(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 786 553**

(51) Int. CI.:

B42D 25/305 (2014.01)
G06Q 10/10 (2012.01)
B42D 25/24 (2014.01)
B41M 3/14 (2006.01)
G06F 3/12 (2006.01)
G06K 9/00 (2006.01)
H04L 29/06 (2006.01)
G06Q 10/06 (2012.01)
G06Q 50/26 (2012.01)
H04N 1/32 (2006.01)

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(86) Fecha de presentación y número de la solicitud internacional: **20.09.2016 PCT/EP2016/072257**

(87) Fecha y número de publicación internacional: **30.03.2017 WO17050737**

(96) Fecha de presentación y número de la solicitud europea: **20.09.2016 E 16775116 (3)**

(97) Fecha y número de publicación de la concesión europea: **29.01.2020 EP 3352994**

(54) Título: **Impresión remota de marcas en un documento de seguridad**

(30) Prioridad:

24.09.2015 EP 15186696

(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

Impresión remota de marcas en un documento de seguridad

Campo técnico

La presente invención se refiere a sistemas, entidades y métodos para impresión remota de marcas en documentos de seguridad. Más específicamente, la presente invención se refiere a marcado remoto 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.

En otras palabras, sellos oficiales (por ejemplo, visado, entada, salida, formulario de aduanas) ocasionalmente se aplican incorrectamente al documento de seguridad asociado (por ejemplo, pasaportes con sellos sellados en una sección incorrecta de un pasaporte, tal como dentro de los límites de una zona legible por máquina). Sellos oficiales pueden además aplicarse incorrectamente ocasionalmente (por ejemplo, mostrando la fecha u hora errónea, aplicado no uniformemente para estar manchado o incluir porciones ilegibles), u ocasionalmente se sella el tipo de sello erróneo (por ejemplo, visado de trabajo, visado de estudiante) en un pasaporte, o un sello oficial (por ejemplo, visado) puede emitirse incorrectamente (por ejemplo, sellado en un pasaporte cuando el titular de pasaporte no reúne, de hecho, los requisitos para el sello oficial seleccionado). Además de lo anterior, los sellos de caucho físicos son fáciles de copiar o de otra manera falsificar.

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, etc. 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. Es adicionalmente común que el equipo de campo produzca etiquetas autoadhesivas, por ejemplo, con un código de barras bidimensional y otras características, de modo de que el oficial puede simplemente imprimir una etiqueta de este tipo y aplicar al misma al pasaporte.

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.

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.

Por lo tanto, es un objeto de la presente invención proporcionar un sistema para impresión remota de marcas en documentos de seguridad que hace, por una parte, uso eficiente la infraestructura existente (es decir, equipo en el campo, procesamiento y repositorios de datos centrales y redes que conectan los mismos), y por otra parte, es lo suficientemente seguro y fiable de modo que puede usarse en el contexto de documentos de seguridad, tal como pasaportes. 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.

Además de lo anterior, puede ser deseable responder al robo, copia y/o falsificación de un sello oficial (por ejemplo, visado) de un país sustituyendo rápidamente todos los sellos oficiales del país con nuevos sellos que tienen un nuevo diseño. Sin embargo, en el caso de sellos de caucho físicos, actualizar un sello oficial implica la sustitución física de una multitud de tales sellos físicos ubicados en una multitud de instalaciones de control fronterizo alrededor de la frontera del país, embajadas en todo el mundo y otras instalaciones que emplean tales sellos, lo que lleva mucho tiempo y es caro, inhibiendo de este modo la capacidad de un país de actualizar rápidamente sus sellos oficiales.

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 14.

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 visas, sellos y etiquetas;

La Figura 2 muestra una vista esquemática de un despliegue de un sistema para impresión remota de marcas en documentos de seguridad de acuerdo con una realización de la presente invención;

La Figura 3 muestra una vista esquemática de una entidad de servidor para impresión remota de marcas en documentos 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 impresión remota de marcas en un 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 y para imprimir. 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/impresora 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.

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 de un 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.

Análogamente, si el punto de control 30 es parte de una entrada fronteriza, el oficial 19 comprueba si el individuo que presenta el documento de seguridad puede entrar en el país y qué clase de estado de visado necesita observarse. Es común que tras el permiso para entrar en el país, el oficial genera y aplica una etiqueta de visado o sello al pasaporte presentado. Las técnicas convencionales consideran en este punto sellos de caucho o la impresión de etiquetas autoadhesivas que se aplican, en consecuencia, a un espacio libre adecuado del documento de seguridad (por ejemplo, pasaporte).

