(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 424 480**

(51) Int. CI.:

G07D 7/00 (2006.01)

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(96) Fecha de presentación y número de la solicitud europea: **14.05.2003 E 03728904 (8)**

(97) Fecha y número de publicación de la concesión europea: **26.06.2013 EP 1514227**

(54) Título: **Patrones de autenticación visibles para documento impreso**

(30) Prioridad:

14.05.2002 US 380189 P
04.11.2002 US 287206

(45) Fecha de publicación y mención en BOPI de la traducción de la patente:
02.10.2013

(73) Titular/es:

SCHREINER GROUP GMBH & CO. KG (100.0%)
BRUCKMANNRING 22
85764 OBERSCHLEISSHEIM, DE

(72) Inventor/es:

ZHAO, JIAN;
PICARD, JUSTIN y
THORWIRTH, NIELS

(74) Agente/Representante:

CURELL AGUILÁ, Mireia

DESCRIPCIÓN

Patrones de autenticación visibles para documento impreso.

Remisiones a solicitudes relacionadas

La presente solicitud reivindica la prioridad con respecto a la solicitud provisional US 60/380.189, *Method and Apparatus for Copy Protection with Copy-Detectable Patterns*, de los mismos inventores que la presente solicitud y presentada el 14/5/02, y reivindica además prioridad sobre la solicitud USSN 10/287.206, de J. Zhao, *et al.*, *Apparatus and methods for improving detection of watermarks in content that has undergone a lossy transformation*, presentada el 4/11/2002, de la cual es una continuación en parte.

Antecedentes de la invención

1. Campo de la invención

La presente invención se refiere en general a unas características de seguridad de documentos impresos y, más particularmente, a unos patrones de autenticación visibles de documentos impresos. Los patrones de autenticación visibles pueden utilizarse para diferenciar documentos impresos originales de fotocopias de dichos documentos impresos, detectar alteraciones en los documentos y transmitir mensajes ocultos y/o visibles.

2. Descripción de la técnica relacionada

Un requisito indispensable para una sociedad mercantil es la capacidad de diferenciar artículos auténticos de imitaciones o falsificaciones. En el caso de los documentos, las preguntas que posiblemente deban formularse para determinar la autenticidad de un documento comprenden las siguientes:

- ¿Es el documento original o una copia de un original?
- ¿Se ha alterado el documento desde que se creó?
- ¿Está autorizado el documento?

Se han diseñado muchas técnicas para permitir en lo posible responder a estas preguntas a partir del propio documento. Las técnicas que permiten determinar con más facilidad si un documento es original o una copia comprenden los complejos grabados utilizados en papel moneda, las fotografías utilizadas en documentos de identidad y los papeles especiales. Se han utilizado papeles y tintas especiales para detectar alteraciones. Las técnicas para demostrar que un documento está autorizado han comprendido las firmas y los sellos.

Con la llegada de las técnicas de escaneo e impresión digital, se han utilizado *marcas de agua digitales* para autenticar documentos impresos. Una marca de agua digital es un mensaje que se incorpora a una representación digital de un documento añadiendo ruido que transmite el mensaje a un elemento gráfico del documento. Cuando se utiliza con fines de autenticación, el mensaje generalmente es invisible y solo puede leerse si se conoce la ubicación en el elemento gráfico de la información que compone el mensaje. En el Apéndice A, empezando por la línea 27 de la columna 17 de la patente US nº 6.345.104, de Rhoads, *Digital watermarks and methods for security documents*, publicada el 5/2/02, se ofrece un estudio sobre las técnicas de inserción de marcas de agua digitales. Para obtener un ejemplo de cómo pueden utilizarse las marcas de agua digitales con fines de autenticación, puede consultarse la patente US nº 6.243.480, de Jian Zhao, *Digital authentication with analog documents,* publicada el 5/6/01.

Los avances en la tecnología de copia han hecho disminuir el valor de todas las técnicas que permiten determinar la autenticidad de un documento a partir de su aspecto. Debido a este progreso, no solo la falsificación de dinero y de instrumentos financieros, sino también la falsificación de otros documentos, tales como tarjetas de embarque y desembarque y diplomas, así como embalajes y etiquetas, causan pérdidas enormes comprendidas entre el 5 % y el 8 % de las ventas mundiales de productos de marca y ponen en peligro la reputación y el valor de las propias marcas. Por otra parte, el crecimiento de Internet fomenta el negocio de la falsificación de documentos (ID, títulos universitarios, cheques, etc.), que se pueden comprar con facilidad y de forma anónima desde cientos de empresas en la red. Puesto que la precisión de los escáneres, el software de formación de imágenes digitales y las impresoras aumenta cada vez más, el problema no hará más que empeorar.

Para hacer frente al perfeccionamiento de los escáneres, software de formación de imágenes digitales e impresoras, se necesitan nuevas maneras de agregar información a un documento para que sea posible determinar si se trata de un original o una copia, si se ha alterado y/o si está autorizado. Las iniciativas emprendidas en esta área comprenden las siguientes:

Incorporación de varias marcas de agua en un documento

La patente US nº 6.332.031, de Rhoads *et al.*, *Multiple watermarking techniques for documents and other data,* publicada el 18 de diciembre de 2001, da a conocer cómo pueden incorporarse a un documento varias marcas de

agua, cada una de las cuales está dotada de propiedades diferentes o pertenece a dominios diferentes. Si se fotocopia o escanea el documento a fin de crear una falsificación, las marcas de agua incorporadas se alterarán o dañarán. Las propiedades de la marca de agua o el dominio en el cual se ha incorporado ésta, afectará al grado de alteración sufrida debido al procedimiento de copia. Por lo tanto, el grado de alteración relativa de cada marca de agua puede indicar si el documento es original o una copia. El uso de marcas de agua descrito presenta una serie de ventajas:

- Es flexible: en teoría puede insertarse una marca de agua digital en cualquier documento, ya que solo introduce modificaciones imperceptibles en el documento.
- Debido a que son invisibles, pueden utilizarse para determinar el origen de las falsificaciones.
- La posible presencia de marcas de agua obliga al falsificador a reproducir todo el documento con una fidelidad muy alta.

Las ventajas de las marcas de agua constituyen también sus desventajas. Debido a que las marcas de agua digitales utilizadas en seguridad se crean añadiendo ruido invisible a un documento, a menudo estas no se pueden leer cuando el documento que las contiene ha sufrido desgaste por el uso. Debido a que las marcas de agua se ocultan con ruido los documentos, esta ocultación resulta difícil en documentos tales como el papel moneda, donde cada elemento del diseño es fijo y, por lo tanto, no hay margen para el ruido.

Incorporación de información que no puede reproducirse mediante una fotocopiadora

Un documento puede contener una parte que es invisible en el espectro de luz visible, porque está impresa con una tinta que es visible en luz ultravioleta. Las fotocopiadoras, que funcionan con luz visible, no puede reproducirla. Véase la patente US nº 5.868.432 de Mantegazza, *Documents with anticopying means to prevent reproducibility by photocopying*, publicada el 9/2/99.

La información puede precisar aún más resolución que la que puede ofrecer el procedimiento de escaneado e impresión. Véase la patente US nº 5.708.717 de Alosia, *Digital anti-counterfeiting software method and apparatus*, publicada el 13/11/98, que da a conocer un procedimiento para combinar una imagen de origen y una imagen latente que solo es visible cuando se observa a través de una lente decodificadora especial. Esta imagen latente puede contener, por ejemplo, la palabra "auténtica" repetida varias veces, o más información específica del documento, tal como información personal en la foto de un documento de identidad. Sin embargo, puesto que la imagen latente se imprime con precisión de "subpíxel", no es fácil de reproducir. Como es de esperar, lo que actualmente es de precisión "subpixel" puede ser fácilmente reproducible en el futuro.

En documentos tales como los documentos de identidad y el papel moneda se insertan hologramas por considerarse fáciles de detectar a través del sentido de la vista y difíciles de reproducir con alta fidelidad.

No obstante, mientras que cualquier persona puede ver si hay un holograma en un documento, un observador inexperto por lo general no podrá detectar si el holograma es auténtico o una copia.

El documento WO 01/15382 da a conocer un procedimiento para verificar una copia impresa de un documento electrónico, en el que un módulo de escaneo escanea dicha copia impresa, un módulo de extracción de marca de agua extrae la marca de agua de la versión digital del documento impreso y un módulo de extracción de compendio extrae un compendio del contenido. Este compendio extraído del contenido de la marca de agua del documento impreso se compara con el compendio original del contenido almacenado inicialmente y, en función de las similitudes, el documento se considera verificado o se rechaza. El módulo de extracción de marca de agua y de compendio deben tolerar la distorsión y los diferentes formatos.

La patente US nº 5.974.150 da a conocer un sistema de autenticación para medios que presentan una pluralidad de elementos con atributos de croma y luminancia diferenciados; presentando el sistema un detector para detectar dichos atributos y la posición de los elementos, un procesador para generar un mensaje encriptado que comprende por lo menos una parte del atributo de luminancia y la posición de los elementos, registrándose dicho mensaje encriptado en asociación física con los medios que se desean autenticar, basándose la autenticación en una correlación vectorial de los elementos de los medios y la comparación de la posición de los elementos con las características presentes en el mensaje encriptado.

El documento EP 1 168 817 da a conocer un sistema de autenticación para autenticar documentos que presentan una marca de agua digital, estando incorporada dicha marca de agua a una imagen auténtica. Cuando se autentica un documento, el sistema lee la imagen auténtica y extrae y compara la marca de agua digital con la correspondiente marca de agua almacenada en una base de datos. Dependiendo de las similitudes de las marcas de agua, el documento se considera auténtico o se rechaza.

