(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 710 901**

(51) Int. CI.:

G06T 1/00 (2006.01)

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(86) Fecha de presentación y número de la solicitud internacional: **23.08.2005 PCT/US2005/029874**

(87) Fecha y número de publicación internacional: **08.09.2006 WO06093531**

(96) Fecha de presentación y número de la solicitud europea: **23.08.2005 E 05790015 (1)**

(97) Fecha y número de publicación de la concesión europea: **14.11.2018 EP 1854239**

(54) Título: **Sistema y método para la autenticación de un objeto basada en red**

(30) Prioridad:

28.02.2005 US 68350
19.08.2005 US 207437

(45) Fecha de publicación y mención en BOPI de la traducción de la patente:
29.04.2019

(73) Titular/es:

GRAPHIC SECURITY SYSTEMS CORPORATION (100.0%)
4450 Jog Road
Lake Worth, FL 33467, US

(72) Inventor/es:

ALASIA, ALFRED, V.;
ALASIA, ALFRED, J.;
ALASIA, THOMAS, C.;
CVETKOVIC, SLOBODAN y
ILIC, IGOR

(74) Agente/Representante:

SÁEZ MAESO, Ana

DESCRIPCIÓN

Sistema y método para la autenticación de un objeto basada en red

Referencia cruzada a solicitudes relacionadas

Esta solicitud es una continuación en parte de la solicitud estadounidense No. 11/68,350, presentada el 28 de febrero de 2005, que reivindica prioridad de la solicitud provisional estadounidense No. 60/565,300 presentada el 26 de abril de 2004. La solicitud también está relacionada con la solicitud estadounidense No. 10/847,962 (solicitud '962) presentada el 18 de mayo de 2004 y la solicitud estadounidense No. 10/897,943 (solicitud '943) presentada el 18 de mayo de 2004.

Campo de la invención

La invención se refiere, en general, al campo de la protección contra falsificaciones, y más particularmente al campo de una autenticación de un objeto a través del uso de una imagen codificada.

Antecedentes de la invención

La falsificación de documentos y la falsificación de productos son problemas significativos que han sido abordados de varias maneras. Uno de los enfoques con más éxito ha sido el uso de imágenes latentes u ocultas aplicadas a o impresas en objetos a proteger. Estas imágenes en general no son visibles sin la ayuda de dispositivos especializados que las convierten en visibles.

Un enfoque para la formación de una imagen latente es codificar ópticamente la imagen de manera que, cuando se imprime, la imagen se puede ver sólo a través del uso de un dispositivo de codificación correspondiente. Dichas imágenes se pueden utilizar virtualmente en cualquier forma de documento impreso incluyendo documentos legales, tarjetas y papeles de identificación, etiquetas, moneda, sellos, etcétera. También se pueden aplicar a artículos o envases de artículos sujetos a falsificación.

Los objetos a los cuales se aplica una imagen codificada pueden autenticarse decodificando la imagen codificada y comparando la imagen de codificada con una imagen de autenticación esperada. La imagen de autenticación puede incluir información específica del objeto que está siendo autenticado o información relativa a un grupo de objetos similares (por ejemplo, productos producidos por un fabricante o instalación particulares). La producción y aplicación de imágenes codificadas se puede controlar de manera que no se puedan duplicar fácilmente. Además, la imagen codificada puede estar configurada de manera que la manipulación de la información del documento o etiqueta es fácilmente evidente.

La autenticación de documentos y otros objetos "en el campo" ha requerido típicamente el uso de decodificadores de hardware tal como lentes lenticulares o de micro-matriz que decodifican ópticamente las imágenes codificadas. Estas lentes deben tener características ópticas que se corresponden con los parámetros utilizados para codificar y aplicar la imagen de autenticación y deben estar orientadas apropiadamente con el fin de que el usuario decodifique y vea la imagen.

Debido a que sólo pueden ser utilizadas imágenes codificadas con características correspondientes, los decodificadores de hardware son herramientas relativamente inflexibles. También hay circunstancias en las que el uso de un decodificador óptico para decodificar imágenes codificadas no es práctico o no es deseable. Por ejemplo, una autenticación utilizando un decodificador óptico requiere una comparación inmediata en el lugar de la imagen decodificada con la imagen de autenticación. Esto requiere que el inspector en el lugar del objeto que se está autenticando deba ser capaz de reconocer diferencias entre la imagen decodificada y la imagen de autenticación esperada. Esto no es práctico en casos en los que hay muchas variaciones posibles en la imagen de autenticación esperada. También puede que no sea deseable para el inspector en el lugar tener acceso a información que pudiera estar embebida en la imagen decodificada.

La solicitud de patente PCT WO0180512A2 divulga un sistema de codificación/decodificación de imagen y un método para producir un dispositivo de seguridad generado por ordenador que puede ser impreso en un documento, tal como un pasaporte, para asegurar el documento contra una alteración de datos. Medios de codificación por desviación comprenden medios para aplicar una lente de software seleccionada a una imagen de origen y producir una imagen desviada. Medios de codificación por encriptación comprenden medios para aplicar una función de encriptación a la imagen desviada o a una imagen de origen y para producir una imagen encriptada. La solicitud de patente estadounidense US2004128512A1 divulga un sistema que responde a documentos con marca de agua para intercambio de datos. El sistema contiene un terminal de usuario que incluye un lector de marca de agua, y un dispositivo de captura para capturar una imagen de un documento con marca de agua, y un sitio central que incluye una base de datos de hashes de imagen. El lector de marca de agua lee una marca de agua y computa un hash de una imagen capturada, y envía el hash al sitio central para la comparación con la base de datos de hashes de imagen.

Resumen de la invención

La presente invención proporciona un método en el sistema para determinar si un objeto de comprobación es un objeto auténtico al cual se ha aplicado una imagen codificada esperada como se reivindica en cualquiera de las reivindicaciones adjuntas.

Breve descripción de los dibujos

La invención se puede entender de forma más completa leyendo la siguiente descripción detallada junto con los dibujos que acompañan, en los cuales indicadores de referencia similares son utilizados para designar elementos similares, y en los cuales:

La figura 1 es una ilustración del uso de un decodificador óptico para decodificar una imagen codificada impresa;

La figura 2 es un diagrama de flujo de un método de autenticación de un objeto de acuerdo con un modo de realización de la invención;

La figura 3 es una ilustración esquemática de un sistema de autenticación de un objeto de acuerdo con un modo de realización de la invención;

La figura 4 es una ilustración esquemática de un sistema de autenticación de un objeto basada en red de acuerdo con un modo de realización de la invención;

La figura 5 es una representación esquemática de un sistema de decodificación digital que puede utilizarse en modos de realización de la invención;

La figura 6 es una representación esquemática de un sistema de decodificación basado en red que puede ser utilizado en modos de realización de la invención;

La figura 7 es una representación esquemática de un sistema de decodificación basado en red que se puede utilizar en modos de realización de la invención; y

La figura 8 es un diagrama de flujo de un método basado en red para proporcionar un servicio de decodificación de imagen interactivo a un usuario.

Descripción detallada de la invención

La presente invención proporciona sistemas y métodos para autenticar documentos, productos comerciales y otros objetos usando imágenes codificadas ópticamente decodificables. Los métodos de la invención proporcionan una captura digitalmente de una imagen codificada aplicada al objeto que se va a autenticar. Esto se puede realizar utilizando un escáner u otro dispositivo de toma de imagen para producir una imagen digital capturada. Un procesador de datos equipado con un decodificador digital puede entonces ser utilizado para identificar y decodificar la imagen codificada a partir de una imagen digital capturada y para extraer indicios y/o información del resultado de codificado. Los indicios y/o información extraídos se pueden entonces utilizar para autenticar el objeto o documento al cual se aplicó la imagen codificada. En algunos modos de realización, la imagen codificada nunca necesita ser vista por un ser humano. En algunos modos de realización, la imagen codificada puede ser capturada mediante un inspector en el lugar que transmite la imagen capturada a un procesador separado (o series de procesadores) donde la imagen es decodificada y, opcionalmente, comparada con una imagen de autenticación esperada. Los resultados pueden entonces ser devueltos al inspector en el lugar o a otro personal autorizado. Otros modos de realización y variaciones serán evidentes a partir de la siguiente exposición.

Tal y como se expuso previamente, los métodos de autenticación de la invención hacen uso de imágenes codificadas que están normalmente embebidas en una imagen de fondo o de origen e impresas en artículos que pueden estar sujetos a una alteración, falsificación o imitación, tal y como se utiliza en el presente documento, el término “imagen codificada” se refiere a una imagen que es manipulada y/u ocultada dentro de un campo de fondo o dentro de otra imagen de tal manera que cuando se aplica o se imprime, la imagen codificada no se puede discernir por el ojo humano sin el uso de un dispositivo de decodificación. Algunas imágenes codificadas están ocultas de manera que su presencia es difícil de discernir de la imagen de fondo o primaria. Otras imágenes codificadas son fácilmente visibles pero son ilegibles debido a que el contenido de la imagen ha sido sistemáticamente revuelto o de otro modo manipulado.

Las imágenes codificadas de una importancia particular para la presente invención son aquellas que están configuradas para ser de codificadas ópticamente utilizando un dispositivo de decodificación basado en lente. Dichas imágenes toman la ventaja de la habilidad de ciertos tipos de lentes (por ejemplo, una lente lenticular) de muestrear un contenido de imagen basándose en sus características ópticas. Por ejemplo, una lente lenticular se puede utilizar para muestrear y aumentar el contenido de imagen basándose en la frecuencia lenticular de la lente. Las imágenes utilizadas son codificadas normalmente por uno de diversos métodos que incluyen establecer un patrón periódico regularizado que tiene una frecuencia que corresponde a la de la lente lenticular que se va utilizar como decodificador, introduciendo después distorsiones del patrón que se corresponden al contenido de la imagen que está siendo codificada. Estas distorsiones pueden realizarse tan pequeñas que hagan la imagen difícil o imposible de discernir del patrón regularizado a simple vista. Las imágenes codificadas de este tipo se pueden producir de una forma analógica

utilizando un equipo fotográfico especializado tal y como se divulga en la patente estadounidense No. 3,937,565 o digitalmente cómo se divulga en la patente estadounidense No. 5,708,717 (patente '717).