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 impresión remota de marcas en documentos de seguridad, tales como pasaportes, 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 impresión remota de marcas en documentos 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, información de petición 111. Esta clase de información puede comprender cualquier dato adecuado para efectuar una petición segura para impresión remota de marcas. Específicamente, la información de petición 11 puede comprender información para identificar un pasaporte presentado y/o titular del mismo, información sobre el tipo de la marca solicitada, información sobre las propiedades de la marca (por ejemplo, duración de estancia permitida a aparecer en la marca) y similares. La petición puede efectuarse, asimismo, recibiendo 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.

De esta manera, el sistema 20 no depende de 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. 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 o impresoras 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 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, impresora o dispositivo integrado 12'. Adicionalmente, se considera cualquier otra fuente de datos para generar y reenviar la información de petición 111 en relación con un documento de seguridad 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 en relación con la información de petición. En el caso de que se proporcionan datos de imagen del documento de seguridad escaneado, el registro de datos puede comprender bien los datos de imagen recibidos y datos adicionales en relación con un propietario del documento de seguridad escaneado.

El sistema 20 comprende además un módulo de generación de marca 25 que se adapta para proporcionar datos que definen la marca a imprimirse en el documento de seguridad. El módulo de generación de marca 25 puede emplear para este propósito también la capacidad de almacenamiento de datos del almacenamiento de datos 22 o puede también acceder bien a un almacenamiento de datos especializado separado. Para generar la marca, el módulo de generación de marca 25 puede basarse en una separación en partes constantes y dinámicas de la marca. Más específicamente, el módulo de generación de marca 25 puede compilar la marca de modo que una parte constante se aplica a varias marcas, mientas que la parte dinámica puede depender de la petición de marca específica. Por ejemplo, la parte constante puede incluir toda la información y características de diseño gráficas para una marca de visado de un país dado. La parte dinámica puede generarse, por lo tanto, específicamente para la marca que tiene que imprimirse en un documento de seguridad objetivo para reflejar información como una fecha de entrada, una duración de permiso, una ubicación de entrada, un número de serie, cualquier otro código de característica de seguridad y similares.

Dentro del sistema 20 puede proporcionarse un módulo de analítica/procesamiento de datos gráfico 23 opcional. Este módulo 23 puede adaptarse para analizar la información de petición recibida con respecto a la generación de un correspondiente resultado de análisis. De esta manera, el sistema 20 puede ser capaz de realizar una comprobación de plausibilidad o conformidad con reglas en respuesta a la información de petición recibida. Por ejemplo, la información de petición puede comprender información que identifica a un individuo que busca entrar en un país dado, y el resultado de análisis puede indicar si se concede acceso o no al individuo. De manera similar, el resultado de análisis puede indicar si una marca solicitada debería, de hecho, imprimirse en el documento de seguridad remoto. De esta manera, el módulo 23 puede disponerse para ordenar a un módulo de control de impresora remoto 24, en consecuencia.

Dicho módulo de control de impresora 24 del sistema 20 se adapta para controlar remotamente equipo de impresión en el campo 1 para imprimir la marca remotamente en el documento de seguridad. Más específicamente, el módulo de control de impresora 24 establece un enlace de control 112 al correspondiente equipo de impresión en el campo uno, tal como el dispositivo 12' que es, en el presente ejemplo, un dispositivo integrado operable tanto para escanear un documento de seguridad presentado así como imprimir en este documento. De acuerdo con una realización específica de la presente invención, el módulo de control de impresora 24 controla el equipo de impresión remoto 12' para imprimir la marca mientras evita la posibilidad de reproducir la marca de una forma no autorizada.

Por ejemplo, el módulo de control de impresora 24 puede proporcionar comandos de impresión al equipo de impresión remoto 12' en alguna clase de secuencia troceada en donde una porción posterior de la marca se transmite únicamente desde el módulo de control de impresora 24 cuando se ha recibido correspondiente realimentación de que una secuencia anterior se imprimió realmente en el documento de seguridad. Este enfoque de uno a uno puede hacer difícil interceptar el fujo de datos de control para reproducir la marca de una forma ilegal.