Problemas comunes de las características de protección contra copia invisibles

Uno de los problemas que entrañan todas las características de protección contra copia invisibles es que su invisibilidad hace que sean completamente inútiles para las personas que no disponen de los instrumentos especiales que se necesitan para leerlas. Por otra parte, la invisibilidad de las características causa problemas de impresión y/o detección. Con las marcas de agua, su requisito de invisibilidad determina forzosamente que sean difíciles de detectar, lo cual es especialmente cierto en los casos en que el desgaste por el uso añade ruido adicional a un documento. Con tinta invisible, tanto la impresión como la detección son complicadas, siendo este el caso de las imágenes latentes impresas con "precisión de subpíxel".

Lo que se necesita son técnicas que puedan determinar de un modo fiable, y a un coste inferior, si un documento es original o una copia, si este se ha alterado o está autorizado y que permitan constatar que el documento es fácilmente autenticable y puedan integrarse con facilidad con otras técnicas de autenticación de documentos. Uno de los objetivos de la presente invención dado a conocer en la presente memoria es la provisión de dichas técnicas.

Sumario de la invención

El objetivo de la presente invención se alcanza en un aspecto mediante unas técnicas para determinar si una forma analógica de un objeto es una forma analógica original, es decir, una forma analógica que no se ha obtenido mediante fotocopia o escaneo de una forma analógica, sino a partir de una representación digital original. En un procedimiento en el que se emplean las técnicas, una parte del registro digital realizado a partir de la forma analógica se compara con una representación digital original de la parte de la forma analógica para determinar el grado de disimilitud entre la parte registrada y la representación digital original de la parte y, mediante el grado de disimilitud, determinar si la forma analógica es una forma analógica original. Otra característica de la presente invención es que la disimilitud que se determina es una disimilitud que está causada por las operaciones implicadas en la creación de una forma analógica no original.

Otras características de este aspecto son la puesta en práctica del procedimiento en un nodo de una red que recibe el registro digital desde otro nodo de la red y la devolución, a otro nodo, de una indicación que especifica si se ha determinado que la forma analógica es una forma analógica original, así como la puesta en práctica del procedimiento en un procesador al cual se conectan un dispositivo de registro digital y un dispositivo de salida. El procesador crea el registro digital a partir de la entrada recibida desde el dispositivo de registro digital y facilita una indicación en la que se comunica si se ha determinado que la forma analógica es una forma analógica original al dispositivo de salida.

En una forma de realización ventajosa de la presente invención, la representación digital original de la parte presenta un patrón con ruido. La representación digital original puede crearse mediante una clave, pudiendo presentar la representación digital original una función en la forma analógica, además de la de permitir determinar si la forma analógica es original. La función puede ser la de servir de código de barras o imagen de fondo o transmitir un mensaje.

Otro aspecto de la presente invención es un procedimiento para aplicar una comprobación de autenticidad a una forma analógica. El procedimiento compara un registro digital de un patrón con ruido de la forma analógica con la representación digital original del patrón con ruido, y el resultado de la comparación se utiliza para realizar la comprobación de autenticidad. La técnica puede utilizarse para determinar si se ha destruido una parte del patrón con ruido en la forma analógica. El patrón con ruido puede contener además un mensaje.

Otro aspecto de la presente invención es un procedimiento de ocultación de un mensaje en una forma analógica. En el procedimiento, se crea una representación digital de un patrón con ruido visible en el que se ha ocultado el mensaje y esta se integra en la forma analógica.

Otros objetivos y ventajas resultarán evidentes a los expertos en la materia, a quienes va dirigida la presente invención, tras la lectura minuciosa de la siguiente *Descripción detallada* y los dibujos adjuntos.

Breve descripción de los dibujos

La figura 1 es una visión de conjunto de cómo se genera e inserta en un documento un patrón de autenticación visible (VAP).

La figura 2 representa cómo se registra un VAP de un documento.

La figura 3 es un diagrama de flujo que representa una visión de conjunto de cómo puede utilizarse un VAP en la autenticación.

La figura 4 es una visión de conjunto de la impresión y autenticación de las formas analógicas originales y no originales.

La figura 5 representa unas GUI para la detección de marcas de agua y la detección de alteraciones.

La figura 6 es un gráfico que representa la correlación entre las energías de las bandas de frecuencia de una representación digital original de un VAP y un VAP registrado a partir de un documento no original.

La figura 7 es un gráfico que representa la correlación entre las energías de las bandas de frecuencia de una representación digital original de un VAP y los VAP registrados a partir de documentos originales.

La figura 8 representa cómo puede utilizarse una clave de mensaje para incorporar una marca de agua sin contenido a una imagen.

La figura 9 representa una técnica para determinar si una representación digital particular proviene de una representación digital a la que se incorporó una marca de agua mediante una clave de mensaje.

La figura 10 representa cómo puede utilizarse un VAP para detectar la alteración de un documento.

La figura 11 representa cómo puede incorporarse un VAP a un código de barras o un logotipo.

Los números de referencia del dibujo presentan tres o más dígitos: los dos dígitos de la derecha son números de referencia del dibujo indicado por los dígitos restantes. Por lo tanto, un elemento con el número de referencia *203* aparece por primera vez como elemento 203 en la figura 2.

Descripción detallada

Utilización de la mera presencia de marcas de agua para autenticar un documento

En términos generales, en las técnicas de autenticación de documentos que comprenden marcas de agua, las marcas de agua se utilizan para ocultar algún tipo de *información* de autenticación para el documento en un elemento gráfico del documento. Un ejemplo de lo anterior es la utilización de la marca de agua para ocultar un compendio elaborado a partir de los códigos de caracteres del documento, tal como se indica en la patente US n^{o} 6.243.480 antes mencionada. Una dificultad de las técnicas que utilizan marcas de agua para ocultar información de autenticación en un elemento gráfico de un documento es que el desgaste por el uso del documento determina a menudo que la marca de agua resulte ilegible.

El documento principal USSN 10/287.206 de la presente solicitud explora formas de obtener por lo menos algo de información a partir de marcas de agua ilegibles y formas de crear marcas de agua más resistentes a las transformaciones que implican pérdidas de datos, tales como las causadas por el desgaste por el uso de un documento. Entre los descubrimientos realizados por los inventores del documento USSN 10/287.206 en el transcurso de su trabajo cabe mencionar, en primer lugar, que la simple presencia de una marca de agua podría utilizarse para autenticar un documento y, en segundo lugar, que la simple presencia de una marca de agua podría utilizarse para descubrir en qué lugar presentaba el documento la alteración. A continuación, se indican las partes del documento USSN 10/287.206 que se ocupan de estas consideraciones.

Marcas de agua que se incorporan mediante claves de mensajes: figuras 8 y 9

La aplicación estándar de las marcas de agua digitales es la de ocultar un mensaje en una representación digital. Uno de los usos de dicho mensaje es la validación o la autenticación de la representación digital: se supone que la representación digital que se va a validar contiene una marca de agua que contiene un mensaje particular; se lee la marca de agua y su contenido se compara con el mensaje particular. Si ambos coinciden, la representación digital es válida o auténtica. Cuando la representación digital ha experimentado una transformación con pérdidas, la marca de agua puede ser ilegible; en estas situaciones, las técnicas que se describen en el documento USSN 10/287.206 permiten una validación o autenticación limitada. La validación por medio de los mensajes contenidos en las marcas de agua entraña un problema general y es que la validación conlleva a menudo mensajes largos, tales como números de seguridad social o números de cuenta, mientras que las marcas de agua que contienen dichos mensajes largos son menos resistentes que las marcas de agua que contienen mensajes cortos y, por consiguiente, tienen más probabilidades de volverse ilegibles debido a transformaciones con pérdidas.

Una solución a este problema general se fundamenta en la observación de que, para fines de validación o autenticación, no es necesario que la marca de agua *contenga* realmente el mensaje que constituye la base para la validación o la autenticación, sino que basta con que una marca de agua determinada esté presente en una representación digital *solo si* la marca de agua se creó *mediante* el mensaje que constituye la base para la validación. En ese caso, no es necesario que la marca de agua sea legible; en su lugar, la mera *presencia* de la marca de agua permite que se valide la representación digital. Además, debido a que es la presencia de la marca de agua y no su contenido la que indica que la representación digital es válida o auténtica, el contenido de la marca de agua no necesita desempeñar ninguna función más que la de indicar la presencia de la marca de agua y su longitud

no precisa ser más larga que la que se requiere para desempeñar esta función; de hecho, el vector de marca de agua para dicha marca de agua solo necesita especificar el valor de un único bit. Esto, a su vez, determina que dichas marcas de agua sean mucho más resistentes que las marcas de agua que contienen el mensaje que constituye la base para la validación o la autenticación.

Una forma de crear una marca de agua cuya mera presencia en una representación digital valide o autentique la representación digital consiste en utilizar el mensaje para determinar la ubicación de la marca de agua en la representación digital. Esto se indica mediante el número de referencia 801 en la figura 8. Se utiliza una función clave 805 (*f*) para crear una clave 806 (*K2*) a partir de un mensaje 803 (*m*)*: K2 =f*(*m*)*;* cuando es necesario, la función 805 pueden utilizar una clave secreta *K1*, así como *m* para crear la clave: K*2-f*(*K1,m*)*.* La clave 806 se suministra al insertador de marcas de agua 809 junto con un vector de marca de agua corto (mínimo de 1 bit) WM 807, y el insertador de marcas de agua 809 incorpora una marca de agua creada mediante el vector de marca de agua 807 en los lugares indicados por la clave 806 de la representación digital que contiene la marca de agua 813.