Las imágenes codificadas digitalmente se pueden embeber dentro de un fondo o en otras imágenes de manera que la mera presencia de la imagen codificada es difícil de discernir. Con referencia a la figura 1, una imagen 10 codificada puede establecerse utilizando una imagen 20 primaria o de origen y una imagen 40 secundaria, que es embebida en la imagen 20 primaria de tal manera que la imagen 40 secundaria se puede ver únicamente con un dispositivo 3030 de decodificación de una frecuencia predeterminada. La imagen primaria puede ser una imagen de fondo en blanco y gris o en color como en la imagen 10 codificada de la figura 1 o puede incluir un contenido de imagen visible tal como un diseño o fotografía de cualquier otra forma de indicios. La imagen secundaria también puede tener cualquier forma de imagen o indicios y puede incluir indicios relacionados de alguna manera con la imagen primaria. En el ejemplo de la imagen 10 codificada, la imagen 40 secundaria es un patrón de repetición basado en las palabras "Departamento de Transporte". La imagen secundaria se puede modificar de forma separada después combinar o embeber en la imagen primaria o el proceso de embebido se puede lograr de tal manera que la imagen secundaria es codificada cuando es embebida. Tal y como se muestra en la figura 1, la imagen secundaria puede verse colocando el dispositivo 30 de decodificación sobre la imagen 10 codificada en una orientación correcta. En el ejemplo de la figura 1, el dispositivo de decodificación tiene un eje 32 horizontal y un eje 34 vertical y la imagen 10 codificada tiene un eje 22 horizontal y un eje 24 vertical. La imagen 40 secundaria es revelada cuando el eje 32 horizontal del dispositivo 30 de decodificación está orientado formando un ángulo α de decodificación con respecto al eje 22 horizontal de la imagen 10 codificada. El ángulo α de codificación es un parámetro decodificación que se establece antes de decodificar y embeber la imagen secundaria.

Los métodos mediante los cuales se embebe o se combina la imagen secundaria con la imagen primaria se pueden dividir en dos enfoques generales. En el primer enfoque, se impone un comportamiento periódico regularizado en la imagen primaria utilizando una frecuencia predeterminada. Esto se logra principalmente explorando la imagen primaria a la frecuencia predeterminada. La imagen secundaria es después mapeada en la imagen primaria de manera que el comportamiento regularizado de la imagen primaria se puede alterar en ubicaciones correspondientes a aquellas en la imagen secundaria que incluyen un contenido de imagen. Las alteraciones son tan pequeñas que son difíciles de discernir para el ojo humano. Sin embargo, cuando una lente lenticular que tiene una frecuencia correspondiente a la frecuencia predeterminada es colocada sobre la imagen primaria, muestreará el contenido de imagen primaria de tal manera que las alteraciones se revelan para formar la imagen secundaria latente.

En el segundo enfoque, el comportamiento periódico regularizado se impone en primer lugar en la imagen secundaria en lugar de en la imagen primaria, con alteraciones en ese comportamiento sucediendo en cualquier sitio en el que haya un contenido en la imagen secundaria. La imagen secundaria es después mapeada en la imagen primaria y el contenido de la imagen primaria alterado pixel a píxel basándose en el contenido de la imagen secundaria codificada.

Otro método de embebido de una imagen se utiliza comúnmente en billetes de banco y cheques. En este método, se crea una imagen latente cambiando la dirección de los elementos de exploración en las imágenes visibles en posiciones correspondientes al contenido de la imagen oculta. Por ejemplo, se pueden cambiar líneas de exploración verticales en la imagen primaria a líneas horizontales en las ubicaciones correspondientes a la imagen latente. La imagen latente puede típicamente ser vista inclinando el billete de banco ligeramente. Sin embargo, las desviaciones en la imagen primaria también se pueden decodificar utilizando un decodificador óptico. Esto es debido a que las líneas de exploración de la imagen primaria discurrirán a lo largo de la longitud de la línea lenticular del decodificador en las posiciones en las que no hay un contenido oculto, pero tendrán sólo una sección trasversal en las condiciones en las que hay un contenido oculto. Esta diferencia hace que la imagen oculta aparezca mucho más brillante que la visible cuando se ve a través del decodificador.

El hilo común de todos los métodos de codificación gráficos anteriores y sus imágenes codificadas resultantes es que incluyen desviaciones del comportamiento periódico regular (por ejemplo, una ubicación espacial, una densidad de tono, un ángulo de exploración). El comportamiento periódico regular y las desviaciones del mismo se pueden establecer basándose en la metodología de codificación utilizada y conjunto predeterminado de parámetros de codificación. Las desviaciones se hacen evidentes a través del uso de un decodificador que tiene características que se corresponden a uno o más de los parámetros de codificación. Por ejemplo, uno de los parámetros de codificación puede ser la frecuencia del comportamiento periódico regular. El codificador (esté basado en hardware o en software) debe estar configurado de acuerdo con esa frecuencia. Por ejemplo, en el caso de una lente lenticular, la frecuencia de lentes establece de manera que la frecuencia del comportamiento periódico regular es igual a la frecuencia de la lente o un múltiplo par de la frecuencia de la lente. La lente lenticular puede entonces actuar como un muestreador/aumentador del contenido que enfatiza las desviaciones del comportamiento regularizado y las ensambla en la imagen secundaria.

Se puede utilizar una lente lenticular para decodificar tanto imágenes codificadas visibles cuyo contenido ha sido revueltos sistemáticamente, e imágenes codificadas embebidas en una imagen primaria o fondo. Tal y como se describe en la solicitud de patente estadounidense No. 11/068,350 (solicitud '350) sin embargo, también se pueden utilizar decodificadores basados en software para decodificar imágenes codificadas que han sido creadas o capturadas digitalmente. Estos decodificadores se pueden adaptar para decodificar cualquier versión digital de una imagen codificada ópticamente incluyendo imágenes codificadas digitales que nunca han sido impresas e imágenes

codificadas impresas que han sido escaneadas o transformadas por otros medios en forma digital. Las imágenes codificadas digitales pueden ser imágenes latentes embebidas en imágenes de fondo o primarias o pueden ser imágenes visibles que han sido revueltas o manipuladas sistemáticamente. La imagen primaria puede ser una imagen en blanco con ningún contenido discernible (por ejemplo, una caja gris) o puede ser una imagen real con un contenido discernible.

El software para decodificar digitalmente imágenes codificadas digitales se puede incorporar en virtualmente cualquier procesador de datos. Con el propósito de llevar a la práctica los métodos de autenticación de la presente invención, el software puede utilizar cualquier metodología de decodificación incluyendo, pero no limitada a, los métodos descritos en la solicitud '350. Esto incluye (1) métodos que requieren información del contenido de la imagen primaria, la imagen secundaria o tanto la imagen primaria como secundaria; y (2) métodos que no requieren ningún conocimiento anterior con respecto al contenido de la imagen. Ambos de estos tipos de métodos requieren un conocimiento de los parámetros de codificación utilizados para codificar y embeber la imagen secundaria.

Tal y como se describe en la solicitud '350, se pueden escanear imágenes codificadas impresas o capturadas digitalmente utilizando un dispositivo de adquisición de imagen. Tal y como se utiliza en el presente documento, el término "dispositivo de adquisición de imagen" significa cualquier dispositivo o sistema utilizado para capturar o producir una imagen digitalizada de un documento o un objeto o porciones objetivo del mismo. Los dispositivos de adquisición de imagen incluyen, pero no están limitados a, escáneres, cámaras digitales, y sistemas que tienen una combinación de una cámara analógica y un capturador de fotogramas. El dispositivo de adquisición de imagen se puede adaptar para capturar imágenes utilizando luz en las porciones visible o no visible (por ejemplo, UV e IR) del espectro electromagnético.

Una imagen codificada capturada (es decir, una imagen codificada impresa que ha sido escaneada o de otro modo capturada digitalmente utilizando un dispositivo de adquisición de imagen) se puede procesar mediante un procesador de decodificación adaptado para aplicar uno o más algoritmos de decodificación basados en software para producir un resultado de decodificación. Utilizando dichos métodos como un reconocimiento de caracteres ópticos (OCR), el procesador de decodificación puede también adaptarse para extraer indicios y/o información de la imagen decodificada y para comparar los indicios extraídos y/o la información con un criterio de autenticación predeterminado. Tal y como se expondrá, el procesador de decodificación puede estar en una ubicación remota del dispositivo de adquisición de imagen.

Con referencia ahora a la figura 2, un método M100 de autenticación básico de acuerdo con la presente invención hace uso de la habilidad de decodificar digitalmente una imagen codificada capturada. El método M10 se puede utilizar para inspeccionar un objeto de prueba para determinar si una imagen codificada esperada ha sido aplicada al mismo, la imagen codificada esperada que ha sido aplicada a todos los objetos auténticos. Tal y como se utiliza en el presente documento, el término "auténtico" normalmente indica que un objeto fue producido mediante una fuente autorizada o de una manera autorizada. La imagen codificada esperada es una versión modificada de una imagen de autenticación predeterminada. La imagen codificada esperada puede ser la misma para cada objeto que está siendo comprobado o puede ser una imagen codificada variable que es diferente para cada objeto. Cualquier objeto que no porte la imagen codificada esperada se puede asumir que es indicativo de una ausencia de autenticidad o es indicativo de que el objeto o indicio aplicado al mismo no ha sido alterado.

El método M100 comienza en S100 y en S110 una imagen digital del objeto de prueba es capturada utilizando un dispositivo de adquisición de imagen. La imagen digital capturada puede incluir todo o una porción del objeto siempre que incluya un área objetivo donde se pueda aplicar una imagen codificada esperada sobre un objeto auténtico. La imagen digital capturada puede estar configurada de manera que sólo el área objetivo es capturada o puede estar configurada de manera que el área objetivo es incluida en una vista más grande. En cualquier caso, la imagen capturada puede también incluir marcas de orientación identificables que permiten la identificación y la orientación apropiada de la porción de área objetivo de la imagen digital capturada. En S120, la imagen digital capturada es enviada a un procesador de autenticación. Tal y como se expondrá, alguno o todos los procesadores de autenticación pueden estar coubicados con el lugar de inspección (es decir, la ubicación donde se captura la imagen digital del objeto de prueba) y alguno o todos los procesadores de autenticación pueden ser remotos al lugar de inspección. En cualquier caso, el procesador de autenticación puede estar conectado al dispositivo de adquisición de imagen mediante una red.

El procesador de autenticación puede estar configurado para llevar a cabo automáticamente alguna o todas las etapas restantes del método M100. En S130, el procesador de autenticación determina uno o más de los parámetros de codificación que se utilizaron para codificar la imagen de autenticación para producir la imagen codificada esperada. El número de parámetros requeridos puede depender de la metodología de decodificación digital específica utilizada. Los parámetros de codificación pueden obtenerse a partir de un almacenamiento de datos donde están situados en el momento de la codificación. Este almacenamiento de datos puede ser una parte de o estar coubicado con el procesador de autenticación no se puede disponer en un procesador de base de datos separado o servidor accesible al procesador de autenticación mediante una red. El almacenamiento de datos también puede tomar la forma de una banda magnética, una tarjeta láser, una tarjeta inteligente, un chip de procesador, un chip de memoria, o un código de barras, que se pueden aplicar o fijar o de otro modo asociar con un objeto al cual se aplica la imagen codificada. Los parámetros de codificación y o la imagen de autenticación pueden ser específicos del objeto o pueden ser constantes

para un conjunto de objetos particulares. En algunos modos de realización, algunos o todos los parámetros de codificación se pueden recibir con una petición de codificación o determinar a partir del contenido de la imagen.