De acuerdo con una realización adicional de la presente invención, el módulo 23 puede efectuar, adicionalmente o como alternativa al análisis, 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 23 puede adaptarse, a continuación, para superponer una imagen 49 de una marca proporcionada por el módulo 25 en la imagen del documento de seguridad. De esta manera, el módulo 23 puede 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 que puede reflejar ventajosamente la marca impresa realmente en el documento de seguridad. De esta manera, el acceso a estos datos gráficos adicionales puede permitir que personal autorizado verifique el aspecto de una marca impresa en un documento de seguridad presentado. Por ejemplo, el personal autorizado puede determinar una irregularidad si el aspecto de la marca impresa realmente en un documento de seguridad no coincide con el aspecto de los datos gráficos adicionales.

En general, las realizaciones de la presente invención permiten la impresión de marcas en un documento de seguridad con una calidad controlada y bien definida siguiendo igualmente requisitos y reglas bien definidos. Específicamente, la marca puede imprimirse en el documento de seguridad en una posición adecuada empleando colores adecuados y/o variaciones de contrastes. Específicamente, el almacenamiento de datos 22 puede almacenar, o el sistema 20 puede adquirir de una fuente de datos externa, datos que reflejan la posición de marcas impresas en un documento de seguridad específico en el pasado. Consultando y evaluando tales datos, es posible determinar una ubicación de impresión de la marca en el documento de seguridad de una forma más eficiente. En particular, puede elegirse que la posición de una marca de salida del país esté cerca de la ubicación de una marca de entrada al país. Esto puede permitir un procesamiento sencillo y rápido en puntos de control. Además, el espacio limitado de un documento de seguridad puede usarse de forma más eficiente, de modo que puede transportar más marcas mientras que evita que una marca afecte al aspecto y/o legibilidad de otra marca.

La Figura 3 muestra una vista esquemática de una entidad de servidor para impresión remota de marcas 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, información de petición 111. La entidad de servidor 20' comprende además un almacenamiento de datos 22 adaptado para almacenar un registro de datos que comprende cualesquiera datos de imagen recibidos y datos adicionales en relación con un propietario del documento de seguridad escaneado y cualquier petición recibida.

Además, la entidad de servidor 20' puede comprender un módulo de analítica adicional 23' y/o un módulo de procesamiento de datos gráficos adicional 23A adaptado para evaluar una petición recibida y generar un correspondiente análisis de resultado y, respectivamente, superponer una imagen de una marca en la imagen del documento de seguridad. El módulo de procesamiento de datos gráficos 23A 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 oficiales implicados, etc. (x) identidad del funcionario 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 módulo de analítica opcional 23’ puede adaptarse para analizar los registros de datos almacenados en el almacenamiento de datos 22 y para generar un correspondiente resultado de análisis. Específicamente, el módulo de analítica 23A puede mirar 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 o puede lanzarse 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 23’ 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 23’ 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). El módulo de control de impresora 24’ se adapta, como en las otras realizaciones descritas, para controlar una impresora remota 12 para imprimir una marca proporcionada por el módulo de generación de marca 25’ en el documento de seguridad en el campo.

Además, 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 23' 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 26 (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 27 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 26 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 27 como un módulo de cortafuegos o antimanipulación.

Puede proporcionarse un módulo de comunicaciones seguras 28 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 28 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 28 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 28 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 adaptada para recibir, desde el equipo de campo a través de una red, información de petición relacionada con la marca a imprimir en un documento de seguridad. 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 adicionalmente un módulo de generación de marca adaptado para generar datos que definen una marca a imprimirse en el documento de seguridad y un módulo de control de impresora remoto adaptado para controlar equipo de impresión remoto del sistema para imprimir la marca en el documento de seguridad.

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 (RECIBIR INFORMACIÓN DE PETICIÓN) de recepción, desde equipo de campo y a través de una red, de información de petición relacionada con marca a imprimirse en un documento de seguridad. En una etapa S52 (GENERAR DATOS DE MARCA) se generan datos que definen una marca a imprimirse en el documento de seguridad. Además, en una etapa S53 (IMPRESORA DE CONTROL REMOTO) se controla equipo de impresión remoto del sistema para imprimir la marca en el documento de seguridad.