En la figura 8, la marca de agua de la representación digital 813 se representa mediante los recuadros en línea de puntos 807. Puesto que el mensaje 803 ya no se halla en la marca de agua, sino que se utiliza para crear la clave 806, y el vector de marca de agua corto 807 solo necesita ser de 1 bit de longitud, la longitud del mensaje no tiene efecto alguno sobre la resistencia de la marca de agua. Como bien se sabe en el ámbito de las matemáticas, podrían utilizarse muchas funciones para generar la clave 806 a partir del mensaje 803, de tal forma que la clave 806 y, por tanto, la marca de agua creada con esta, sea exclusiva para el mensaje. Evidentemente, el grado de exclusividad que se requiere podrá variar con la aplicación. En algunos casos, la función puede ser una función de identidad, es decir, la clave es el propio mensaje. Una de las ventajas de la técnica es que la función determina la longitud de la clave de la marca de agua, y por lo tanto, la clave puede tener la longitud necesaria para una aplicación particular.

Con el número de referencia 901 de la figura 9, se representa un sistema que determina si una representación digital 903, donde se supone que está contenida una marca de agua creada de la forma descrita, es auténtica. La representación digital 903 contiene un conjunto de ubicaciones 905 que deberían contener el vector de marca de agua 807 si la representación digital 903 procediera realmente de la representación digital 813. Las ubicaciones se hallan en las posiciones que, en la representación digital 813, se determinaron mediante la clave 806. El sistema que realiza la autenticación obtiene el mensaje 803 y asimismo obtiene o posee la función clave 805. La función clave 805 se aplica al mensaje 803 para generar la clave 806 tal como se ha descrito anteriormente. A continuación, el sistema facilita la clave 806 al lector de marcas de agua 907, que la utiliza para encontrar las ubicaciones 905. Cuando se encuentra una ubicación, esta se transmite al comparador 909, tal como se representa en 909. El sistema 901 también posee el vector de marca de agua corto 807 y lo transmite al comparador 911 para que por su parte este lo compare con el valor de cada una de las ubicaciones 905. El resultado 912 de cada comparación pasa al agregador 913, donde los resultados se agregan para generar el resultado global 915, que indica si la marca de agua que se incorporó a la representación digital 813 está presente en la representación digital 903. El comparador 911 y el agregador 913 pueden utilizar cualquiera de las técnicas descritas anteriormente con respecto a las marcas de agua ilegibles a fin de realizar la comparación y la agregación. Tal como se describe más adelante en relación con las técnicas utilizadas con las marcas de agua ilegibles, el patrón de ubicaciones 905 que coinciden con la marca de agua de la representación digital 813 puede utilizarse para indicar las ubicaciones en las que la representación digital 903 ha sido alterada.

En algunas aplicaciones, el agregador 913 generará un resultado visual de la comparación. En la figura 5, se representa un ejemplo de dicha comparación en 501. Los bloques a los que se ha aplicado la marca de agua presentan diferentes sombreados que dependen del grado de detección de la presencia de la marca de agua. Cuanto más claro es el bloque, más pronunciada es la presencia de la marca de agua en el bloque. Debido a que la imagen 501 ha sufrido transformaciones con pérdidas, la distribución de los bloques con marcas de agua pronunciadas no será la misma que en el original, pero como los errores causados por las transformaciones con pérdidas son aleatorios, si la imagen es auténtica, todas las áreas que contienen la marca de agua deberían tener aproximadamente la misma distribución de bloques claros, tal como se representa en 501. Esta técnica de visualización puede, por supuesto, utilizarse también con marcas de agua, en las que el mensaje determina el contenido de la marca de agua.

<u>Utilización de marcas de agua para localizar alteraciones en documentos digitales y documentos analógicos creados a partir de documentos digitales</u>

Una forma de atacar un documento digital o una forma analógica creada a partir del documento digital es la modificación local de una imagen del documento o la forma para cambiar su contenido semántico. Entre los ejemplos de modificaciones locales cabe mencionar:

- modificación del número de matrícula de la imagen de un coche captada por un DVR en la escena de un accidente o delito o
- modificación de áreas del retrato de un documento de identidad; o

- sustitución del retrato de un documento de identidad.

Si el documento o la forma contiene una marca de agua, el objetivo de la falsificación será cambiar el contenido semántico del documento digital o la forma sin afectar a la marca de agua o a la legibilidad de esta. En general, cuando una marca de agua es suficientemente resistente como para ser legible, la realización de pequeños cambios en el documento o la forma con fines fraudulentos sin afectar a la marca de agua o la legibilidad de esta no entrañará mucha dificultad. Por otro lado, la misma resistencia de la marca de agua hace que esta sea muy útil para detectar y rastrear las alteraciones.

Con el fin de utilizar una marca de agua para localizar una alteración, solo es necesario saber los lugares en los que se espera encontrar la marca de agua y su vector de marca de agua. Puesto que la técnica no requiere que la marca de agua presente un contenido particular, basta con que el vector de marca de agua sea de un solo bit. Una vez que el detector conoce las ubicaciones de la marca de agua y el vector de marca de agua, el detector puede utilizar el vector de marca de agua w', que es una réplica del vector de marca de agua de la marca de agua original w, y comparar w' con la marca de agua w'' del contenido que se ha puesto en cuestión. Las diferencias entre w' y w'' pueden demostrar si se ha modificado el documento digital o la forma analógica que es la fuente del contenido puesto en cuestión, y de ser así, qué partes se han modificado.

En mayor detalle, el detector compara el vector de marca de agua w'' de cada subparte (denominada *bloque* en la presente memoria) del documento digital o la forma analógica con el vector w'. La comparación indica si cada bloque del documento o la forma contiene la información de marca de agua correcta. En un documento digital, si no se ha producido ninguna alteración, la mayoría de los bloques contendrán la información de marca de agua correcta. Con las formas analógicas, el procedimiento de impresión y escaneo deteriora la marca de agua y, en consecuencia, no todos los bloques conservarán la información de marca de agua correcta (por ejemplo, pueden contener del orden de un 20 % a un 40 % de errores). Estos errores de impresión y escaneo generalmente son de carácter aleatorio y, por consiguiente, puede esperarse que estén distribuidos de forma más o menos uniforme en la forma analógica. Por lo tanto, si la imagen se ha alterado localmente y por lo tanto ha perdido su marca de agua en las zonas alteradas, el detector de marcas de agua responderá a las zonas alteradas de la misma manera en que responde a las zonas que no contienen una marca de agua. De esta manera, el detector de marcas de agua detecta la alteración. La técnica también puede utilizarse para mostrar la resistencia de la marca de agua en cada área de la imagen.

La réplica del vector de marca de agua utilizada para detectar alteraciones o la resistencia de la marca de agua puede provenir de cualquier fuente. Entre los ejemplos de fuente cabe citar la imagen original, un vector de marca de agua del contenido puesto en cuestión que se ha leído correctamente o un vector de marca de agua que se ha generado de nuevo a partir del mensaje. La incorporación y detección adaptativa puede utilizarse para aumentar la eficacia de la detección de alteraciones. Por ejemplo, las áreas del contenido que necesitan una protección especial contra los cambios pueden recibir una marca de agua de mayor resistencia que otras áreas del contenido, y la mayor resistencia de la marca de agua de estas áreas puede tenerse en cuenta cuando se analizan las marcas de agua de la forma descrita anteriormente. Por supuesto, la técnica que se utiliza para mostrar la resistencia de la marca de agua en cada área de la imagen puede emplearse para facilitar el diseño de máscaras para la incorporación y detección adaptativa.

Pueden aplicarse diferentes técnicas basadas en datos estadísticos, procesamiento de señales o reconocimiento de patrones para detectar de forma automática áreas que contienen un número anormalmente elevado de bloques que contienen información incorrecta (o que no contienen información). Por ejemplo, una técnica basada en el reconocimiento de patrones consiste en determinar las conexiones de bloques incorrectos y extraer las conexiones que superen un umbral. Otra técnica sería la de determinar si hay más de *P* bloques incorrectos en todas las áreas de tamaño *NxN* de la forma analógica. Otra técnica basada en el procesamiento de señales consiste en asignar valores positivos a los bloques correctos y valores negativos a los bloques incorrectos y, a continuación, hacer pasar la matriz resultante por un filtro pasabaja. Se considera que las áreas de la matriz filtrada en las que los valores están por debajo de un umbral han sufrido alguna alteración. Por último, puede aplicarse el cálculo estadístico a todos los sistemas para caracterizar las áreas de la imagen que no se han alterado y las que sí se han alterado y para determinar los parámetros de detección en relación con las expectativas del usuario (por ejemplo, el tamaño mínimo de las áreas alteradas, la probabilidad de falsas alarmas o rechazos, etc.). También es posible presentar al usuario una imagen con los bloques correctos e incorrectos en diferentes colores, para permitir la interpretación de los datos por el usuario.

La figura 5 representa el efecto de las alteraciones sobre la resistencia de la marca de agua y también facilita un ejemplo de una forma gráfica de mostrar las áreas alteradas. En este caso, la imagen 501 se modificó después de que se le incorporara la marca de agua, sustituyendo la cara por otra cara a la que no se había incorporado una marca de agua de la misma manera que la cara de la imagen 501. El resultado de la modificación es la imagen 502. Cuando se compara la imagen 502 con la imagen 501, se puede apreciar que el área facial de la imagen 502 es más oscura que el área facial de la imagen 501. A su vez, esto demuestra que los bloques del área facial de la imagen 502 presentan una marca de agua mucho más débil que los bloques del área facial de la imagen 501. La débil

marca de agua del área facial de la imagen 502 es, por supuesto, consecuencia directa de la modificación. Cuando se aplica un filtro que resalta las áreas con muchos bloques débiles, el resultado es la imagen 503, en la que se pone claramente de manifiesto el área modificada 505.

Ampliaciones de la técnica

- Detección de más de un área alterada
- Utilización de módulos externos (por ejemplo, reconocimiento facial), para centrar la detección de la alteración en las áreas más significativas desde el punto de vista semántico (p. ej., los ojos en una foto de documento de identidad)
- Escaneo múltiple de documento físico para anular la variabilidad del escaneo.