En S140, el procesador de autenticación puede utilizar puntos de referencia de objeto para orientar el área objetivo de la imagen digital capturada para la decodificación. Estos puntos de referencia se pueden basar en la geometría inherente del objeto o pueden aplicarse específicamente en el momento en que se aplica la imagen codificada a los objetos auténticos. En este último caso, la presencia de dichos puntos de referencia se podría utilizar como una comprobación de autenticación inicial. Se entenderá para los expertos en la técnica que si se captura la imagen digital de una manera tal que el objeto está siempre orientado en exactamente la misma manera con respecto al dispositivo de adquisición de imagen, puede que no haya necesidad para la orientación digital de la imagen capturada. Por ejemplo, si los objetos comprobados son documentos que pueden situarse de forma precisa para el escaneado, la orientación del área objetivo puede ser lo suficientemente constante para qué no sea necesaria la orientación de la imagen digital capturada.

Una vez que el área objetivo de la imagen digital capturada es orientada, el procesador de autenticación aplica una metodología de decodificación digital a la imagen digital capturada para producir un resultado de decodificación en S150. El resultado de decodificación puede entonces ser comparado con el criterio de autenticación para determinar un resultado de autenticación en S160. Esto se puede lograr mostrando los resultados de decodificación para la comparación visual con la imagen de autenticación. De forma alternativa, se puede utilizar un software de OCR o de otro reconocimiento de patrón para comparar el resultado de decodificación con la imagen de autenticación. En los casos en los que la imagen de autenticación contenga información que es específica del objeto, el contenido de información del resultado de decodificación se puede comparar con la información derivada directamente del objeto en lugar de con la imagen de autenticación original.

En S170, se realiza una determinación de autenticación basándose en la comparación del resultado de decodificación con el criterio de autenticación. Esta determinación se puede realizar mediante un revisor humano del resultado de decodificación o se puede realizar automáticamente mediante el procesador de autenticación. En cualquier caso, el resultado de autenticación se puede almacenar y/o devolver a un usuario o a otro(s) solicitante(s) autorizado(s). En modos de realización en los que se hace la determinación de autenticación en una ubicación remota del lugar de inspección, la determinación de autenticación se puede transmitir al lugar de inspección. El método finaliza en S180.

Con referencia la figura 3, el método M100 y otros métodos de acuerdo con la invención se pueden llevar a cabo utilizando un sistema 100 de autenticación de objeto que comprende un dispositivo 110 de adquisición de imagen digital y un procesador 120 de autenticación. El sistema 120 de autenticación de objeto puede también comprender una base 130 de datos de información de codificación que puede estar incluida en o en comunicación con el procesador 120 de autenticación. El sistema 100 de autenticación de objeto está configurado para la inspección y la autenticación de los objetos de prueba para verificar la presencia de una imagen de autenticación codificada en los mismos. Alguno o todos los parámetros de codificación y la imagen de autenticación utilizados para codificar la imagen de autenticación se pueden almacenar en la base 130 de datos de información de codificación de tal manera que sean accesibles al procesador 120 de autenticación.

El dispositivo 110 de adquisición de imagen puede ser cualquier dispositivo adaptado para registrar una imagen digital de al menos una porción del objeto demuestra que contiene un área objetivo en la cual, en objetos auténticos, se ha aplicado una imagen de autenticación codificada. El procesador 120 de autenticación puede ser cualquier procesador de datos configurado para recibir y procesar imágenes digitales. El procesador 120 de autenticación incluye un módulo 122 de recepción de imagen adaptado para una comunicación selectiva con el dispositivo 110 de adquisición de imagen y para recibir imágenes digitales capturadas del mismo. El módulo 122 de recepción de imagen transfiere las imágenes digitales capturadas a un módulo 124 de procesamiento de imagen. La imagen digital capturada también puede ser almacenada en una base de datos en el procesador de autenticación. El módulo 124 de procesamiento de imagen puede adaptarse para realizar cualquier procesamiento requerido antes de que la imagen digital capturada pueda ser de codificada digitalmente. Esto puede incluir identificar puntos de referencia en el área objetivo y orientar la imagen digital capturada de forma correspondiente.

El procesador 120 de autenticación también incluye un módulo 126 de decodificación y un módulo 128 de autenticación. El módulo 126 de decodificación puede estar programado con un software de codificación digital adaptado para realizar uno o más algoritmos de decodificación en la imagen digital capturada para producir un resultado de decodificación. El módulo 126 de decodificación puede obtener a partir de la base de datos de información de codificación cualquier información (por ejemplo, la imagen de autenticación y los parámetros de codificación) necesaria para decodificar la imagen codificada capturada. El resultado de decodificación se puede hacer pasar al módulo 128 de autenticación que compara el resultado de decodificación con uno o más criterios de autenticación para establecer un resultado de autenticación. El resultado de decodificación, el resultado de autenticación o ambos pueden almacenarse en la memoria, o en una base de datos local o remota, o mostrarse para el uso a un inspector en el lugar u otro usuario.

Los componentes del sistema 100 de autenticación pueden estar interconectados a través de cualquier medio adecuado incluyendo mediante una red. El procesador 120 de autenticación puede tomar la forma de un dispositivo de procesamiento portátil que se puede transportar por un inspector individual junto con un dispositivo de adquisición

de imágenes de mano (por ejemplo, un escáner portátil o una cámara digital). En algunos modos de realización de la invención, el dispositivo de adquisición de imagen y el procesador de autenticación pueden realmente estar integrados en una sola unidad. De forma alternativa, un inspector puede trasportar sólo un dispositivo 110 de adquisición digital que se puede conectar de forma selectiva a un procesador 120 de autenticación ubicado remotamente. Por ejemplo, un dispositivo de escaneado puede estar configurado para enviar una imagen capturada al procesador de autenticación mediante un correo electrónico. En otro ejemplo, un teléfono inalámbrico con capacidad de tomar imágenes se puede utilizar para capturar una imagen y reenviar la al procesador de autenticación mediante una red de telecomunicaciones. Una aplicación práctica de este aspecto es un escenario en el cual un comprador potencial de un producto captura una imagen de producto utilizando un teléfono con cámara y envía por teléfono una petición de autenticación a un procesador de autenticación. El resultado de autenticación podría retornarse al solicitante mediante la red telefónica en, por ejemplo, un mensaje de texto.

El sistema 100 de autenticación se adapta bien para el uso en la autenticación de un gran número de objetos similares tales como, por ejemplo, objetos envasados en un almacén o gran número de documentos similares. El procesador 120 de autenticación puede estar adaptado de manera que la información que se refiere a objetos individuales pueda ser introducida o derivada de la imagen digital capturada. Esto permite la asociación de la imagen digital capturada con el objeto particular. Esto, a su vez, permite la recuperación de la información de codificación específica del objeto, que puede ser requerida para decodificar la imagen codificada capturada o para determinar el resultado de autenticación.

Se entenderá que si la información de codificación no es específica del objeto, un grupo de objetos de prueba con la misma imagen codificada esperada se puede autenticar mediante el procesador 120 de autenticación utilizando un único conjunto de información de codificación. Este conjunto de información de codificación se puede obtener a partir de la base 130 de datos de información de codificación una vez y almacenarse en la memoria del procesador 120 de autenticación donde es accesible a los módulos 126, 128 de decodificación y de autenticación.

Las funciones del procesador de autenticación no necesitan ser llevadas a cabo en un único dispositivo de procesamiento. Pueden, en su lugar ser distribuidas entre una pluralidad de procesadores, que se pueden interconectar mediante una red. Además, la información de codificación requerida para decodificar las imágenes codificadas capturadas tomadas de los objetos de prueba y los resultados de decodificación y de autenticación pueden almacenarse en bases de datos que son accesibles para varios usuarios a lo largo de la misma o una red diferente. Con referencia la figura 4, un sistema 200 de autenticación comprende uno o más procesadores 220 de inspección, un servidor 240 de autenticación y un servidor 250 de base de datos en comunicación selectiva entre sí a través de una o más redes 230, 270, 280.

Cada procesador 220 de inspección está en comunicación con uno o más dispositivos 210 de adquisición de imagen asociados adaptados para capturar imágenes digitales de al menos una porción de los objetos de prueba que se van a autenticar. Cada procesador 220 de inspección puede incluir un módulo 222 de recepción de imagen adaptado para recibir imágenes digitales capturadas desde el dispositivo 210 de adquisición de datos. El procesador 220 de inspección también puede incluir un módulo 224 de transmisión de datos adaptado para transmitir una petición de autenticación que incluye la imagen digital capturada al servidor 240 de autenticación mediante una primera red 280. De forma alternativa, el módulo de transmisión puede transmitir la imagen digital capturada al servidor 250 de base de datos para una autenticación posterior. El procesador 220 de inspección puede estar configurado para la introducción de datos asociados con el objeto del cual se ha capturado una imagen digital particular. De forma alternativa, el procesador de inspección puede estar provisto con un software para el procesamiento de la imagen digital capturada para identificar y almacenar información relacionada con el objeto. Por ejemplo, la imagen digital capturada puede incluir indicios reconocibles tal como un código de barras o identificador numérico que se pueden decodificar para proporcionar información referente al objeto.

El procesador 220 de dispersión puede, opcionalmente, incluir sus propios módulos de procesamiento de imagen, de codificación y autenticación similares a los descritos previamente para el procesador 120 de autenticación del sistema 100 de autenticación. Los resultados de decodificación y autenticación producidos por el procesador de inspección se pueden comparar con los resultados obtenidos del servidor de autenticación o se pueden almacenar para un uso posterior. Para facilitar la decodificación de imagen, el procesador 220 de inspección puede estar configurado para recuperar parámetros de codificación y/o imágenes de autenticación del servidor 250 de base de datos mediante una segunda red 230, que puede ser la misma que la primera red 280.

El módulo 224 de transmisión se puede adaptar para trasmitir la petición de autenticación mediante la primera red 280. Adicionalmente a la imagen digital capturada, la petición de transmisión puede incluir información adicional asociada con el objeto del cual se capturó la imagen digital. Esto puede incluir cualquier resultado de decodificación o autenticación producido por el procesador 220 de inspección. La imagen digital capturada y cualquier información asociada se pueden trasmitir directamente al servidor 240 de autenticación o se pueden almacenar temporalmente en el servidor 250 de base de datos u otro servidor para un acceso posterior mediante el servidor 240 de autenticación. La petición de autenticación también puede incluir información adicional tal como información referente al procesador de inspección particular y/o al inspector/usuario, información de seguridad del usuario (por ejemplo, nombre de usuario y contraseña), la ubicación del lugar de inspección, etcétera.

El servidor 240 de autenticación puede comprender un módulo 242 de recepción de datos configurado para recibir la imagen digital capturada y la información asociada del procesador 220 de inspección. El módulo 242 de recepción de datos puede, de forma alternativa o adicionalmente estar configurado para recuperar dicha información del servidor 250 de base de datos mediante la segunda red 230 o una red diferente. El módulo 242 de recepción de datos se puede adaptar para verificar las credenciales de usuario y proporcionar una confirmación de petición de vuelta al procesador de dispersión. El módulo 242 de recepción de datos también puede estar configurado para transmitir una denegación de la petición de autenticación si las credenciales de usuario o la información de seguridad proporcionada indican que la petición no cumple criterios de autorización predeterminados.

