módulo de analítica 23' puede supervisar adicionalmente restricciones de duración de estancia para emitir una alerta si un titular de pasaporte tiene una "permanencia demasiado larga" (por ejemplo, no ha salido de un país en la fecha de expiración de su visado) o tiene una "permanencia demasiado corta" (por ejemplo, no ha estado una cantidad de tiempo suficiente en un país para cualificar para un estado de inmigración especificable).

Además del módulo de acceso 24', puede implementarse un módulo de alerta 24A como un módulo de alerta especializado que se dispone para alertar al oficial responsable u otro funcionario cuando el documento/artículo (por

ejemplo, pasaporte u otro artículo de valor) escaneado por el oficial se ha indicado por el módulo de analítica 23A como asociado con uso irregular o de otra manera problemático. También pueden generarse alertas cuando se detecta manipulación u otro daño físico a la entidad de servidor 20' o un módulo del mismo. Para este propósito puede proporcionarse un sensor 25 (por ejemplo, temperatura, presión, vibración, ubicación, etc.) que se configura para detectar manipulación. Pueden proporcionarse alertas o, más en general, notificación a través de un módulo de comunicaciones seguras (descrito a continuación), y/o por correo electrónico, mensaje de texto y/o voz (por ejemplo, a un teléfono móvil), etc. al oficial responsable u otro funcionario. Pueden proporcionarse alertas a cualquier agencia oficial en todo el mundo, según permita la ley, para los propósitos de seguridad proactiva.

Puede proporcionarse un módulo de cortafuegos 26 que se adapta para proteger la entidad de servidor 20' de ataques basados en internet externos. El módulo de cortafuegos también puede comprender los sensores 25 anteriormente mencionados que son adecuados para supervisar manipulación física, intrusión u otro daño a los componentes de hardware de fin especial. De esta manera, puede denominarse el módulo 26 como un módulo de cortafuegos o antimanipulación.

Puede proporcionarse un módulo de comunicaciones seguras 27 para cifrado de comunicaciones entre la entidad de servidor 20' y sistemas electrónicos de gobiernos nacionales participantes, agencias de los mismos, empresas comerciales u otros clientes, es decir, el equipo de campo, que usan técnicas de cifrado consistentes con preferencias de cliente y requisitos legales. El módulo de comunicaciones seguras 27 puede facilitar, por lo tanto, comunicaciones entre la entidad de servidor 20' y los ordenadores de cliente, incluyendo escáneres, lectores, impresoras y/o dispositivos integrados, en, por ejemplo, instalaciones de escaneo de pasaportes. El módulo de comunicaciones seguras 27 puede ser operable para comunicar con ordenadores de cliente dentro de cada país a través de una VPN (Red Privada Virtual) específica de país. En algunas realizaciones, puede emplearse una VPN separada para cada instalación de escaneo (de pasaportes). Comunicaciones específicas de país facilitan la transferencia de información entre países (dentro de los límites de las leyes de ambos países) a través de la entidad de servidor, a pesar de la incompatibilidad entre respectivos sistemas electrónicos relacionados con pasaportes de diferentes países.

Más en general, el módulo de comunicaciones seguras 27 puede adaptarse para facilitar la transferencia de información entre clientes abonados a pesar de las incompatibilidades entre sus respectivos sistemas recibiendo datos desde un primer cliente abonado de acuerdo con un primer protocolo de comunicación y, a continuación, transmitir datos desde la entidad de servidor a un segundo cliente abonado de acuerdo con un segundo protocolo de comunicación en donde el primer y segundo protocolos de comunicación no son necesariamente compatibles entre sí. Cualquier número de módulos de la entidad de servidor 20' puede integrarse en una "unidad de caja negra" personalizada, y cualquier módulo dado puede comercializarse como una unidad autónoma adecuada para integrarse con sistemas electrónicos de terceros existentes.