Si la marca de agua es ilegible, la detección de la alteración puede utilizarse para analizar las razones de su ilegibilidad.

Patrones de autenticación visibles

Las consideraciones anteriores vinieron seguidas de la consideración que condujo hasta la presente invención: cuando se utiliza la mera presencia de una marca de agua para determinar la autenticidad de una forma analógica, la marca de agua se utiliza como un patrón sin contenido. Puesto que el patrón no tiene contenido, no hay ninguna necesidad de que este sea invisible, sino que, en su lugar, puede añadirse al documento como un elemento visible. En lo sucesivo, los patrones visibles que se utilizan para la autenticación se denominan *patrones de autenticación visibles* o VAP. Debido a que el VAP es visible, es mucho más fácil de detectar que una marca de agua. Sin embargo, puede seguir siendo capaz de desempeñar todas las funciones de autenticación de marcas de agua invisibles y, además, dar a conocer a los usuarios del documento que la autenticidad del documento está protegida.

Terminología

En la *Descripción detallada,* se utilizará la terminología indicada a continuación para aclarar las relaciones entre las representaciones digitales y las formas analógicas.

Una *representación digital* de un objeto es una forma del objeto en la que un sistema de procesamiento digital puede almacenar y manipular el objeto. Los objetos pueden ser o comprender como componentes: imágenes, audio, vídeo o cualquier otro medio del cual pueda estar compuesta una representación digital.

Una *forma analógica* de una representación digital es la forma de un objeto o un componente que se obtiene cuando la representación digital se transmite a un dispositivo analógico, tal como una pantalla, una impresora o un altavoz.

Un *registro digital* de una forma analógica es una representación digital creada a partir de la forma analógica. La manera en que se realiza el registro digital depende de los medios; por ejemplo, para un documento o una imagen, el registro digital se efectúa por medio de la digitalización de una imagen creada a partir de una forma analógica del documento o la imagen.

Una representación digital *original* es una representación digital realizada o copiada por una persona autorizada; una forma analógica *original* es la que se obtiene a partir de una representación digital original.

Una representación digital *no-original* es la que se obtiene registrando digitalmente una forma analógica sin autorización; una forma analógica *no original* se obtiene a partir de una representación digital no original o fotocopiando una forma analógica.

A un *documento* se le dará el significado especial de cualquier forma analógica que se genere mediante un procedimiento de impresión, incluidos los documentos en el sentido más habitual de la palabra, etiquetas, embalaje y objetos que ya vienen impresos. En la medida en que se puedan establecer analogías razonables, todo lo que en lo sucesivo haga referencia a los documentos puede aplicarse también a otros medios. Por ejemplo, una forma analógica de audio puede comprender un patrón de autenticación audible que es el audio equivalente del VAP.

Creación de un patrón de autenticación visible: figura 1

La paradoja del patrón de autenticación visible es que mientras el patrón sea visible, un posible infractor no deberá ser capaz de modificar el patrón para autenticar un documento que no es auténtico. Este fin se cumple en una forma de realización preferida añadiendo *ruido* al patrón, es decir, una gran parte del valor de los píxeles que componen el patrón parece ser determinada al azar. Debido a que el patrón contiene ruido, es imposible saber qué valores deberían tener los píxeles que componen la representación digital del patrón sin acceder a la representación digital original del patrón. Por otro lado, dada la representación digital original de un VAP, se puede comparar un registro

digital de un VAP de un documento con la representación digital original del VAP, determinar cómo se ha alterado el VAP registrado con respecto a la representación original del VAP y, a partir de las diferencias, determinar cómo se ha alterado el documento en cuestión. Como se verá en mayor detalle en lo sucesivo, las alteraciones que pueden detectarse comprenden las involucradas en la creación de documentos no originales y las involucradas en la alteración de información de un documento.

La figura 1 representa una manera de crear un patrón de autenticación visible e insertarlo en un documento. Esto conlleva las tres etapas siguientes:

- generación una representación digital del patrón, representada en 101;
- etapa opcional de adición de un logotipo o leyenda visible al patrón de autenticación, representada en 107; e
- inserción del patrón de autenticación en el documento, representada en 113.

La representación digital original del patrón 105 puede generarse de cualquier manera que dé por resultado un patrón con píxeles que parezcan tener valores con un componente sumamente aleatorio. La representación digital del patrón 105 puede ser un patrón en escala de grises o puede emplear píxeles de color. Resulta particularmente útil emplear una clave para generar el patrón, siendo utilizada dicha clave 103 como valor inicial para un generador de números pseudoaleatorios que genera la secuencia de valores que se dan a los píxeles del patrón. Los usos de la clave se describirán en detalle más adelante. La representación digital original del patrón 105 también puede comprender componentes que ayudan a localizar el patrón en una representación digital que se ha creado escaneando un documento que contiene el patrón 105. En el patrón 105, el borde negro 106 desempeña esta función.

Puede añadirse un logotipo o leyenda visible 109 a la representación digital original del patrón 105 para crear la representación digital original del patrón 111 sin poner en riesgo el nivel de ruido del patrón 105, debido a que solo una parte del valor de los píxeles que componen el patrón necesitan ser determinados al azar. Por lo tanto, el logotipo o la leyenda se pueden superponer al patrón 105 manipulando los valores de los píxeles que componen el logotipo o la leyenda, de una manera que mantiene su aleatoriedad y permite al mismo tiempo la visualización del logotipo o la leyenda. Por ejemplo, si el patrón 105 es un patrón en escala de grises, la leyenda o el logotipo puede crearse oscureciendo o aclarando uniformemente los píxeles de la leyenda o el logotipo respecto de sus valores aleatorios originales. La técnica es parecida a la de añadir una marca de agua visible a una imagen, excepto en que conserva el ruido del patrón 105.

Una vez que se ha creado la representación digital original del patrón 111, esta se inserta en la representación digital original del documento 115, tal como se representa en 113. Cuando se imprime el documento 117 a partir de la representación digital original 115, el documento 117 comprende el patrón de autenticación visible impreso 119. Es por supuesto posible imprimir el documento en un sustrato que ya contiene material impreso. Por lo tanto, el patrón 119 puede añadirse a un sustrato preimpreso.

Utilización de un patrón de autenticación visible para autenticar un documento: figuras 2 y 3

Cuando se autentica un documento que contiene un VAP 119 impreso, sucede lo siguiente:

- se detecta el VAP impreso 119 en el documento;
- se realiza un registro digital del VAP impreso detectado 119;
- se compara el registro digital del VAP con la representación digital original del VAP; y
- se determina la autenticidad basándose en la comparación.

La manera en que se compara el registro digital del VAP impreso con la representación digital original del VAP depende del tipo de autenticación que se realiza; además, la autenticación de un documento determinado puede conllevar la realización de diferentes tipos de comparaciones entre el registro digital y la representación digital original. Por ejemplo, un registro digital de un patrón de autenticación visible en el campo del importe de un cheque puede compararse, en primer lugar, con la representación digital original para determinar si el cheque es falso y, en segundo lugar, para determinar si se ha alterado el importe indicado en el campo de importe.

La figura 2 representa cómo se detecta el VAP impreso y se crea un registro digital del VAP en una forma de realización preferida. Ambas acciones se realizan mediante el programa de aplicación "Scanread" comercializado por MediaSec Technologies. Pueden emplearse también otras aplicaciones que detectan una parte de un documento y realizan un registro digital de esta. Scanread 201 utiliza un borde negro 106 para detectar la presencia de un patrón de autenticación visible 119 en el documento impreso 117 y, a continuación, crea el registro digital 203 del patrón de autenticación visible 119. La figura 3 representa un diagrama de flujo general 301 de un programa que utiliza el registro digital 203 y la representación digital original 111 del VAP 119 para determinar la autenticidad. La representación digital original 111 del VAP puede ser el propio original, una copia del original o un nueva representación digital original 111 creada exactamente de la misma manera que la primera representación digital original. Las representaciones digitales originales obtenidas mediante cualquiera de estos procedimientos son, por supuesto, completamente equivalentes, y el procedimiento elegido depende de cuestiones de implementación, tales

como el coste de almacenamiento de la representación digital original del VAP, el coste de transmisión de la representación digital original del VAP a través de una red y el coste de la generación de la representación digital original cada vez que se necesita.

Empezando por 303, las características de registro digital 203 y la representación digital original 111 se comparan en 305, dependiendo la elección de las características comparadas y el modo de compararlas del tipo de autenticación que se realice. Si las diferencias entre el registro digital 203 y la representación digital original 111 superan un umbral (307), se plantea un problema de autenticación y se sigue la bifurcación 309. El umbral dependerá también del tipo de autenticación que se realice. En la bifurcación 309, se indica la existencia de un problema al programa de aplicación que realiza la autenticación en 311. Si resulta útil, el programa puede facilitar asimismo información acerca de la comparación (315); también en este caso, el tipo de información y la manera en que se facilita dependerá del tipo de autenticación. Por ejemplo, si el importe del campo de importe parece haber sido alterado, el programa puede presentar una imagen que muestra cuál de los píxeles de la representación digital original parece haber sido alterado en el registro digital del patrón de autenticación visible. Si las diferencias no superan el umbral, se sigue por la bifurcación 317. Entonces, se informa sobre la no detección de ningún problema de autenticación al programa de aplicación que realiza la autenticación. Ambas bifurcaciones y el programa terminan en 321.