Para las correspondientes implementaciones, pueden emplearse lector, escáneres e impresora y/o dispositivos

integrados disponibles para realizar la impresión y/o escaneo de un pasaporte. El sistema puede realizar inicialmente analítica en tiempo real siempre que un pasaporte se está escaneando en una instalación de escaneo de pasaportes para determinar si el número y cronología de entradas y salidas coinciden, para comprobar si un titular de pasaporte es una persona de interés para funcionarios en el país en el que el pasaporte del titular se está escaneando, y/o para determinar si el comportamiento del titular de pasaporte es oficialmente llamativo (por ejemplo, sospechoso). Si un uso pasaporte se indica como problemático, el sistema es capaz de lanzar una alerta al oficial responsable u otros funcionarios de acuerdo con leyes nacionales y protocolos.

Sobre la base de los datos recopilados y transferidos al sistema, el tipo de sello oficial (por ejemplo, visado de trabajo, visado de estudiante, etc.) que se está buscando puede determinarse de una forma fiable y centralmente controlada. El sistema puede comunicar a continuación al oficial responsable que opera el equipo de campo (lector/impresora) información predeterminada para guiar al oficial a través de los procedimientos para interrogar al titular de pasaporte. La información comunicada puede incluir preguntas sugeridas para preguntar, que pueden incluir preguntas seleccionadas aleatoriamente, una lista de verificación de artículos para que considere el oficial antes de aprobar el sellado, otra información procedimental relacionada y cualquier combinación de los mismos.

Si el pasaporte es adecuado para sellarse, el sistema recupera de la base de datos la plantilla de sello oficial apropiada (parte constante) y su parte dinámica y contenido (es decir, valores de campo de plantilla), y controla centralmente (es decir, remotamente) la impresora para imprimir el sello oficial en el pasaporte (u otro documento de seguridad u oficial) de acuerdo con reglas específicas de país en cuanto a la colación del sello oficial. En variaciones, el sello oficial puede imprimirse en una ubicación aleatoria, en una ubicación aleatoria dentro de límites especificables o una ubicación seleccionada por el oficial implicado (siempre que sistema determine que tal ubicación cumple con las reglas específicas de país en cuanto a la colocación). El sello oficial (marca) puede incluir datos cifrados, incluyendo datos cifrados dinámicamente, para un nivel de seguridad inalcanzable por los sellos de caucho físicos. Además, el sistema puede controlar el equipo de campo para imprimir cualquier número de sellos oficiales implicando cualquier número de plantillas de sellos oficiales, aunque una plantilla (y en ocasiones dos plantillas) es más común.

Por lo tanto, un método de operación puede incluir adicionalmente una etapa de análisis de cualquier dato de imagen recibido para hacer una determinación de si, y posiblemente dónde, una marca tiene que imprimirse o no en el documento de seguridad. 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.

En general, cada plantilla de marca (sello oficial) puede tener cualquier diseño y composición artísticos adecuados, incluyendo especificar un color, tono y tipo de tinta (por ejemplo, selección de conjunto de cartuchos o conjunto de depósitos de tinta) a emplear cuando se imprime el sello oficial. Además, puede existir cualquier número de campos de plantilla, incluyendo campos de plantilla asociados con la posición (por ejemplo, retrato, apaisado, ángulo personalizado) del sello oficial en el pasaporte; texto adicional (por ejemplo, nombre de ubicación, restricciones de viaje, otros mensajes, etc.) a aplicarse dinámicamente; códigos legibles por humano y/o por máquina (por ejemplo, de barras) para incluir datos encriptados (por ejemplo, identificación de sello, biométricas del oficial o titular del pasaporte u otros datos de identificación, mensajes cifrados, formas cifradas de cualquier dato de otro campo, etc.); otros campos; y cualquier combinación de los mismos.