La Figura 4 muestra una vista esquemática de una realización de aparato general de una entidad de servidor para análisis de documento de seguridad. En general, la entidad de servidor 20 puede ser una entidad que proporciona recursos de procesamiento 211 (por ejemplo, unidad de procesamiento, colección de unidades de procesamiento, CPU, porción de un centro de datos/procesamiento, etc.), recursos de memoria 212 (dispositivo de memoria, base de datos, porción de un centro de datos) y medios de comunicación 213. Por medio de estos últimos, la entidad 20 puede comunicarse con la red de comunicación 110. Los recursos de memoria 212 pueden almacenar código que ordena a los recursos de procesamiento 211 durante operación que implementen cualquier realización de la presente invención. Específicamente, los recursos de memoria 212 pueden almacenar código que ordena a los recursos de procesamiento 211 durante operación que implementen una interfaz para recibir, a través de la red 110, datos de imagen de un documento de seguridad escaneado. Además, puede implementarse un almacenamiento de datos para adaptarse para almacenar el registro de datos que comprende los datos de imagen recibidos y datos adicionales en relación con un propietario del documento de seguridad escaneado.

De acuerdo con la presente realización, los recursos de memoria 212 almacenan código que ordena a los recursos de procesamiento 211 durante operación que implementen un módulo de procesamiento de datos gráficos adaptado para superponer una imagen de una marca en la imagen del documento de seguridad y adaptado para generar datos gráficos adicionales de la imagen escaneada del documento de seguridad con la marca, y un módulo de acceso adaptado para proporcionar acceso a dichos datos gráficos adicionales.

La Figura 5 muestra un diagrama de flujo de un método general de realización de operación de la presente invención. Esta realización de método se describe en el contexto de un escenario ilustrativo relacionado con control y autenticación de pasaportes. Este escenario considera una primera etapa S51 (ESCANEAR DOCUMENTO DE SEGURIDAD) de escaneo de un documento de seguridad (o artículo de valor) para generar respectivos datos de imagen. Por lo tanto, incluso en países en los que no está en uso ningún escáner/lector/impresora particular, se escanean pasaportes, sin embargo, por correspondiente equipo de campo en entradas y/o salidas en y del país usando esas instalaciones (equipo) de escaneo de pasaportes existentes del país. El sistema, a continuación, puede comunicarse, tal como a través de una VPN específica de país y mediante comunicaciones cifradas seguras, con las instalaciones de escaneo de pasaportes existentes para recopilar y almacenar información asociada con cada uso de un pasaporte. Más específicamente, en una etapa S52 (RECIBIR DATOS DE IMAGEN) el servidor o sistema

para el marcado remoto de documento de seguridad recibe los datos de imagen a través de una red.

En una etapa S53 (SUPERPONER MARCA), el sistema realiza procesamiento de datos gráficos para superponer una imagen de una marca en la imagen del documento de seguridad y adaptado para generar datos gráficos adicionales de la imagen escaneada del documento de seguridad con la marca. En una etapa S54 (PROPORCIONAR ACCESO), se proporciona acceso a los datos gráficos adicionales generados.

Un método realización puede incluir adicionalmente una etapa de análisis de los datos de imagen recibidos para hacer una determinación de si, y posiblemente dónde, una marca tiene que superponerse o no en la imagen del documento de seguridad escaneado. Específicamente, los mecanismos ya mencionados (plausibilidad, conformidad con reglas y similares) pueden emplearse para encontrar cualquier posible irregularidad. Si no se encuentra ninguna irregularidad o el uso de documento de seguridad presentado (por ejemplo, pasaporte) no es objetable de otra manera, puede generarse una marca como sello oficial "virtual" (es decir, almacenado digitalmente), que puede ser un sello de entrada y/o salida por ejemplo, que se almacena en el módulo de base de datos de tal forma que es accesible para el oficial responsable y posteriormente para funcionarios en otras instalaciones de escaneo de pasaportes dentro de los límites permitidos por las leyes de cada par de países (es decir, el país donde se recopilaron los datos y el país donde se están accediendo). En algunas realizaciones, el sistema puede informar en tiempo real al oficial responsable u otro funcionario que ha escaneado un pasaporte dónde se ubican sellos oficiales anteriores (por ejemplo, visado) en el pasaporte. Por ejemplo, cuando un titular de pasaporte está saliendo de un país, realizaciones de la presente invención pueden informar al oficial responsable del número de página en la que se ubica en correspondiente sello de entrada anterior.