Utilización de patrones de autenticación visibles para distinguir un documento original de un documento no original: figuras 4 y 5

Una de las posibles maneras de utilizar un patrón de autenticación visible para autenticar un documento es determinando si un documento es original, es decir, si se ha imprimido a partir de una representación digital original o no es original (es una fotocopia de un documento o se ha imprimido a partir de una representación digital no original, es decir, una representación digital realizada a partir de un registro digital no autorizado de un documento). La razón por la cual un patrón de autenticación visible puede utilizarse de esta manera es que la impresión de un documento a partir de su representación digital y la creación de una representación digital de un documento a partir de un registro digital de este o una fotocopia de un documento siempre provocan pérdidas de información en el patrón de autenticación visible, independientemente de la precisión de los procedimientos de impresión, registro digital o fotocopia; en consecuencia, mediante la comparación de una representación digital original de un patrón de autenticación visible con una representación digital creada registrando el patrón de autenticación visible a partir de un documento, se puede determinar si el documento es original o no. En el caso de un documento original, el patrón de autenticación visible se habrá impreso una vez y registrado digitalmente una vez; en el caso de un documento no original, el patrón de autenticación visible se habrá impreso y registrado digitalmente una vez para generar el documento original a partir del cual se creó el documento no original y, a continuación, dependiendo de la manera en que se creó el documento no original, se habrá fotocopiado o imprimido y registrado digitalmente de nuevo, provocando una pérdida de información en el patrón de autenticación visible del documento no original que es superior a la del patrón de autenticación visible del documento original.

La técnica básica se representa en detalle en la figura 4. En 401, se representa cómo funciona la autenticación mediante un patrón de autenticación visible con un documento original. La representación digital original 403 del documento contiene un patrón de autenticación visible original (ovap) 405. A continuación, la representación digital original 403 se imprime en 407 para generar una forma analógica original 409. La operación de impresión causa una pérdida (*loss1)* en el patrón de autenticación analógico visible original (oavap) 411 de la forma analógica 409. Cuando el autenticador 421 autentica la forma analógica 409, se realiza un registro digital del oavap 411 que provoca una pérdida (*loss2*). El registro obtenido se identifica como "roavap" en 415. Entonces, el autenticador 421 emplea el comparador 417 para comparar el ovap 406 con el roavap 415. La diferencia entre estos es la suma de *loss1* y *loss2.* Esto se cumplirá cuando cualquier roavap sin ningún otro daño 415 se compare con el oavap 405, siendo una diferencia de ese tamaño una indicación fiable de que la forma analógica 409 es en realidad una forma analógica original.

En 420, puede verse cómo funciona la autenticación con un documento no original. La diferencia entre el documento original y el documento no original es que el documento no original no se ha imprimido directamente a partir de la representación digital original 403 del documento, sino a partir de una representación digital no original 423 del documento que se ha creado registrando digitalmente un documento original 409 (422). Como resultado del registro digital, el patrón de autenticación visible no original 425 de la representación digital 423 ha sufrido una pérdida adicional de información que se identifica en la figura 4 como *loss3.* Cuando se imprime (427) una forma analógica no original 429 a partir de la representación digital 423, se produce otra pérdida en el patrón de autenticación visual analógico no original 431, indicada como *loss4.* Cuando el autenticador 421 autentica la forma analógica no original 429 tal como se ha descrito anteriormente y se compara el moavap 435 creado a partir del noavap 431 con el ovap 405, el efecto de *loss3* y *loss4* se pondrá de manifiesto como una diferencia entre el ovap 405 y el movap 435 superior a la que había entre el ovap 405 y el roavap 415. Puesto que el noavap 431 de una forma analógica no original 429 siempre sufrirá las pérdidas adicionales *loss3* y *loss4*, la diferencia superior es un indicador fiable de un documento no original.

La forma analógica no original 429 puede, por supuesto, generarse mediante cualquier procedimiento de fotocopia, así como mediante el procedimiento de registro de la forma analógica original (422) para crear una representación

digital no original 423 y, a continuación, impresión (427) de la representación digital 423 para generar la forma analógica no original 429. El procedimiento de adquisición de la imagen de la forma analógica original 409 y, a continuación, impresión de la forma analógica no original 429 de la imagen provoca pérdidas adicionales como *loss3* y la *loss4;* por consiguiente, el moavap 435 obtenido de esta manera será menos similar al ovap 405 que el roavap 425.

Por supuesto, si la propia representación digital no original 423 se crea a partir de una representación digital no original, el movap 435 comprenderá también las pérdidas adicionales resultantes de la fotocopia o la impresión y el registro digital de dicha representación digital no original. Como resultará obvio, si *loss1* y *loss2* fueran valores fijos, el detector podría determinar siempre de forma correcta si el documento es original o no. Sin embargo, en general se produce cierta variación en cada pérdida; por ejemplo, algunos originales podrían imprimirse con una mayor calidad (fidelidad) que otros. Parece, pues, que la detección debería abordarse desde un punto de vista estadístico.

Detalles de una forma de realización preferida de la técnica para distinguir entre un documento original y un documento no original: figuras 6 y 7

Una técnica de autenticación resulta adecuada en la medida en que es fiable. La clave para reducir al mínimo la probabilidad de que se produzcan errores de detección es el procedimiento para medir cuán "diferente" es un patrón de autenticación visual registrado a partir de un documento de la representación digital original del patrón de autenticación visual. El procedimiento de medición elegido debe basarse en las propiedades del VAP que han sido afectadas por el procedimiento de creación de un documento no original y debe distinguir claramente un documento original de un documento no original.

Nuestro enfoque es el de considerar los procedimientos de fotocopia, registro e impresión como filtros y, más particularmente, como filtros pasabaja. Así pues, las altas frecuencias se atenuarán más que las frecuencias bajas debido a los procedimientos de impresión y registro, y perderán más información en cada etapa de registro e impresión o fotocopia. Para las frecuencias bajas a las que un procedimiento de registro e impresión o fotocopia conserva casi toda la energía, el VAP de un documento no original puede no presentar mucha menos información que el VAP del documento original. Las frecuencias muy altas pueden no resultar útiles tampoco, puesto que la mayor parte de la energía de estas frecuencias del VAP se pierde la primera vez que el imprime el VAP. En consecuencia, incluso los VAP de los documentos originales contienen muy poca información de esas frecuencias. Por consiguiente, las frecuencias utilizadas por el detector deben seleccionarse y/o ponderarse correctamente. La selección de las frecuencias para la comparación, así como la selección de un umbral para determinar si un documento es original o no, suele aplicarse mediante entrenamiento del software de comparación a los VAP de documentos originales.

Cabe señalar en ese sentido que la técnica descrita anteriormente no requiere ningún patrón de autenticación visual especial. En su lugar, el documento completo o una parte de este pueden utilizarse como patrón. No obstante, debido a que muchos documentos posiblemente no contengan información a los niveles de energía necesarios para determinar si un documento es original o una copia, es mejor utilizar un patrón de autenticación visual que contenga la información a los niveles de energía adecuados. En lo sucesivo, dichos patrones de autenticación visual se denominarán *patrones de detección de copia* o CDP*.* La información de un CDP se distribuye en frecuencias adecuadas. En una forma de realización preferida, la representación digital original del CDP se genera pseudoaleatoriamente mediante una clave y, en consecuencia, un programa que tenga acceso a la clave puede crear una nueva copia de la representación digital original del CDP en cualquier momento. Esta clave puede mantenerse en secreto o revelarse solo a las personas de confianza. El patrón de detección de copia se inserta o imprime en el documento que debe protegerse. En una forma de realización preferida, el análisis de un patrón de detección de copia de un documento se realiza registrando digitalmente el CDP del documento, utilizando la clave para generar una copia nueva de la representación digital original del CDP y comparando el CDP registrado con la representación digital original del CDP. En otras formas de realización, el CDP registrado puede compararse simplemente con una copia preexistente de la representación digital original del CDP.

Algoritmos utilizados en la técnica

En esta sección, se describen los algoritmos utilizados para (1) generar una representación digital original de un CDP; (2) detectar y extraer un CDP de un documento; (3) comparar la representación digital original de un CDP con un CDP registrado; y (4) determinar si un CDP es original o no. La manera en la que se comparan los CDP en el algoritmo (4) y los umbrales para determinar si un CDP es original o no se determinan mediante un procedimiento de entrenamiento en el que se utiliza el algoritmo (3) para recopilar datos de entrenamiento.

Generación de la representación digital original del CDP

Se utiliza la función *make_pattern* para crear una representación digital *(pattern_img*) de un patrón de detección de copia que se puede identificar con una fuente de la representación digital a partir de la cual se crea un documento original. *Make_pattern* genera un patrón en escala de grises o en color con ruido. Puede añadirse también un borde de color negro al patrón para facilitar su detección en el documento. Opcionalmente, el CDP también puede

presentar un logotipo. Por lo general, el logotipo afectará a las bandas de frecuencias más bajas y su repercusión en la detección será, por consiguiente, limitada. Los valores comunes se facilitan junto con la descripción de los parámetros.

Pattern_img = make_pattern(type, height, width, key, filename, border, logo_img, logo_weight).

Parámetros para la generación de patrones

Se necesita:

1. *Type*: tipo de valores de números aleatorios generados, por ejemplo, "randn" (N(0,1) gaussiano), "rand" (distribución equiprobable), "randint" (distribución binaria +1 o -1) o algoritmos MD5 y SHA (número entero 0-255). Los valores de números aleatorios se utilizan entonces para crear una imagen en escala de grises o en color.
2. *Height*: altura del patrón en píxeles (por ejemplo, 104).
3. *Width*: anchura del patrón en píxeles (por ejemplo, 304).
4. *Key*: clave secreta o contraseña de valor entero utilizada como valor inicial para el generador de números aleatorios.