El servidor 240 de autenticación incluye módulos 244, 246, 248 de procesamiento de imagen, de codificación y autenticación similares a los descritos previamente para el procesador 120 de autenticación del sistema 100 de autenticación. Tras establecer que la petición de autenticación se obtuvo de un usuario autorizado y está asociada con el objeto para el cual está disponible la información de codificación asociada, el módulo de recepción de datos pasa la imagen digital capturada al módulo 244 de procesamiento de imagen para iniciar el proceso de decodificación. Uno o más de los módulos 242, 244, 246, 248 de servidor de autenticación se pueden adaptar para recuperar información almacenada en el servidor 250 de base de datos. El servidor 250 de base de datos puede incluir un servidor 252 de información de codificación, en la cual se pueden almacenar alguna o todas las imágenes de autenticación y los parámetros de codificación utilizados para codificar la imagen de autenticación asociada con los objetos que están siendo autenticados. Se entenderá que la información de codificación se puede almacenar para un gran número de objetos que se pueden autenticar no relacionados y grupos de objetos para una variedad de usuarios de cliente. La información es recuperada basándose en la información de objeto proporcionada con la petición de autenticación o derivada de la propia imagen digital capturada. La información recuperada se puede utilizar por el módulo 246 de decodificación para producir un resultado de decodificación y mediante el módulo 248 de autenticación para producir un resultado de autenticación.

El servidor 240 de autenticación puede también comprender un módulo 249 de trasmisión de resultado adaptado para ensamblar y transmitir una respuesta de petición de autenticación que incluye el resultado de autenticación en algunos modos de realización, la respuesta de petición puede también incluir el resultado de decodificación y/u otra información relacionada con el objeto. La respuesta de petición se puede transmitir al procesador 220 de inspección u otro receptor designado previamente a través de la primera red 280. El resultado de autenticación, el resultado de decodificación o ambos pueden de forma alternativa o adicionalmente ser transmitidos mediante la segunda red 230 para el almacenamiento en una base 254 de datos de autenticación. La base 254 de datos de autenticación puede residir en el servidor 250 de base de datos u otro servidor conectado a la red 230. La base 254 de datos de autenticación puede ser accesible selectivamente a uno o más procesadores 260 de monitorización de autenticación mediante una tercera red 270. Esto permite a los usuarios autorizados acceder a la base de datos de autenticación para monitorizar información y estadísticas de autenticación individuales y acumulativas.

Se entenderá que las redes 230, 270 y 280 pueden ser las mismas o redes diferentes. Cualquiera o todas ellas pueden ser cualquier forma de red local o de área amplia. Cualquiera o todas pueden, por ejemplo, ser o incluir Internet para permitir un gran número de usuarios extendidos. La red 280 puede también ser una red de telecomunicaciones sobre la cual se pueden transmitir imágenes digitales desde los dispositivos de adquisición de imagen tal como teléfonos con cámara. También se entenderá que los módulos y funciones para el servidor 240 de autenticación se pueden distribuir entre múltiples servidores y procesadores interconectados.

Los sistemas de autenticación de la invención son altamente flexibles y se pueden utilizar en una amplia variedad de escenarios de autenticación. En un escenario típico, una imagen de autenticación codificada es aplicada al envase de un producto de un fabricante cliente que está sujeto a una falsificación o alteración. Un inspector en el lugar equipado con un procesador de inspección portátil y un dispositivo de adquisición de imagen puede ser enviado a un lugar tal como un almacén donde está almacenado un grupo de productos envasados. El inspector puede utilizar el dispositivo de adquisición de imagen para escanear o de otro modo capturar una imagen digital de un área objetivo de un envase del producto sospechoso. Información adicional tal como la fecha, la hora, la ubicación, el número de serie del producto, etcétera se pueden introducir por el inspector. Alguna de esta información puede ser introducida de forma alternativa automáticamente mediante el procesador de inspección. Si el procesador de inspección está equipado con su propio software de decodificación y autenticación, el inspector puede autenticar el producto sospechoso inmediatamente. De forma alternativa o adicionalmente, el procesador de inspección puede ser utilizado para enviar una petición de autenticación a un servidor de autenticación remoto. Las peticiones de autenticación pueden enviarse en una base de artículo individual. De forma alternativa, las imágenes de autenticación capturadas y la información de producto asociado se pueden recoger para múltiples objetos de prueba y enviar como parte de una petición de autenticación única. Esto podría permitir, por ejemplo, al procesador de inspección ser utilizado independientemente de una conexión de red para recoger datos de autenticación de una pluralidad de artículos de prueba, después conectarse a la red (por ejemplo, accediendo a un sitio web de Internet) para enviar una petición de autenticación en un lote único.

Tras recibir la petición de autenticación del procesador de inspección, el servidor de autenticación valida la petición, recupera cualquier información de codificación imagen requerida de la base de datos de información de codificación y procesa la imagen digital capturada. La imagen capturada es decodificada y comparada con los criterios de autenticación recuperados para determinar un resultado de autenticación. El resultado de autenticación es después

almacenado en la base de datos de autenticación. Un representante del fabricante u otro usuario autorizado es entonces capaz de acceder a los resultados de autenticación conectándose a la base de datos de autenticación. En algunos modos de realización esto se puede lograr accediendo a un sitio web controlado por seguridad y enviando una petición para los resultados de autenticación para los objetos de prueba.

En algunos modos de realización, el servidor de autenticación puede estar configurado para accederse a través de un sitio web. Usuarios autorizados pueden iniciar sesión en el sitio web, cargar imágenes descargadas y recibir inmediatamente un resultado de autenticación en su navegador. Los resultados se pueden también almacenar en una base de datos de autenticación para futuras revisiones.

En algunos modos de realización, se puede implementar un servicio de autenticación basado en la web utilizando estándares para la interfaz y la representación de datos, tal como SOAP y XML, para permitir a terceras partes conectar sus servicios de información y de software al servicio de autenticación. Este enfoque podría permitir un flujo ininterrumpido de petición/respuesta de autenticación entre diversas plataformas y aplicaciones de software.

Tal y como se expuso anteriormente, las funciones de los sistemas de autenticación y las acciones de los métodos de autenticación de la invención se pueden llevar a cabo utilizando un único procesador de datos o se pueden distribuir entre múltiples procesadores interconectados. En algunos modos de realización, por ejemplo, las funciones de decodificación y autenticación se pueden llevar a cabo mediante diferentes procesadores. Aspectos de funciones de decodificación en sí misma se pueden llevar a cabo utilizando un único procesador o una pluralidad de procesadores conectados en red.

Las figuras 5-7 ilustran sistemas típicos para la decodificación de acuerdo con la invención. Con referencia a la figura 5, un sistema 300 para una decodificación digital de una imagen digital capturada es un sistema independiente que puede comprender un único procesador 310 de decodificación y un dispositivo 320 de adquisición de imagen. El procesador 310 de decodificación está configurado para recibir imágenes digitales capturadas desde el dispositivo de adquisición de datos y procesar las tal y como se requiera para proporcionar un resultado de decodificación. El procesador 310 de decodificación puesta configurado con el software requerido para aplicar una metodología digital de decodificación particular. Algo o toda la información de codificación requerida por el software de decodificación se puede almacenar en el procesador 310 de decodificación y/o puede ser proporcionada por un usuario.

El procesador 310 de decodificación incluirá típicamente una pantalla o una impresora que permite al usuario del sistema 300 de decodificación independiente escanear un envase o documento e inmediatamente ver el resultado decodificado. El resultado se puede almacenar o se puede utilizar únicamente como un sistema de inspección “in situ” en el cual se puede descartar el resultado después de ser visto por el usuario/inspector.

Otro enfoque del sistema de decodificación proporciona la recopilación de imágenes capturadas múltiples e información de artículo asociada, que se pueden después enviar en un lote a un procesador o servidor de decodificación centralizada. Con referencia la figura 6, un sistema 400 de decodificación de este tipo puede comprender una o más estaciones de intención, cada una que tiene un dispositivo 420 de adquisición de imagen en comunicación con un procesador 410 de inspección que tiene una aplicación de procesamiento de imagen residente en el mismo. En un modo de realización típico, el dispositivo 420 de adquisición de imagen puede ser un escáner y la aplicación de procesamiento de imagen está configurada para recibir imágenes escaneadas del escáner. Las imágenes escaneadas se pueden transmitir individualmente o de forma colectiva a un procesador 430 de recopilación de datos. El procesador 430 de recopilación de datos puede estar en comunicación selectiva con el procesador 410 de inspección mediante una red. En algunos modos de realización, el procesador 410 de inspección puede estar configurado para recopilar y enviar una pluralidad de imágenes e información de objeto asociada al mismo tiempo al procesador 430 de recopilación de datos.

Las imágenes escaneadas pueden ser transferidas junto con la información referente al objeto o al documento escaneado. El procesador 430 de recopilación de datos puede estar adaptado para recibir imágenes capturadas e información de objeto asociada de cualquier número de procesadores 410 de inspección. Las imágenes capturadas y la información de objeto asociada se pueden recopilar y enviar al mismo tiempo a un procesador o servidor 450 de decodificación mediante una red 440. En un modo de realización particular la red 440 es Internet y el procesador 450 de decodificación es accedido a través de una página web. Los resultados de decodificación producidos por el procesador 450 de decodificación pueden ser accedidos mediante un procesador 470 de monitorización mediante una segunda red 460 que puede ser la misma que la primera red 440.

En un escenario típico para utilizar un sistema 400 de decodificación, los inspectores escanean etiquetas de un envase o documentos utilizando los dispositivos 420 de adquisición de imagen y proporcionan información apropiada (por ejemplo, la ubicación donde se recogió el envase, la fecha y la hora, el número de serie del producto, etcétera) para cada imagen capturada. Al final de la jornada de trabajo, las imágenes escaneadas y los datos correspondientes son enviados por lotes al procesador 450 de decodificación, donde son decodificados. Los resultados de decodificación se pueden almacenar en el procesador de decodificación o en una base de datos separada. Los resultados de decodificación se hacen accesibles a procesadores 470 de monitorización autorizados. En un modo de realización particular, los resultados de decodificación se pueden recibir mediante Internet o pueden verse utilizando un navegador

web, que muestra todas las imágenes escaneadas y codificadas, así como otros datos proporcionados por los inspectores en el momento del escaneado.