Puede identificarse, como se indica a continuación, una lista detallada de posibles campos de plantilla, a partir de los cuales puede seleccionarse cualquier número de campo o campos de plantilla para encontrar implementación en una realización de la presente invención:

1) SELLO_DIRECCIÓN = 0;
2) SELLO_NOMBRE_AEROPUERTO = 1;
3) SELLO_NÚMERO_AEROPUERTO = 2;
4) SELLO_NOMBRE_OFICIAL = 3;
5) OFICIAL_NÚMERO = 4;
6) PUERTA_SECCIÓN = 5;
7) PUERTA_NÚMERO = 6;
8) ENTRADA_FECHA = 7;
9) ENTRADA_HORA = 8;

10) SALIDA_FECHA = 9;
11) SALIDA_HORA = 10;
12) DURACIÓN = 11;
13) DOCUMENTO_TIPO = 12;
14) DOCUMENTO_SUBTIPO = 13;
15) DOCUMENTO_NÚMERO = 14;
16) DOCUMENTO_PAÍS_EMISIÓN = 15;
17) PASAJERO_APELLIDO = 16;
18) PASAJERO_NOMBRE = 17;
19) PASAJERO_NACIONALIDAD = 18;
20) PASAJERO_FECHA_NACIMIENTO = 19;
21) PASAJERO_SEXO = 20;
22) PASAJERO_LUGAR_NACIMIENTO = 21;
23) DOCUMENTO_FECHA_EMISIÓN= 22;
24) DOCUMENTO_LUGAR_EMISIÓN = 23;
25) DOCUMENTO_FECHA_EXPIRACIÓN = 24;
26) PASAJERO_ID_SOCIAL = 25;
27) PROPÓSITO_VIAJE = 26;
28) SELLO_ID = 27;

En una realización adicional de la presente invención, el sistema se configura para realizar el siguiente modo de operación: el sistema recibe entrada de usuario que proporciona datos de plantilla alterada o de otra manera nueva, determina el país al que se aplican los datos de nueva plantilla, transfiere los datos de nueva plantilla a cada uno del equipo de campo de ese país, comunica un mensaje a funcionarios en el campo que hay disponible una actualización. Cuando cualquier dispositivo del equipo de campo se reinicializa a continuación o actualiza de otra manera, los datos de nueva plantilla sustituyen los datos de plantilla que estaban anteriormente en uso. Distribuir la nueva plantilla cada equipo de campo de ese país puede implicar distribuir la nueva plantilla a instalaciones fronterizas, embajadas en todo el mundo, organizaciones policiales u otras agencias en todo el mundo, por ejemplo.

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 para imprimir remotamente una marca, tal como un visado, sello o etiqueta, en un documento de seguridad, tal como un pasaporte, que comprende:

- una interfaz (21) adaptada para recibir, desde equipo de campo y a través de una red, información de petición relacionada con una marca a imprimirse en dicho documento de seguridad;
- un módulo de generación de marca (25) adaptado para generar datos que definen una marca a imprimirse en el documento de seguridad; y **caracterizado por**
- un módulo de control de impresora remoto (24) adaptado para controlar equipo de impresión remoto del sistema para imprimir la marca en el documento de seguridad.

2. El sistema de acuerdo con la reivindicación 1, en donde el módulo de control de impresora remoto se adapta para transmitir partes de datos de comandos de impresión una tras otra, y se adapta para esperar un acuse de recibo antes de que se transmita la siguiente parte.

3. El sistema de acuerdo con la reivindicación 1 o 2, en donde el módulo de generación de marca se adapta para generar los datos a partir de una parte de plantilla y una parte dinámica.

4. El sistema de acuerdo con la reivindicación 3, en donde la parte de plantilla se almacena en una ubicación central y el sistema se configura para actualizar centralmente dicha parte de plantilla.

5. El sistema de acuerdo con una cualquiera de las reivindicaciones 1 a 4, comprendiendo adicionalmente un módulo de analítica adaptado para analizar datos gráficos recibidos de una imagen del documento de seguridad y para generar un resultado de análisis.

6. El sistema de acuerdo con la reivindicación 5, en donde el módulo de analítica se adapta adicionalmente para hacer una determinación de si la marca tiene que imprimirse o no en el documento de seguridad.

7. El sistema de acuerdo con la reivindicación 5 o 6, en donde el módulo de analítica se adapta adicionalmente para hacer una determinación de dónde en el documento de seguridad se imprime la marca.

8. El sistema de acuerdo con una cualquiera de las reivindicaciones 1 a 7, comprendiendo adicionalmente un sensor adaptado para detectar manipulación con el sistema.

9. El sistema de acuerdo con la reivindicación 8, 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.

10. El sistema de acuerdo con una cualquiera de las reivindicaciones 1 a 9, comprendiendo adicionalmente un módulo de cortafuegos adaptado para proteger el sistema de ataques de red y/o ataques físicos al hardware del sistema.