Aunque se han descrito realizaciones detalladas, estas únicamente sirven para proporcionar un mejor entendimiento de la invención definida por las reivindicaciones independientes, y no deben verse como limitantes.

REIVINDICACIONES

1. Un sistema (29) para marcar remotamente un documento de seguridad, tal como un pasaporte (40), con un correspondiente sello, etiqueta o visado virtual, que comprende:

- una interfaz (21) adaptada para recibir, desde equipo de campo y a través de una red, datos gráficos de una imagen escaneada de un documento de seguridad;
- un almacenamiento de datos (22) adaptado para almacenar un registro de datos que comprende dichos datos de imagen recibidos y datos adicionales en relación con un propietario del documento de seguridad escaneado;
- un módulo de procesamiento de datos gráficos (23) adaptado para superponer una imagen de una marca en la imagen del documento de seguridad y adaptado para generar datos gráficos adicionales de la imagen escaneada del documento de seguridad con la marca;
- un módulo de acceso (24) adaptado para proporcionar acceso a dichos datos gráficos adicionales.

2. El sistema de acuerdo con la reivindicación 1, comprendiendo adicionalmente un módulo de analítica adaptado para analizar los datos gráficos recibidos y para generar un resultado de análisis.

3. El sistema de acuerdo con la reivindicación 2, en donde el módulo de analítica se adapta adicionalmente para hacer una determinación de si el módulo de procesamiento de datos gráficos tiene que superponer o no la marca.

4. El sistema de acuerdo con la reivindicación 2 o 3, en donde el módulo de analítica se adapta adicionalmente para hacer una determinación de dónde se superpone la marca por el módulo de procesamiento de datos gráficos.

5. El sistema de acuerdo con una cualquiera de las reivindicaciones 1 a 4, comprendiendo adicionalmente un sensor adaptado para detectar manipulación con el sistema.

6. El sistema de acuerdo con la reivindicación 5, en donde dicho sensor es uno cualquiera de un sensor de temperatura, un sensor de presión, un sensor de vibración y/o un sensor de ubicación.

7. El sistema de acuerdo con una cualquiera de las reivindicaciones 1 a 6, comprendiendo adicionalmente un módulo de cortafuegos adaptado para proteger el sistema de ataques de red y/o ataques físicos al hardware del sistema.

8. El sistema de acuerdo con una cualquiera de las reivindicaciones 1 a 7, comprendiendo adicionalmente un módulo de comunicación segura adaptado para proporcionar comunicación segura de dichos datos de imagen y/o una notificación.

9. El sistema de acuerdo con una cualquiera de las reivindicaciones 1 a 8, adaptándose para comunicarse con una base de datos externa.

10. El sistema de acuerdo con una cualquiera de las reivindicaciones 1 a 9, en donde el sistema está remoto del equipo que realiza escaneo del documento de seguridad para generar dichos datos de imagen.

11. El sistema de acuerdo con la reivindicación 10, en donde se proporciona acceso a dichos datos gráficos adicionales hacia una ubicación en la que se realizó el escaneo del documento de seguridad.

12. Un método para marcar remotamente un documento de seguridad, tal como un pasaporte (40), con un correspondiente sello, etiqueta o visado virtual, que comprende:

- una etapa (S52) de recepción, desde equipo de campo y a través de una red, de datos gráficos de una imagen escaneada de un documento de seguridad;
- una etapa de almacenamiento de un registro de datos que comprende dichos datos de imagen recibidos y datos adicionales en relación con un propietario del documento de seguridad escaneado;
- una etapa (S53) de superposición de una imagen de una marca en la imagen del documento de seguridad y de generación de datos gráficos adicionales de la imagen escaneada del documento de seguridad con la marca;
- una etapa (S54) de provisión de acceso a dichos datos gráficos adicionales.