La separación de la recopilación y decodificación de datos permite una recopilación de información distribuida y una decodificación basada en la web centralizada. Esto también permite un almacenamiento centralizado de los resultados de decodificación y facilita la autenticación automatizada. Los resultados se pueden compartir entre miembros de un grupo de usuarios específico (por ejemplo, un equipo de protección de marca) y se pueden realizar por su dirección. El análisis de los resultados acumulativos puede ayudar en la detección de tendencias de facilitación globales y locales. También puede proporcionar una visión de la eficiencia de las medidas disuasorias actuales en diferentes mercados. Otra ventaja de la separación e independencia de las operaciones de recopilación y decodificación de datos es que los clientes pueden alquilar a contratistas para el escaneado de envases en ciertos mercados, sin revelar información detallada sobre características antifalsificación del envase. Adicionalmente, los inspectores no necesitan un acceso a la red ininterrumpido, sólo necesitan conectarse al procesador de decodificación de forma ocasional (por ejemplo, al final de la jornada de trabajo o de la semana de trabajo).

En algunos casos, sin embargo, un inspector puede necesitar autenticar un único artículo. Si el acceso a la red está disponible en el momento que se captura la imagen, el enfoque distribuido para la recopilación de datos puede retrasar de forma innecesaria la decodificación y la autenticación. Además, el enfoque distribuido puede requerir la presencia de un software dedicado para adaptarse a múltiples cargas de archivos desde el procesador del cliente al procesador central y asegurar la integridad de este intercambio de datos. Un modelo alternativo para una funcionalidad de decodificación única es una aplicación de red que proporciona una subida de un único archivo escaneado para decodificar y recibir inmediatamente y mostrar una imagen decodificada. Este modelo es particularmente útil en el contexto de un sistema basado en Internet en el cual el inspector inicia sesión en el sitio web de decodificación utilizando un navegador web. Utilizando el sitio web, el inspector puede cargar una imagen capturada única y recibir/mostrar un resultado de decodificación en su navegador. Este enfoque se puede utilizar ampliamente por individuos que necesitan autenticar un único producto envasado. Se podría utilizar, por ejemplo, por un farmacéutico que quiere autenticar un único en base de medicamentos, o un examinador forense que quiere comprobar un billete de banco único o tarjeta de identificación. El único equipo requerido podría ser un escáner (u otro dispositivo de adquisición de imágenes) y un ordenador que se pueda conectar a Internet, una intranet u otra red de comunicaciones a través de la cual se puede acceder al servidor/procesador de decodificación.

La figura 7 ilustra un sistema 500 de decodificación basado en red de acuerdo con un modo de realización de la invención. El sistema 500 de decodificación puede incluir uno o más procesadores 510 de inspección en comunicación selectiva con el servidor 540 de decodificación mediante una red 530. Cada procesador 510 de inspección puede tener un dispositivo 520 de adquisición de imagen para capturar imágenes digitales y transferirlas al procesador 510 de inspección. Se entenderá que el dispositivo 520 de adquisición de imagen y el procesador 510 de inspección se pueden combinar en una única unidad de procesamiento. En un modo de realización típico, el dispositivo 520 de adquisición de imagen es un escáner y el procesador 510 de inspección está configurado para recibir una imagen escaneada del escáner y cargarla de forma selectiva en el servidor 540 de decodificación.

La red 530 puede ser cualquier red de comunicaciones tal como Internet, una intranet, o una red móvil o de otras telecomunicaciones. En un modo de realización particular del sistema 500 de decodificación, la red 530 es Internet y el procesador 510 de inspección está equipado con un navegador web para establecer una comunicación con el servidor 540 de decodificación a través de un sitio web administrado por el servidor 540 de decodificación. Esto proporciona la capacidad de un proceso de decodificación basado en la web interactiva en el cual una imagen digital capturada es cargada en el servidor 540 de decodificación donde es procesada para proporcionar un resultado de decodificación. El resultado de decodificación es después devuelto al procesador de inspección para su visualización o impresión.

El servidor 540 de decodificación puede incluir o tener acceso a una o más bases de datos en las cuales se almacena la información de codificación para el uso en la aplicación de una metodología de decodificación apropiada para un usuario particular. Esta información puede ser asociada previamente con una línea de producto o incluso productos o documentos específicos. La información de usuario y/o las reglas de acceso también se pueden almacenar de manera que el servidor 540 de decodificación pueda determinar si un usuario particular tiene derecho a iniciar sesión en el sistema o a recibir un resultado de decodificación particular.

Un método para proporcionar un servicio de decodificación de imagen digital en una sesión basada en la red interactiva es ilustrado en la figura 8. El método comienza en S200. En S210 una página de conexión es transmitida al procesador de inspección para mostrar sea través de un navegador web o una aplicación similar. En S220, se recibe una petición de conexión del procesador de inspección. La petición de conexión puede incluir un nombre de usuario y una contraseña y/u otra información de usuario requerida. En S230, la información de conexión es revisada para determinar si el conexión es válido y si se debería establecer una sesión de codificación. Si la información de conexión no está asociada con una cuenta de usuario válida o la información de seguridad asociada no corresponde a la información para el usuario especificado, el método procede a S232 donde se realiza una comprobación para determinar si se ha alcanzado un número predeterminado de fallos de conexión consecutivos. Si no es así, se puede transmitir un mensaje de error y el método vuelve a S210. El límite de fallo predeterminado ha sido alcanzado, la cuenta de usuario es bloqueada en S234 y el método finaliza en S236.

Si se recibe una conexión válida, el método procede a S240 donde se obtiene información de codificación basándose en la información asociada con la cuenta de usuario y/o información suministrada por el usuario de forma interactiva. La información suministrada por el usuario puede, por ejemplo, incluir una identificación del producto o documento. La información de codificación se puede obtener a partir de una base de datos en la cual dicha información está asociada con el usuario y/o la información del producto. También se puede incluir cierta información de codificación en la información suministrada por el usuario.

La información suministrada por el usuario puede ser incluida en una petición de conexión o puede ser proporcionada en respuesta a avisos transmitidos al procesador de inspección del usuario. En un modo de realización particular, el servidor de codificación puede tener almacenado en el mismo o puede tener acceso a una o más configuraciones de decodificación que han sido asociadas previamente con el usuario o la clase de usuario. Estas configuraciones de decodificación representan opciones que se pueden utilizar para decodificar imágenes capturadas de productos, documentos u otros objetos diferentes. Tras validar la conexión de un usuario particular, el servidor de decodificación puede recuperar una lista de las configuraciones de decodificación asociadas con el usuario y trasmitir la lista al procesador de inspección para mostrarla al usuario. El usuario puede después seleccionar la configuración de decodificación apropiada para el objeto que ha sido capturado en la imagen digital que se va a decodificar. Tras recibir la selección de usuario, el procesador de decodificación puede después obtener la información de codificación necesaria para decodificar la imagen capturada.

Una configuración de decodificación particular puede requerir que la imagen digital sea capturada de una manera particular. Por ejemplo, puede ser necesario que la imagen pueda ser escaneada en una orientación particular. Por consiguiente, en S250, se pueden transmitir opcionalmente instrucciones de escaneado al procesador de inspección para su visualización. El usuario puede después escanear o de otro modo capturar la imagen digital de la manera apropiada y cargarla en el servidor de decodificación.

En S260, el archivo de la imagen digital capturada es recibido del usuario/solicitante de decodificación. En S270, la información decodificación y la metodología de codificación apropiada son utilizadas para procesar la imagen digital capturada y obtener un resultado de decodificación. En S280, el resultado de decodificación es transmitido al usuario donde se puede mostrar o imprimir. Cualquier número de imágenes adicionales se puede cargar y decodificar en una sesión interactiva particular. En S290, una petición de cierre de sesión es recibida y el método finaliza en S299.

Se entenderá fácilmente por los expertos en la técnica que la presente invención es susceptible de ampliar la utilidad y la aplicación. Muchos modos de realización y adaptaciones a la presente invención diferentes de las descritas en el presente documento, así como muchas variaciones, modificaciones y disposiciones y equivalentes serán evidentes a partir de o sugeridas de forma razonable por la presente invención y la descripción anterior de la misma, sin alejarse de la esencia o alcance de la invención.

Aunque lo anterior ilustra y describe modos de realización de ejemplo de esta invención, se ha de entender que la invención no está limitada a la constitución divulgada en el presente documento. La invención se puede implementar de otras formas específicas sin alejarse de su alcance tal y como se define en las reivindicaciones adjuntas.

REIVINDICACIONES

1. Un método (M100) implementado por ordenador para determinar si un objeto de prueba es un objeto auténtico en el cual se ha aplicado una imagen codificada esperada, el objeto de prueba que es un documento, un envase, o artículos, la imagen codificada esperada que ha sido constituida mediante la codificación de una imagen de autenticación utilizando uno de una pluralidad de conjuntos de información de codificación, cada conjunto de información de codificación que comprende uno o más parámetros de modificación que proporciona desviaciones de un comportamiento periódico regular y hace que la imagen de autenticación no sea discernible para un visor de la imagen codificada esperada sin el uso de un dispositivo de decodificación, el método que comprende:

recibir (S120) una imagen digital de al menos una porción del objeto de prueba, la imagen digital que incluye la imagen codificada esperada generada utilizando uno de la pluralidad de conjuntos de información de codificación;

caracterizado por introducir o derivar (S130) una información de objeto de prueba de la imagen digital, la información de objeto de prueba que está siendo utilizada para asociar la imagen digital con el objeto de prueba a partir del cual se capturó la imagen digital;

recuperar (S130), basándose en la información del objeto de prueba, un conjunto específico del objeto de prueba de la pluralidad de conjunto de información decodificación de una base (130, 252) de datos de información de codificación que almacena la pluralidad de conjuntos de información de codificación, el conjunto específico de objeto de prueba de la pluralidad de conjuntos de información decodificación que está asociado con el objeto de prueba; y

utilizar uno o más parámetros de codificación del conjunto de información decodificación específico del objeto de prueba para obtener un algoritmo de decodificación digital, aplicando (S150) el algoritmo de decodificación digital a la imagen digital para establecer un resultado de decodificación para la comparación (S160) con criterios de autenticación del objeto auténtico para establecer un resultado de autenticación (S170).

2. Un método de acuerdo con la reivindicación 1, que además comprende:

almacenar uno o más parámetros de codificación correspondientes a la pluralidad de conjuntos de información de codificación en un servidor (126, 246) de decodificación; y recibir la imagen digital de un procesador (220) de inspección mediante una red (230, 280).

3. Un método de acuerdo con la reivindicación 2, en donde la red (230, 280) es Internet.

4. Un método de acuerdo con la reivindicación 2, en donde la red (230, 280) es una red de telecomunicaciones.

5. Un método de acuerdo con la reivindicación 1, que además comprende:

almacenar los criterios de autenticación del objeto auténtico en un servidor (240) de autenticación; y recibir la imagen digital de un procesador (220) de inspección mediante una red (230, 280).

6. Un método de acuerdo con la reivindicación 5, en donde la imagen digital es recibida con una petición para la autenticación del objeto de prueba.

7. Un método de acuerdo con la reivindicación 6, en donde la petición para la autenticación incluye al menos una de, la información de objeto de prueba, la información de procesador de inspección, la información del solicitante, la información de nombre de usuario y contraseña, y la información de la ubicación de la inspección.