11. El sistema de acuerdo con una cualquiera de las reivindicaciones 1 a 10, comprendiendo adicionalmente un módulo de comunicación segura adaptado para proporcionar comunicación segura de dichos datos de imagen y/o una notificación.

12. El sistema de acuerdo con una cualquiera de las reivindicaciones 1 a 11, adaptándose para comunicarse con una base de datos externa.

13. El sistema de acuerdo con una cualquiera de las reivindicaciones 1 a 12, en donde el sistema está remoto del equipo que realiza la impresión de la marca en el documento de seguridad.

14. Un método para imprimir remotamente una marca, tal como un visado, sello o etiqueta, en un documento de seguridad, tal como un pasaporte, que comprende:

- una etapa (S51) de recepción, desde equipo de campo y a través de una red, de información de petición relacionada con una marca a imprimirse en dicho documento de seguridad;
- una etapa (S52) de generación de datos que definen una marca a imprimirse en el documento de seguridad; y **caracterizado por**
- una etapa (S53) de control remotamente de equipo de impresión remoto del sistema para imprimir la marca en el documento de seguridad.

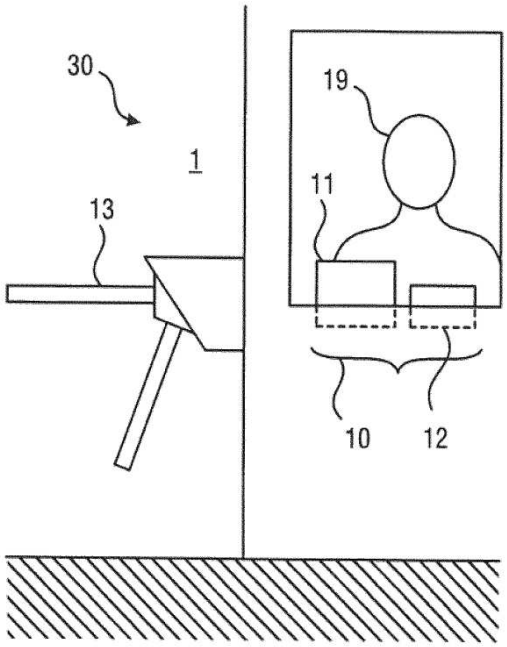

Fig. 1A

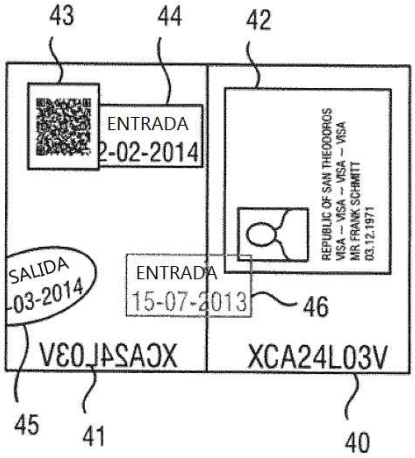

Fig. 1B

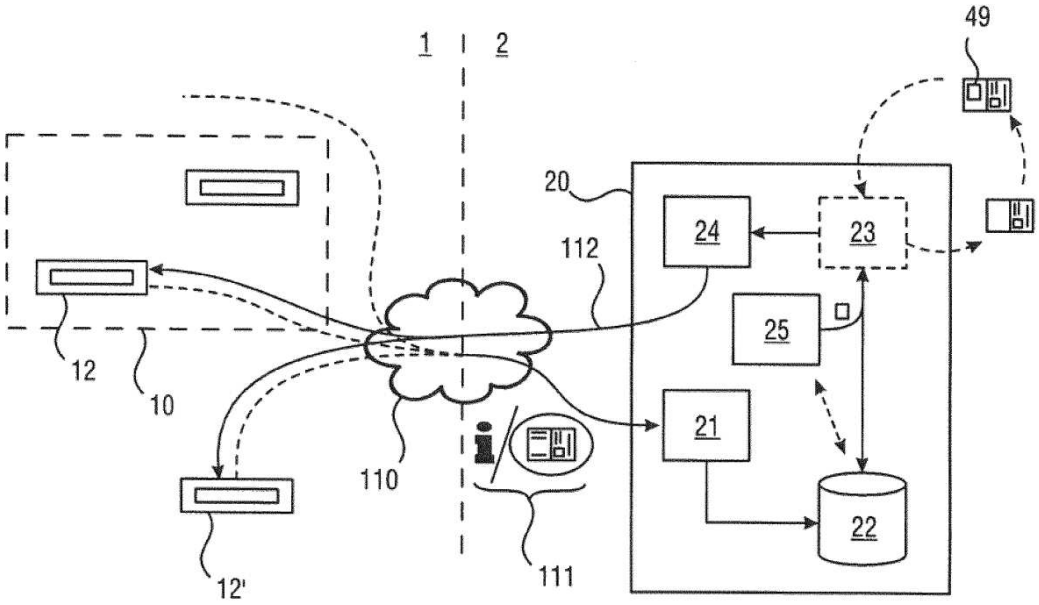

Fig. 2

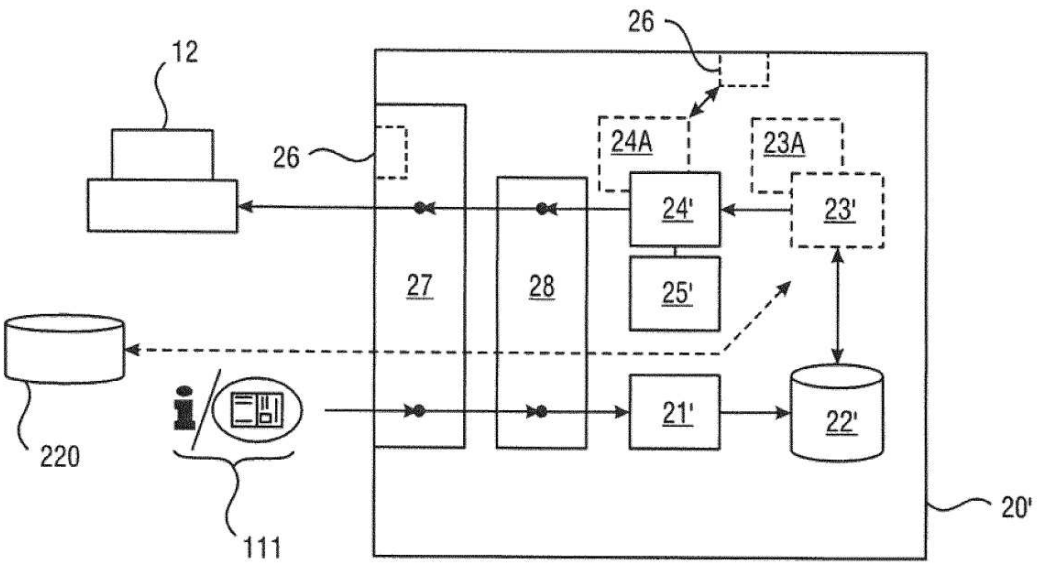

Fig. 3

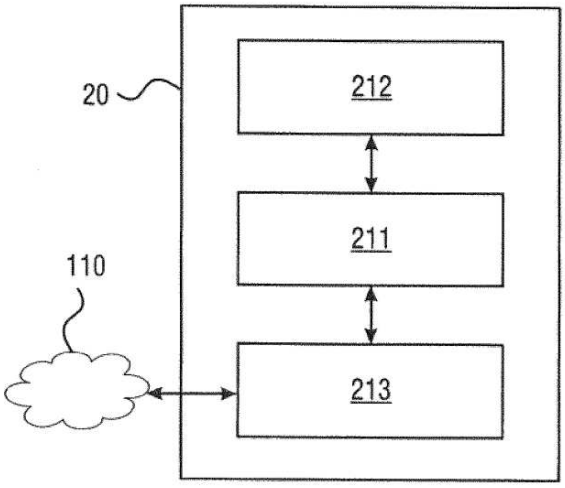

Fig. 4

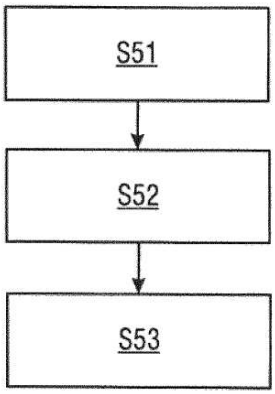

Fig. 5