Opcional:

5. *Filename*: nombre del archivo en el que se guarda la imagen del patrón.
6. *Registration mark* (por ejemplo, borde de color negro añadido a los lados de la imagen del patrón, puntos añadidos a las cuatro esquinas de la imagen del patrón).
7. *Logo_img*: imagen que se va a utilizar como logotipo de fondo, ajustada automáticamente a la dimensión de la imagen del patrón.
8. *Logo_weight*: valor entre 0 y 1 para ponderar la energía de la imagen del logotipo (por ejemplo, 0,2), que se superpone a la imagen del patrón.

Ejemplo del uso del algoritmo de generación de patrones:

1. Generación de un patrón en un dominio específico (por ejemplo, luminancia en DCT o espacial en modalidad de color RGB):

   pattern = generate_pattern(type, height, width, key).

2. Transformación del patrón al dominio espacial si el dominio de la etapa 1 no es el espacial (por ejemplo, DCT inversa):

   Pattern_img=transform(pattern).

3. Si es necesario, redondeo de valores de píxel p a valores enteros 0 <p<255.
4. Combinación de logotipo con patrón, por ejemplo, la función de mezcla siguiente puede ser:

   *pattern_img=(1-logo_weight)*pattern_img+logo_weight*logo_img.*

5. Adición de marca de registro (por ejemplo, borde negro).
6. Volcado de imagen.

Una imagen de patrón puede consistir en varios componentes o canales, tales como Rojo, Azul, Verde o YUV, que se pueden generar tal como se describe en las etapas 1 y 2 anteriores.

Para combinar un CDP con un logotipo o una imagen de fondo, pueden adoptarse varias funciones de mezcla. Por ejemplo, cuando el CDP se combina con un código de barras (imagen), el CDP solo sustituye las áreas negras del código de barras y deja intactas las áreas blancas.

Puede generarse cualquier forma (por ejemplo, círculo u óvalo) de la imagen del patrón. Un sistema sencillo consiste en utilizar una "máscara de forma" que define una forma arbitraria representada por una matriz de dos dimensiones que consiste en "1" y "0". Puede crearse cualquier forma aplicando la "máscara de forma" a la imagen del patrón rectangular.

Detección y extracción del VAP a partir de un documento

En esta implementación, se realiza un registro digital del documento que se autentica, y el borde negro del VAP se utiliza para localizar el VAP en el registro digital. El borde negro da por resultado una gran variación de la luminancia en la zona de transición, que es fácil de detectar. Pueden utilizarse también otras técnicas para determinar la ubicación del VAP (por ejemplo, características existentes en los documentos, puntos negros, etc.). Una vez que se ha detectado el VAP, se crea una representación digital de este que es comparable con la representación digital original del VAP. Esta representación digital es el VAP registrado.

La representación digital original del VAP y el VAP registrado se comparan mediante la siguiente función, que mide un índice que indica cuánto se parece el VAP registrado a la representación digital original del VAP. La representación digital original del VAP puede almacenarse en la memoria del detector o puede regenerarse si los parámetros utilizados para crear la representación digital original y la función make_pattern(..) están disponibles para el detector. Los parámetros opcionales utilizados al combinar el patrón con un logotipo posiblemente no sean necesarios, ya que el logotipo en general afecta solo ligeramente a las propiedades del patrón. La función para realizar la comparación es *analyze_pattern*, que genera *Results,* y puede adoptar diferentes parámetros dependiendo del caso aplicado realmente:

Results = analyze_pattern (type, height, width, key, ... , test_img);

O

Results = analyze_pattern (orig_jmg, test_img);

Parámetros y salida:

1. *type, height, width* y *key:* como se ha indicado, son para la generación de patrones.
2. *test_img:* imagen de patrón de prueba extraída del documento.
3. *orig_jmg:* representación digital original del patrón.
4. *Results:* contiene todos los resultados del análisis. Por ejemplo, puede comprender diferentes medidas de correlación o resultados estadísticos, calculados para los diferentes elementos de las imágenes, tales como frecuencias diferentes, áreas diferentes, canales de color diferentes, etc.).

El ejemplo siguiente muestra las etapas del algoritmo de regeneración del patrón digital original y las subfunciones necesarias para el algoritmo:

1. (Opcional) Eliminación del borde negro del CDP de prueba.
2. Transformación de la imagen del patrón de prueba al dominio en el que se generó inicialmente, por ejemplo, DCT de bloques 8x8: *test_pattern=transform(test_img).*
3. Regeneración del CDP original:

   pattern = make_pattern(type, height, width, key).

4. (Opcional) Sincronización local del CDP de prueba con el CDP original, tal como se describe más adelante. (Opcional) Aplicación de ciertos filtros de imagen (tal como la nitidez) al CDP a fin de obtener una mejor correlación con el CDP original.
5. Si es necesario, conversión del CDP original y el CDP de prueba al dominio en el que se va a realizar la comparación (por ejemplo DCT de bloques 8X8). Debe tenerse en cuenta que la comparación puede realizarse en más de un dominio, por ejemplo, en el dominio espacial y el dominio de la frecuencia.
6. Cálculo de varias medidas de similitud entre el CDP original y el CDP de prueba para cada canal en el dominio transformado. Se supone, por ejemplo, que se generan y se registran patrones en el dominio de color RGB y que el análisis se realiza en el dominio de la DCT de bloques 8x8. Existen, pues, 192 (es decir, 8x8x3) combinaciones mediante las cuales se pueden comparar los dos patrones y, por lo tanto, calcular 192 medidas de similitud. A su vez, la medida de similitud puede calcularse de diversas maneras, por ejemplo agrupando los valores en clases y manteniendo solo el que presenta una correlación más alta, a fin de excluir las áreas del CDP de prueba que puedan haber resultado dañadas.
7. Recopilación y combinación de todas las medidas de similitud o las medidas basadas en otras características

de la imagen, con el propósito de medir uno o más índices de calidad o de "concordancia" del CDP de prueba con el CDP original. La función de combinación puede ser cualquier función que combine las diferentes entradas, por ejemplo, una función que combine las medidas de similitud asignando más peso o importancia a las características que diferencian mejor entre el CDP original y el CDP de prueba.

Como se ha indicado anteriormente, un procedimiento de duplicación degrada siempre el CDP original, de ahí que en general se espere que las distintas medidas de concordancia o calidad sean inferiores para un CDP que se registra a partir de una forma analógica. No obstante, debido a variaciones estadísticas, una adecuada selección y combinación de las diferentes medidas puede resultar más eficaz a la hora de determinar si un CDP de prueba se ha registrado a partir de una forma analógica original o una forma analógica no original.

La figura 6 representa (605) la correlación entre las energías de las frecuencias en el CDP original y el CDP de prueba del documento que se autentica para treinta bandas de frecuencia (603). Como era de esperar, la correlación entre las energías es más alta en las bandas de frecuencia baja, de las cuales se ha perdido poca información en el procedimiento de copia, y más baja en las bandas de frecuencia alta, en las que incluso una sola operación de impresión causa la pérdida de la mayor parte de la información. Si en las bandas de frecuencia intermedia las correlaciones son considerablemente inferiores a lo que serían por término medio en los CDP de documentos originales, el CDP no es original y, por consiguiente, tampoco lo es el documento que se autentica. Este es el caso del gráfico de la figura 6, que por lo tanto demuestra que el documento que se autentica no es original.

También se pueden tomar en consideración otras características de la imagen cuando los valores de correlación por sí solos no son suficientes para determinar si un documento es una forma analógica original o una forma analógica no original. Otras características de la imagen que se pueden utilizar para generar valores de correlación entre el CDP original y el CDP de prueba comprenden:

- histograma de color
- borde, línea y contorno
- frecuencias en otros dominios (tales como los dominios de Fourier y Wavelet)
- brillo y contraste

Cómo detectar si un CDP procede de un documento original o un documento no original

La función *detect_pattern* analiza los resultados obtenidos mediante *analyze_pattern* y genera el valor *Output*, que indica si un CDP procede de un documento original o un documento no original.

Output = detect_pattern (Results, Parameters)

Results: puede ser un valor escalar o un vector, la salida de la función *analyze_pattern.*

Parameters: valores necesarios para ajustar el comportamiento de la función de detección, que puede depender de los requisitos de la aplicación y las condiciones en las que se lleva a cabo la detección.

Output: son posibles distintos valores de salida. En su forma más simple, *Output* puede adoptar tres valores: ORIGINAL, NON-ORIGINAL o PROCESSING-ERROR. La última salida puede obtenerse cuando el patrón se ha registrado incorrectamente. *Output* puede generar información más detallada, por ejemplo, NON-ORIGINAL puede indicar además cómo se ha creado el patrón de prueba a partir del documento no original (por ejemplo, mediante duplicación, fotocopia, regeneración, etc.). *Output* puede facilitar además índices de calidad o de concordancia.

A continuación, se describe un ejemplo del algoritmo para una función de detección simple:

1. Combinación de los diversos valores de *Results* calculados mediante *analyze_pattern* para obtener un valor escalar *S.* Una forma de realizar esta operación sería la de generar *S* sumando los valores de *Results* obtenidos.

2. Si S>T1, la salida es ORIGINAL; si S>T2, la salida es NON_ORIGINAL, de lo contrario, la salida es PROCESSING ERROR.

En este caso T1 y T2 son dos parámetros escalares obtenidos habitualmente a través de un procedimiento de entrenamiento, en el que por lo general T1>T2.

<u>Resincronización local del CDP del documento con el CDP original</u>

Para comparar el CDP registrado a partir del documento con el CDP original, el CDP registrado debe sincronizarse con el CDP original. Una manera de realizar esta operación consiste en utilizar puntos de sincronización en el CDP registrado, por ejemplo, el borde negro 601, para sincronizar el original. Una vez que los CDP están sincronizados, la comparación entre estos se realiza de píxel en píxel o de bloque en bloque.