8. Un método de acuerdo con la reivindicación 1 que además comprende:

extraer indicios decodificados del resultado de decodificación.

9. Un método de acuerdo con la reivindicación 8 en donde la acción de comparar los resultados de decodificación incluye:

recuperar una imagen de autenticación de la base (130, 252) de datos de información de codificación; y comparar los indicios decodificados con los indicios de imagen de autenticación.

10. Un método de acuerdo con la reivindicación 8, en donde la acción de comparar incluye:

comparar los indicios decodificados con la información específica del objeto de prueba.

11. Un método de acuerdo con la reivindicación 10, en donde la información específica del objeto de prueba es recibida con la imagen digital.

12. Método de acuerdo con la reivindicación 10, en donde la información específica del objeto de prueba es recuperada de al menos una de, una base de datos, una tarjeta inteligente, una banda magnética, un código de barras, un chip de procesador, y un chip de memoria.

13. Un método de acuerdo con la reivindicación 10 en donde la información específica del objeto de prueba es extraída de la imagen digital.

14. Un método de acuerdo con la reivindicación 1 que además comprende:

almacenar en una base (254) de datos de autenticación al menos uno de, el resultado de decodificación y el resultado de autenticación.

15. Un método de acuerdo con la reivindicación 1, que además comprende:

recibir una petición de resultado para el resultado de autenticación de un procesador (260) de monitorización;

determinar si la petición de resultado es válida; y

en respuesta a una determinación de que la petición de resultado es válida, transmitir el resultado de autenticación al procesador de monitorización.

16. Un método de acuerdo con la reivindicación 15, en donde la petición de resultado es recibida del procesador (260 de monitorización y el resultado de autenticación es transmitido al procesador de monitorización mediante una red (270).

17. Un método de acuerdo con la reivindicación 16, en donde la red (270) es Internet.

18. Un sistema (100, 200, 300, 400) para determinar si un objeto de prueba es un objeto auténtico sobre el cual se ha aplicado una imagen codificada esperada, el objeto de prueba que es un documento, un envase o artículos, la imagen codificada esperada que ha sido constituida mediante la codificación de una imagen de autenticación utilizando uno de una pluralidad de conjuntos de información de codificación, cada conjunto de información de codificación que comprende uno o más parámetros de codificación que proporcionan desviaciones de comportamiento periódico regular y hacen que la imagen de autenticación no sea discernible para un usuario de la imagen de codificación esperada sin el uso de un dispositivo de decodificación, el sistema que comprende:

un dispositivo (110, 210, 320, 420) de adquisición de imagen digital adaptado para capturar una imagen digital de al menos una porción del objeto de prueba, la imagen digital que incluye la imagen codificada esperada generada utilizando uno de la pluralidad de conjuntos de información de codificación; y

un sistema de procesamiento de datos que tiene:

un módulo (122, 226) de recepción de imagen adaptado para recibir la imagen digital del dispositivo de adquisición de imagen digital,

una base (130, 252) de datos de información de codificación configurada para almacenar la pluralidad de conjuntos de información de codificación, en donde la pluralidad de conjuntos de información de codificación opcionalmente incluye la imagen de autenticación,

un módulo (126, 246, 310, 450) de decodificación adaptado para recuperar, basándose en la información del objeto de prueba introducida o derivada de la imagen digital del objeto de prueba, la información del objeto de prueba que está siendo utilizada para asociar la imagen digital con el objeto de prueba del cual fue capturada la imagen digital, un conjunto específico del objeto de prueba de la pluralidad de conjuntos de información de codificación de la base de datos de información de codificación, el conjunto específico del objeto de prueba de la pluralidad de conjuntos de información de codificación que está asociado con el objeto de prueba, y adaptado para aplicar un algoritmo de decodificación de imagen codificada utilizando uno o más parámetros de codificación del conjunto de información de codificación específico del objeto de prueba a la imagen digital para producir un resultado de decodificación; y

un módulo (128, 248) de autenticación adaptado para comparar el resultado de decodificación con los criterios de autenticación del objeto auténtico para determinar el resultado de autenticación.

19. Un sistema de acuerdo con la reivindicación 18, en donde el sistema de procesamiento de datos comprende un procesador (220) de datos de inspección que incluye el módulo de recepción de imagen, el procesador de datos de inspección para introducir o derivar la información del objeto de prueba de la imagen digital.

20. Un sistema de acuerdo con la reivindicación 19, en donde el procesador de datos de inspección además incluye el módulo de decodificación y el módulo de autenticación.

21. Un sistema de acuerdo con la reivindicación 19, en donde el procesador (220) de datos de inspección además incluye un módulo (224) de transmisión de datos en comunicación selectiva con una red (280), el módulo (224) de transmisión de datos que está adaptado para transmitir la imagen digital mediante la red, y en donde el sistema de procesamiento de datos además comprende un servidor (240) de autenticación que incluye un módulo (242) de recepción de datos en comunicación selectiva con la red y que está adaptado para recibir la imagen digital del procesador (220) de datos de inspección.

22. Un sistema de acuerdo con la reivindicación 21, en donde el servidor (240) de autenticación incluye al menos uno de, el módulo (246) de decodificación y el módulo (248) de autenticación.

23. Un sistema de acuerdo con la reivindicación 21, en donde el sistema de procesamiento de datos además comprende un servidor (250) de base de datos que incluye la base (252) de datos de información de codificación, el servidor de base de datos que está en comunicación selectiva con la red.

24. Un sistema de acuerdo con la reivindicación 18, que además comprende una base (254) de datos de resultado de autenticación adaptada para el almacenamiento del resultado de autenticación.

25. Un sistema de acuerdo con la reivindicación 24, que además comprende un procesador (260) de monitorización de autenticación en comunicación selectiva con la base (254) de datos de resultado de autenticación mediante una red (270), el procesador de monitorización de autenticación que está adaptado para solicitar y recibir una información de resultado de autenticación del procesador de monitorización de autenticación.

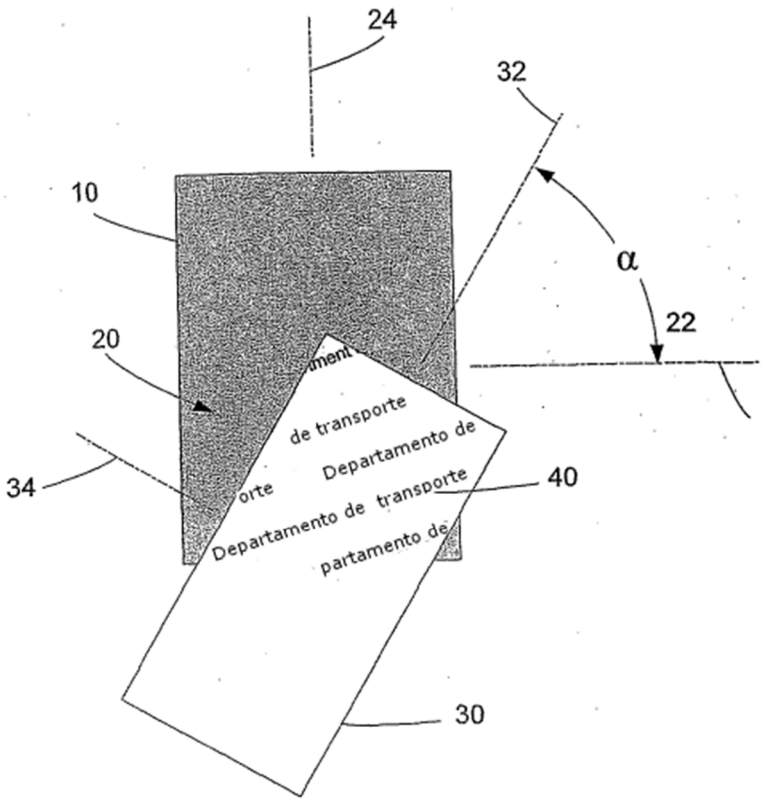
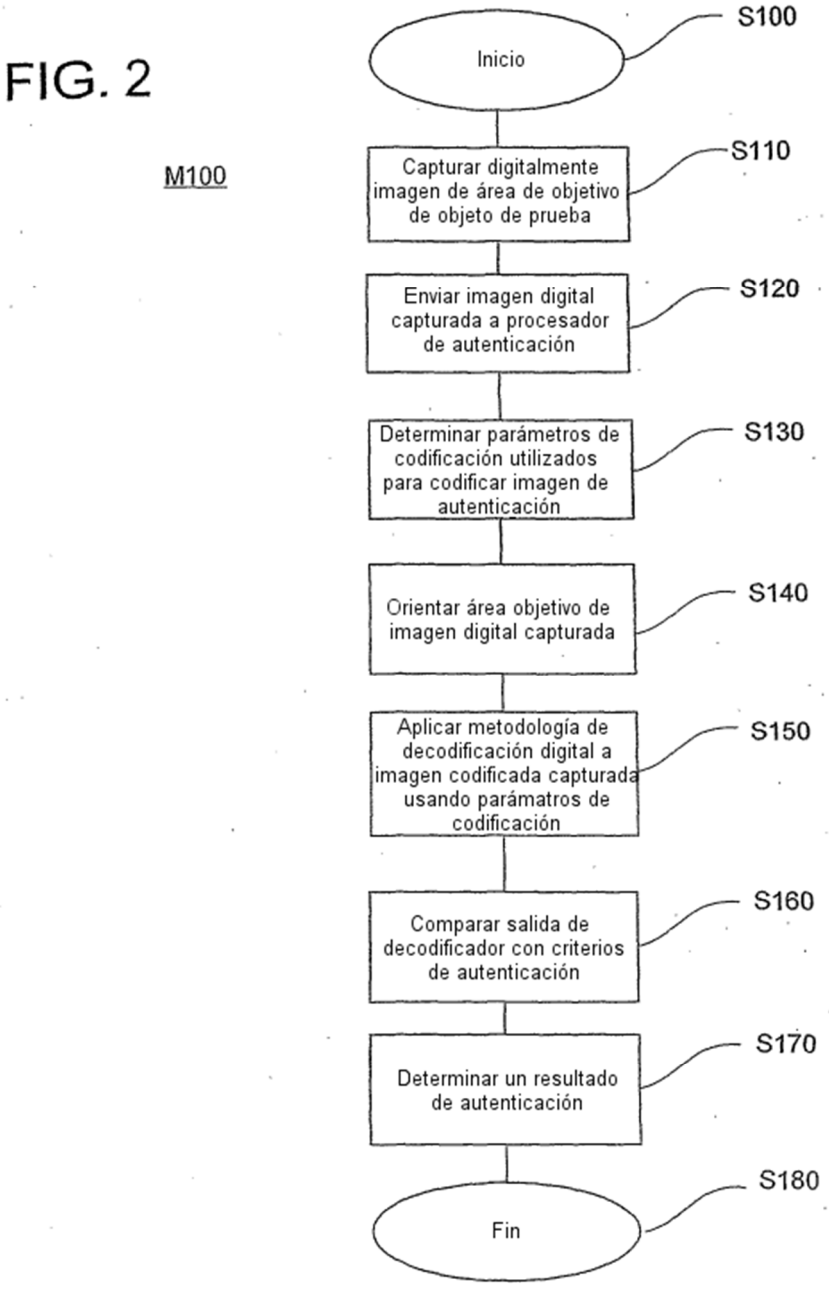