13. El método de acuerdo con la reivindicación 12, comprendiendo adicionalmente una etapa de escaneo de dicho documento de seguridad por equipo de campo y generación de datos de imagen del documento de seguridad escaneado y una etapa de transmisión de los datos de imagen a través de una red a un sistema para análisis remoto de un documento de seguridad.

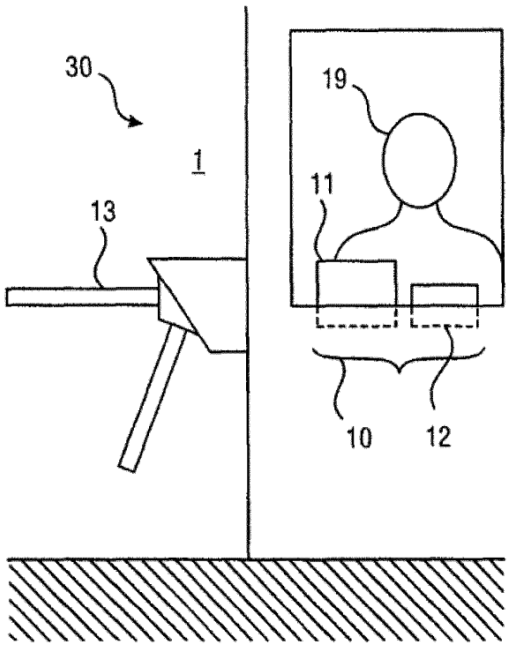

Fig. 1A

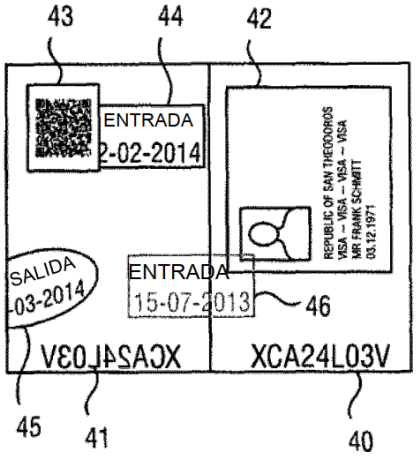

Fig. 1B

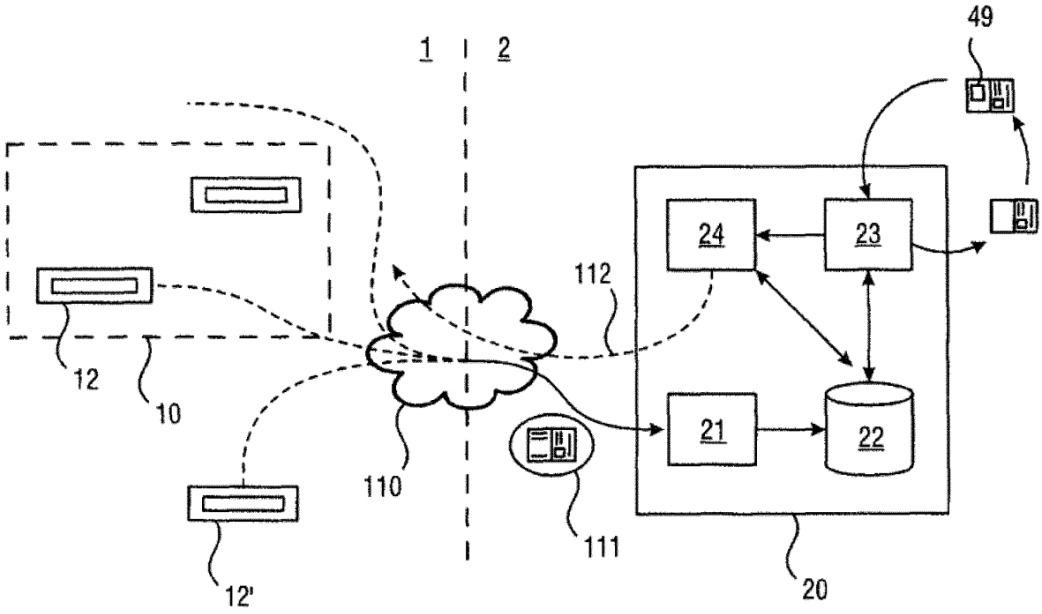

Fig. 2

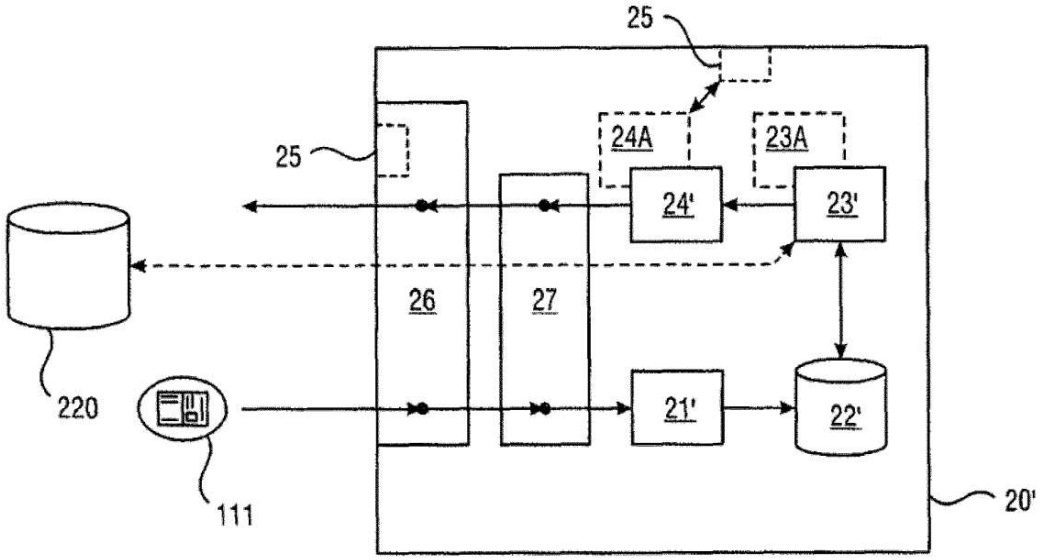

Fig. 3

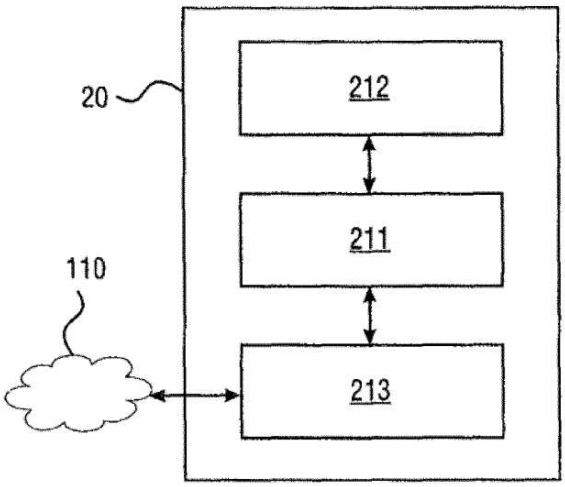

Fig. 4

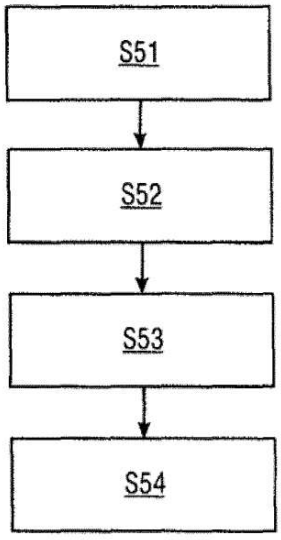

Fig. 5