Cuando se han producido errores en la impresión del CDP del documento o en el registro digital del CDP del documento, los CDP no pueden sincronizarse con precisión mediante este procedimiento. Por ejemplo, podría haber menos de un desplazamiento de píxel entre el CDP original y el registrado a partir del documento. Por otra parte, el desplazamiento puede variar a lo largo del patrón: en algunos casos, la parte superior del CDP registrado puede desplazarse hacia abajo comparado con el CDP original, y la parte inferior, desplazarse hacia arriba (o viceversa, por supuesto). Estos desplazamientos pueden ser muy difíciles de advertir, pueden producirse de manera no coherente y pueden variar localmente en el patrón registrado. Por lo general son causados por ligeras inestabilidades de la impresora, pero también pueden ser causados por inestabilidades similares del dispositivo de registro.

Estos desplazamientos de subpíxel impredecibles pueden reducir la eficacia del detector y, debido a estas desalineaciones, puede considerarse erróneamente que algunos CDP de documentos originales proceden de documentos no originales. Uno de los procedimientos para hacer frente a estos CDP "patológicos" procedentes de documentos originales y, en general, de aumentar la estabilidad de la detección de los CDP consiste en resincronizar localmente los CDP a fin de corregir las desalineaciones locales. Hay varias maneras de realizar la resincronización local, aunque la idea general consiste en utilizar el propio CDP registrado para la resincronización local.

Una manera de realizar la resincronización local consiste en dividir el CDP original en bloques (aunque los bloques pueden superponerse, es preferible que esto no ocurra) y encontrar qué bloque del CDP presenta la mayor coincidencia con un bloque determinado del CDP original. Si no hubiera desalineaciones, el bloque del CDP registrado que coincidiera más con el bloque determinado se hallaría en la misma posición en el CPD registrado que tenía el bloque determinado en el CDP original; por ejemplo, la mayor coincidencia para el bloque 10x10 con posición inicial (80,80) y posición final (89,89) del CDP original se daría en el correspondiente bloque (80,80) a (89,89) del CDP registrado. No obstante, si hay una desalineación, la mejor coincidencia podría darse también con el bloque (81,80) a (90,89) (desplazamiento de un píxel hacia la derecha). Si ese es el caso, entonces el patrón registrado presentará el bloque (81,80) a (90,89) desplazado 1 píxel hacia la izquierda, hasta la posición (80,80) a (89,89). Puede aplicarse la misma idea a cada bloque del CDP registrado para obtener un CDP "resincronizado localmente".

La resincronización local requiere un par de parámetros y funciones. En primer lugar, debe definirse una medida de la distancia entre cada bloque del CDP original y un bloque de las mismas dimensiones del CDP registrado. Una medida conveniente para este propósito es el coeficiente de correlación estándar. También es necesario establecer las dimensiones de los bloques en los que el CDP original se divide: normalmente puede utilizarse un bloque de dimensión 8x8 o 16x16, pero en general pueden utilizarse bloques de tamaño NxM. Como se ha mencionado anteriormente, los bloques pueden estar superpuestos, en cuyo caso, es necesario definir la cantidad de superposición entre bloques consecutivos. Otro parámetro que debe establecerse es el rango de búsqueda o el área de búsqueda: empezando por las posiciones coincidentes, ¿hasta qué punto debería buscar el algoritmo un bloque coincidente? Esto se establece con un parámetro *n*, según el cual se comprueban todos los bloques con la posición *(x+/-i,y+/-i)*, siendo *0<i<n*, empezando por la posición *(x,y)* del CDP original.

También es posible cambiar la escala del CDP digital y el registrado antes de realizar la sincronización local, lo cual permite lograr una coincidencia de grano más fino. Por ejemplo, cambiando los dos CDP a escala 2, se pueden recuperar desplazamientos de medio pixel. Y, por último, el algoritmo de sincronización puede aplicarse repetidamente al CDP resincronizado hasta que no se obtiene ninguna mejora.

Una vez que se ha realizado la resincronización, puede calcularse una medida arbitraria de la similitud o disimilitud entre el CDP registrado y resincronizado y el CDP original. Puede realizarse una correlación simple, o un análisis de frecuencias locales, posiblemente con parámetros basados en un conjunto de entrenamiento. Sin embargo, estas medidas, que suelen constituir el promedio de ciertas cantidades del conjunto del CDP, no siempre pueden ser resistentes a ciertos daños locales que pueden producirse en ciertas aplicaciones sufridos por el CDP escaneado. Por ejemplo, en algunos casos, un área del CDP puede haberse imprimido incorrectamente o puede haber resultado dañada por arañazos, escritura o agua. En otros casos, el dispositivo de escaneo puede haber añadido distorsión al CDP escaneado, siendo este problema habitual en los dispositivos de alimentación automática cuando el documento no se inserta correctamente. Para conferir al CDP más resistencia contra estos tipos de distorsión, pueden utilizarse medidas de similitud más sólidas: una de dichas medidas es la mediana de los coeficientes de correlación local, según la cual se calcula un coeficiente de correlación para cada bloque del CDP y, a continuación, la mediana de todos los coeficientes de correlación local. En este caso, el cálculo de la mediana en lugar del promedio confiere al detector una resistencia mucho mayor a las alteraciones locales. Para hacer frente a una mayor cantidad de áreas dañadas en el CDP, también es posible calcular el promedio de solo el 20 % de los mejores coeficientes de correlación local, que se puede suponer que no están dañados. En una implementación, se aplica este tipo de procedimiento de cálculo de promedio "sesgado" a cada canal de frecuencia por separado y, opcionalmente, a diferentes canales de color. Es por supuesto posible aplicar las técnicas de sincronización anteriores no solo a los CDP, sino a cualquier patrón de autenticación visible registrado que deba sincronizarse con un patrón de autenticación visual original.

Aplicaciones de los CDP

Los CDP pueden utilizarse en cualquier situación en la que sea útil distinguir un documento original de un documento no original. Un CDP puede imprimirse mediante cualquier procedimiento que logre imprimir el CDP con suficiente fidelidad como para que un registro digital del CDP sea comparable con la representación digital original del CDP. El patrón puede estar particularmente adaptado para detectar documentos no originales creados mediante técnicas de fotocopia, escaneo o impresión particulares. Los usos particulares de los CDP comprenden:

1. Impresión de un CDP en el embalaje para la protección de la marca

2. Impresión de un CDP en cheques y moneda para la detección de copia

3. Impresión de un CDP en documentos de valor, incluidos certificados, contratos, etc. para verificar si el documento es original o una copia.

4. Impresión de un CDP en hologramas

5. Impresión de un CDP en etiquetas de objetos de valor, tales como piezas de aviación o automoción o fármacos.

De forma más general, los CDP pueden utilizarse en cualquier aplicación en la que sea deseable poder determinar qué procedimientos se han aplicado a un documento. El patrón puede por supuesto variarse según se requiera para detectar mejor los procedimientos deseados.

Los CDP también pueden utilizarse para las siguientes aplicaciones:

1. Evaluación comparativa de la calidad de impresión

Durante la lectura del CDP, se calcula un índice de calidad del registro digital del CDP. Este índice de calidad variará según la calidad de impresión, la calidad del papel o sustrato o la calidad de la digitalización o el escaneo o del dispositivo que lleva a cabo estos procedimientos. El índice de calidad del CDP puede utilizarse a continuación para cuantificar la calidad de un determinado procedimiento de impresión, un determinado sustrato o un determinado escáner.

2. Control de calidad

En este sentido, el lector de CDP puede utilizarse en un procedimiento de obtención de impresión para el control automático de la calidad. Las ventajas del CDP respecto de la inspección manual es que proporciona una medida automatizada, objetiva y precisa de la calidad.

3. Rastreo

El CDP presenta una estructura y unas características asociadas a la impresora, el papel, la cámara, el uso y el desgaste. En principio, el análisis del CDP puede determinar la "historia" general del documento, es decir, cómo se ha imprimido y qué desgaste por uso ha sufrido.

Utilización de patrones de autenticación visibles para detectar alteraciones en los documentos: figura 10

Ciertas clases de documentos sufren siempre "modificaciones" una vez impresos. Un ejemplo común de lo anterior es el de un cheque impreso con campos en blanco que se cumplimentan en el momento de extender el cheque. Uno de los problemas de los documentos pertenecientes a todas estas clases es que lo que se introduce en los campos que se cumplimentan puede alterarse posteriormente. Por lo tanto, aunque el cheque sea auténtico, los valores semánticos de lo escrito en los campos en blanco pueden cambiarse. Por ejemplo, el beneficiario de un cheque puede modificar el importe de un cheque a su nombre (por ejemplo, de "cien" a "novecientos"), de una manera que es difícil de detectar por el personal de caja.

Este tipo de problema es difícil de resolver, porque los falsificadores en realidad no crean documentos falsos, sino que alteran el valor semántico de documentos auténticos. El problema todavía se complica más, porque el documento auténtico cumplimentado ya contiene modificaciones legales. El problema que se plantea es cómo se pueden diferenciar las modificaciones legales del documento de las modificaciones ilegales posteriores.

Una de las soluciones a este problema es el examen forense. Si el personal de caja sospecha que el talón ha sido modificado, puede solicitar un examen más detenido a un experto. Sin embargo, esta tarea es manual, costosa y lenta y, evidentemente, no es posible aplicarla sistemáticamente a cada documento o cheque. A menudo, los cheques se falsifican borrando primero parte de lo escrito. Por ejemplo, para modificar el importe de "doscientos" a

"novecientos", probablemente se borre la parte "dos" y se cambie por "nove". Para borrar manuscrito, se suelen utilizar productos químicos. Otra posibilidad consiste en raspar el importe original del cheque, volver a pintar el fondo y, a continuación, escribir el nuevo importe.