24
32
10
α
22
20
de transporte
Departamento de
Departamento de transporte
40
34
30

FIG. 1

FIG. 2


M100
Inicio
S100
Capturar digitalmente imagen de área de objetivo de objeto de prueba
S110
Enviar imagen digital capturada a procesador de autenticación
S120
Determinar parámetros de codificación utilizados para codificar imagen de autenticación
S130
Orientar área objetivo de imagen digital capturada
S140
Aplicar metodología de decodificación digital a imagen codificada capturada usando parámatros de codificación
S150
Comparar salida de decodificador con criterios de autenticación
S160
Determinar un resultado de autenticación
S170
Fin
S180

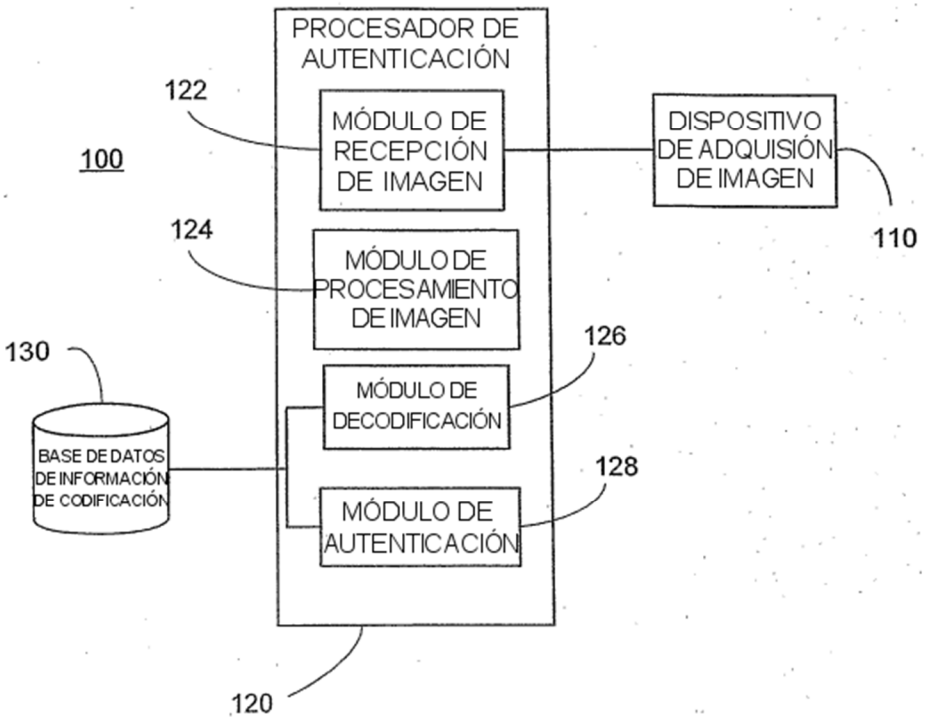

PROCESADOR DE AUTENTICACIÓN
122
100
MÓDULO DE RECEPCIÓN DE IMAGEN
DISPOSITIVO DE ADQUISIÓN DE IMAGEN
110
124
MÓDULO DE PROCESAMIENTO DE IMAGEN
130
126
MÓDULO DE DECODIFICACIÓN
BASE DE DATOS DE INFORMACIÓN DE CODIFICACIÓN
128
MÓDULO DE AUTENTICACIÓN
120

FIG. 3

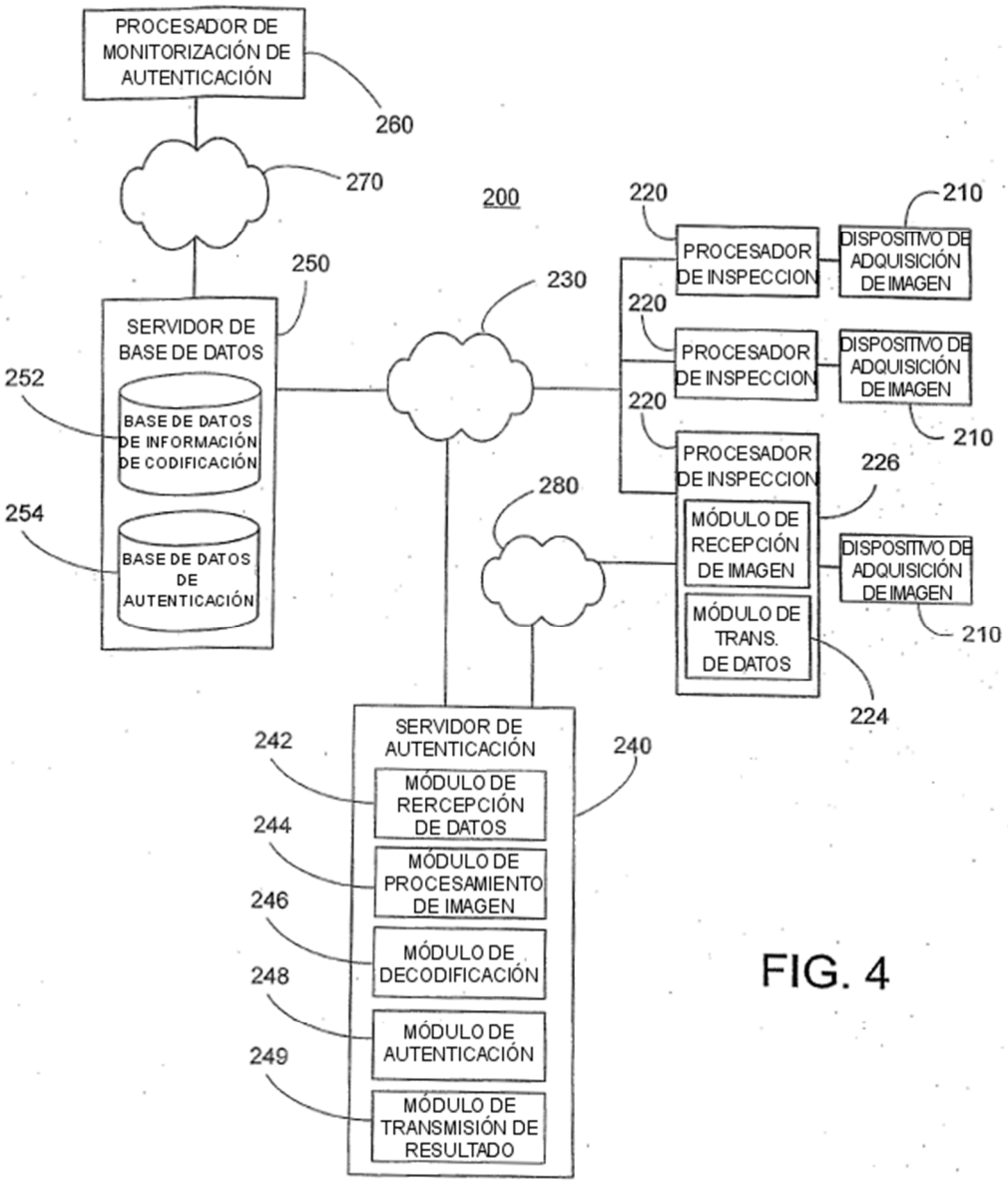

PROCESADOR DE MONITORIZACIÓN DE AUTENTICACIÓN
260
270
200
220
210
PROCESADOR DE INSPECCION
DISPOSITIVO DE ADQUISICIÓN DE IMAGEN
250
230
SERVIDOR DE BASE DE DATOS
252
BASE DE DATOS DE INFORMACIÓN DE CODIFICACIÓN
254
BASE DE DATOS DE AUTENTICACIÓN
280
226
MÓDULO DE RECEPCIÓN DE IMAGEN
MÓDULO DE TRANS. DE DATOS
224
SERVIDOR DE AUTENTICACIÓN
240
242
MÓDULO DE RERCEPCIÓN DE DATOS
244
MÓDULO DE PROCESAMIENTO DE IMAGEN
246
MÓDULO DE DECODIFICACIÓN
248
MÓDULO DE AUTENTICACIÓN
249
MÓDULO DE TRANSMISIÓN DE RESULTADO

FIG. 4

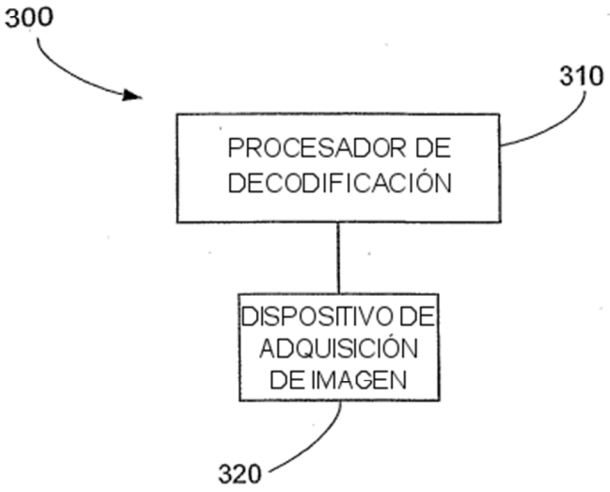

300
310
PROCESADOR DE DECODIFICACIÓN
DISPOSITIVO DE ADQUISICIÓN DE IMAGEN
320

FIG. 5

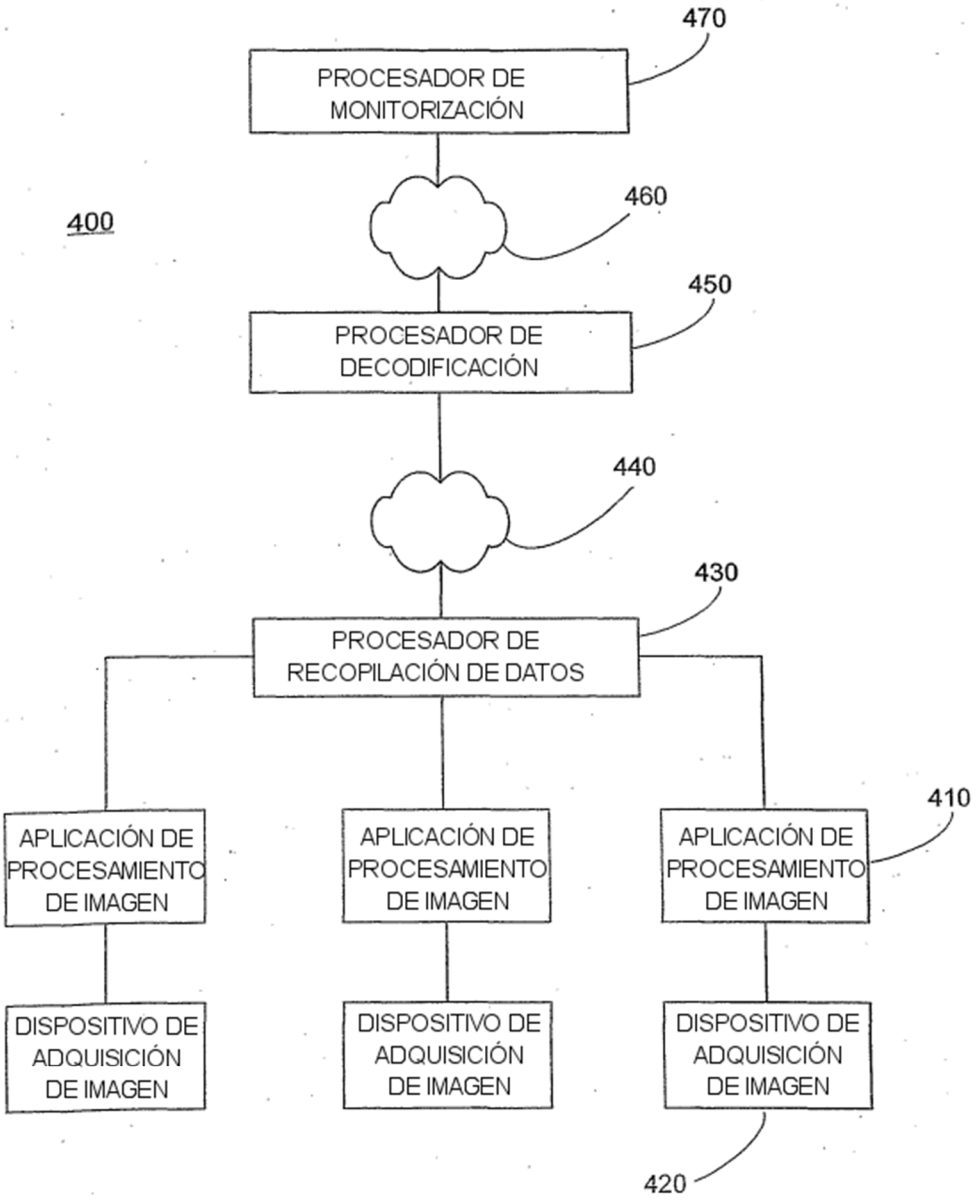

470
PROCESADOR DE MONITORIZACIÓN
460
400
450
PROCESADOR DE DECODIFICACIÓN
440
430
PROCESADOR DE RECOPILACIÓN DE DATOS
410
APLICACIÓN DE PROCESAMIENTO DE IMAGEN
APLICACIÓN DE PROCESAMIENTO DE IMAGEN
APLICACIÓN DE PROCESAMIENTO DE IMAGEN
DISPOSITIVO DE ADQUISICIÓN DE IMAGEN
DISPOSITIVO DE ADQUISICIÓN DE IMAGEN
DISPOSITIVO DE ADQUISICIÓN DE IMAGEN
420

FIG. 6

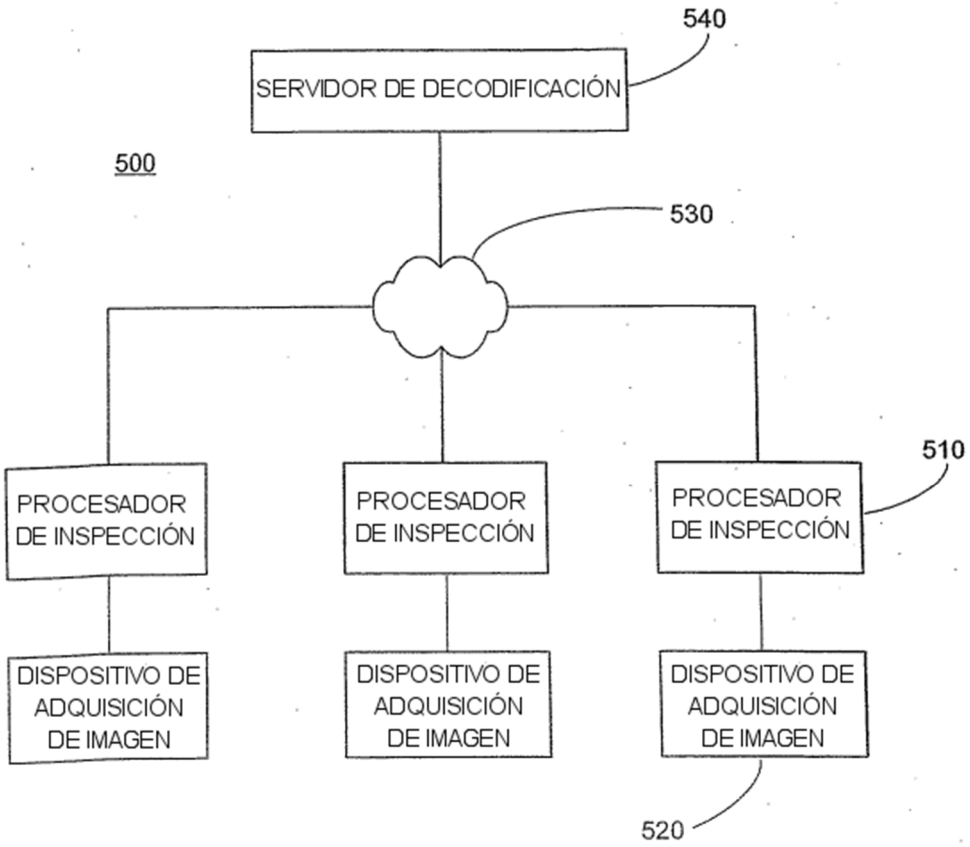

540
SERVIDOR DE DECODIFICACIÓN
500
530
510
PROCESADOR DE INSPECCIÓN
PROCESADOR DE INSPECCIÓN
PROCESADOR DE INSPECCIÓN
DISPOSITIVO DE ADQUISICIÓN DE IMAGEN
DISPOSITIVO DE ADQUISICIÓN DE IMAGEN
DISPOSITIVO DE ADQUISICIÓN DE IMAGEN
520

FIG. 7

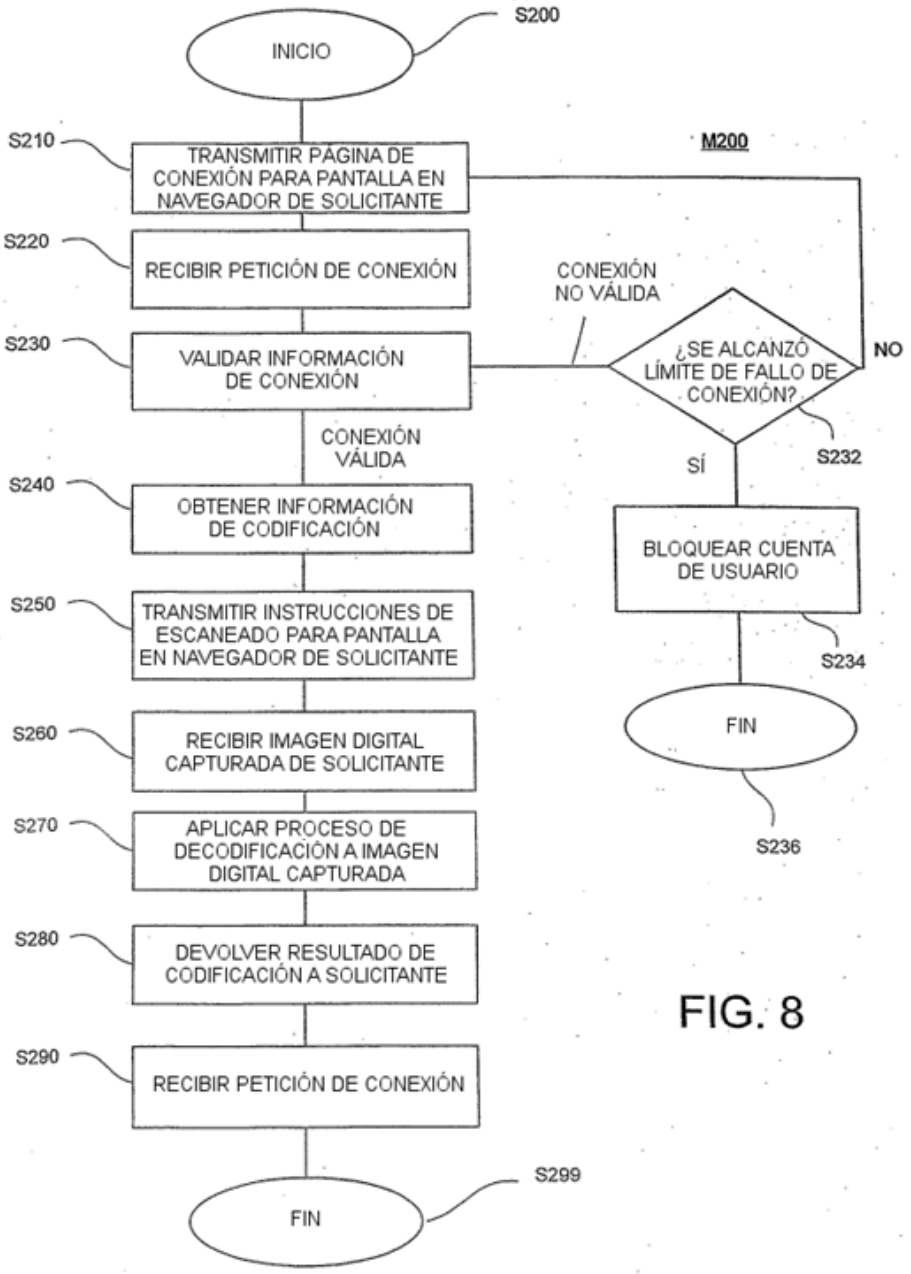

INICIO
S200
S210
TRANSMITIR PÁGINA DE CONEXIÓN PARA PANTALLA EN NAVEGADOR DE SOLICITANTE
M200
S220
RECIBIR PETICIÓN DE CONEXIÓN
CONEXIÓN NO VÁLIDA
S230
VALIDAR INFORMACIÓN DE CONEXIÓN
¿SE ALCANZÓ LÍMITE DE FALLO DE CONEXIÓN?
NO
S232
CONEXIÓN VÁLIDA
SÍ
S240
OBTENER INFORMACIÓN DE CODIFICACIÓN
BLOQUEAR CUENTA DE USUARIO
S250
TRANSMITIR INSTRUCCIONES DE ESCANEADO PARA PANTALLA EN NAVEGADOR DE SOLICITANTE
S234
S260
RECIBIR IMAGEN DIGITAL CAPTURADA DE SOLICITANTE
FIN
S270
APLICAR PROCESO DE DECODIFICACIÓN A IMAGEN DIGITAL CAPTURADA
S236
S280
DEVOLVER RESULTADO DE CODIFICACIÓN A SOLICITANTE
S290
RECIBIR PETICIÓN DE CONEXIÓN
S299
FIN

FIG. 8