Los patrones de autenticación visibles se pueden utilizar para detectar estas modificaciones ilegales. La idea general de este procedimiento consiste en imprimir un VAP en cada una de las áreas del documento donde se desean detectar las modificaciones ilegales. A continuación, se crean las modificaciones legales escribiendo en el VAP. La estructura precisa, única e incopiable del VAP puede utilizarse más adelante para detectar modificaciones y determinar si las modificaciones son aceptables. La idea es que tanto la escritura en un VAP como el borrado de escritura en un VAP acarreen modificaciones detectables en el VAP. La escritura en el VAP destruye el patrón, al igual que el raspado de la escritura del VAP o la aplicación de un agente de borrado químico al VAP. Un VAP que se utiliza de este modo se denominará en lo sucesivo *patrón de detección de modificación* o *MDP.*

La manera en que puede utilizarse un MDP para detectar modificaciones ilegales puede resumirse como sigue:

- Inserción de un MDP en cada área del documento que necesita protección contra modificaciones no autorizadas.
- Cuando se verifica la autenticidad del documento, en primer lugar, registro de una imagen de cada uno de los MDP del documento.
- Para cada MDP registrado, comparación del MDP registrado con la representación digital original del MDP para detectar las áreas en las que el MDP se ha dañado.

Los resultados de la comparación del MDP registrado con la representación digital original del MDP pueden utilizarse de varias maneras:

- Presentación de los resultados de la comparación con las áreas dañadas resaltadas a la persona que toma las decisiones. De esta forma, se mostrarán las áreas que contienen escritura y las áreas borradas.
- Presentación de los resultados de la comparación con las áreas dañadas no escritas resaltadas a la persona que toma las decisiones.
- Comparación del tamaño del área dañada con el tamaño del área donde se ha escrito y, si la diferencia es superior a un umbral, tratamiento del campo como modificado.

La figura 10 representa cómo puede utilizarse un MDP para detectar modificaciones. En 1001, se representa un MDP 1002 que se utiliza en un campo de importe de un documento. Igual que en el caso anterior, el MDP 1002 está rodeado de un borde negro 106. Como se indica en 1003, se ha escrito el importe 250 en el MDP 1002. En 1005, puede observarse cómo el falsificador ha modificado el importe de 250 $ como importe 950 $ borrando la "cola" del 2 y añadiendo un bucle para convertirlo en el número 9. Para encubrir el borrado, el falsificador ha imitado el patrón del MDP. La imitación aún es visible en 1005, pero incluso tal como aparece en la figura, es suficientemente buena como para pasar desapercibida para el personal de caja en condiciones de especial ajetreo, aunque fácilmente perfeccionable por los falsificadores expertos.

El problema de este tipo de falsificación es que el borrado ha destruido el MDP. Mediante el escaneo del MDP y el análisis local de este, es posible detectar con gran precisión qué parte del MDP ha cambiado con respecto al original. Los borrados pueden detectarse hallando áreas del MDP que no contienen ni texto ni el patrón original. Esto se representa en 1009. Las áreas de texto son fáciles de encontrar, porque normalmente son de un color uniforme y más oscuro que el MDP. Para encontrar las áreas borradas, basta pues con comparar las áreas del MDP registrado que no contienen texto con la representación digital original del MDP. Las áreas borradas aparecen como partes del MDP registrado que no coinciden con la representación digital original, tal como se representa en 1011. En una forma de realización preferida, dichas partes no coincidentes aparecen en color rojo.

A continuación, se indican algunos detalles adicionales sobre el algoritmo para utilizar un MDP a fin de detectar la alteración de un documento:

- Creación de MDP: Un MDP puede crearse de cualquiera de las maneras en que se crea un VAP, pero a continuación los valores de los píxeles se incrementan para hacer más claro el MDP (de lo contrario, el texto escrito en el MDP no podría distinguirse con facilidad del MDP).
- Utilización de marcas de registro (por ejemplo, un borde negro o marcas de esquina) para extraer el MDP registrado del documento.
- Detección de áreas de texto: se aplica un filtro pasabaja al MDP registrado, y se considera que los píxeles con valores por debajo de un umbral forman parte del texto y las modificaciones legales.

- Detección de modificaciones del MDP: una vez que se ha aplicado la resincronización local, se calcula un coeficiente de correlación para cada bloque del MDP. Tal como se muestra en 1009, puede observarse que las áreas del texto y las áreas de la modificación ilegal se han alterado.

- Mediante exclusión de las modificaciones legales (1003) de la imagen 1001, posibilidad de aplicación de varios algoritmos para detectar las modificaciones ilegales. Un sistema posible consiste, en primer lugar, en clasificar áreas en "modificadas" o "no modificadas" (mediante umbralización de la correlación local) y, a continuación, aplicar un algoritmo de procesamiento de ruido o filtro pasabaja que elimine áreas individuales o no significativas modificadas. También pueden aplicarse algoritmos de detección de zona para encontrar zonas significativas modificadas. El resultado se representa en 1009: las modificaciones no permitidas aparecen en rojo, mientras que las áreas permitidas (del texto) aparecen en verde.

- Dependiendo de la cantidad de modificaciones no permitidas, posibilidad de toma opcional de decisión sobre la autenticidad del documento al que pertenece el MDP.

Detalles de implementación del VAP

Forma del VAP en el documento

Para utilizar un VAP con el fin de detectar alteraciones en una forma analógica, basta con que exista un área en la forma analógica que presente un patrón que sea útil para estos efectos y una representación digital original del patrón que pueda compararse con el patrón registrado a partir de la forma analógica. Será pues posible utilizar en ciertos casos un patrón preexistente en una forma analógica para la técnica. Más comúnmente, el VAP se integrará como una parte del diseño de una nueva forma analógica. Como es obvio, no hay ninguna necesidad de ocultar el VAP en la forma analógica y, de hecho, en algunos casos puede informarse de su presencia para dar confianza a los clientes con respecto a la capacidad de detección de las formas analógicas ilegítimas. Por otro lado, el VAP puede adoptar cualquier forma y, por lo tanto, puede integrarse con facilidad en otras características de la forma analógica. En la figura 11, se representan dos ejemplos. En 1101, se representa un código de barras cuyas barras conforman el VAP. En 1103, se representa un logotipo que contiene el VAP. Evidentemente, es posible que exista más de un VAP en un documento y que más de un VAP compartan una ubicación. Esto se puede llevar a cabo, asignando a cada patrón un valor ponderado, de tal forma que la suma de los pesos de todos los patrones sea igual a uno, por ejemplo:

*Final_pattern=a*pattern1+(1-a)*pattern2, siendo 0<a<1.*

Una de las aplicaciones de los diversos patrones sería la autenticación de contratos, en la que cada parte añadiría su propio patrón al firmar el contrato o concluir una fase de las negociaciones.

También es posible insertar varios CDP en diferentes lugares de un documento, creados habitualmente con claves diferentes, para permitir a las diversas partes verificar su propio CDP sin tener capacidad de verificar los CDP de las otras partes (y en consecuencia duplicarlos). Es posible incluso generar un CDP mediante claves diferentes (pudiendo cada clave controlar diferentes áreas espaciales o frecuenciales del CDP), a fin de permitir a las diferentes partes verificar el CDP. De esta manera, si una de las partes revela su clave, la clave no es suficiente para realizar una duplicación exacta del CDP (pues se necesitan todas las claves), y no se pone en peligro la seguridad. Este concepto es análogo al de "secretos compartidos".

Registro del VAP

La forma de realización preferida emplea un registro tipo "Black Box" 106 para el VAP. No obstante, pueden utilizarse muchas otras técnicas de registro. Por ejemplo, podrían utilizarse patrones visibles, tales como marcos, códigos de barras o similares que ya aparecen en el embalaje para localizar el VAP, así como OCR. También se pueden utilizar marcas UV o cualquier técnica descrita en la solicitud de patente principal USSN 10/287.206, J. Zhao, *et al.*, *Apparatus and methods for improving detection of watermarks in content that has undergone a lossy transformation,* presentada el 4/11/2002. Además, también se podría calcular la transformada de Fourier-Mellin del VAP registrado y compararla con la representación digital original del VAP.

En algunas aplicaciones, es difícil saber si la orientación del registro digital del VAP es la correcta o si debe voltearse (rotar 180 grados) antes de su lectura. Para evitar tener que analizar el VAP una vez y, si el análisis no resulta satisfactorio, girarlo después para orientarlo en la dirección vertical contraria y analizarlo nuevamente, es posible diseñar un VAP simétrico, en el que la parte inferior es la imagen especular de la parte superior. Entonces, el análisis del VAP podría realizarse independientemente de su orientación vertical.

Propiedades del patrón del VAP

El patrón puede ser un patrón en escala de grises o puede ser un patrón en color. En este último caso, se pueden

emplear diferentes canales de color, por ejemplo, RGB y YUV. Asimismo, el patrón puede generarse en diversos dominios de frecuencia, por ejemplo, espacial, wavelet, DFT o DCT.

Generación del VAP

El ruido, es decir, la naturaleza aleatoria, del VAP es lo que dificulta su manipulación por los falsificadores. Cualquier técnica que pueda generar un patrón aleatorio o pseudoaleatorio servirá para generar el VAP. En la forma de realización preferida, la generación tiene lugar aportando un valor a un generador de números pseudoaleatorios que genera una secuencia de números aleatorios que es exclusiva para el valor. El valor sirve pues de clave para generar nuevas copias del patrón. Pueden utilizarse diferentes generadores de números pseudoaleatorios en diferentes formas de realización, y los valores de frecuencia probabilística para los números aleatorios generados pueden obtenerse a partir de diferentes distribuciones de probabilidad. La clave también puede utilizarse para determinar las ubicaciones del VAP en las cuales se realiza el análisis. Como se indicará más adelante con referencia a la utilización del VAP para transmitir otro tipo de información, la clave puede comprender dicho otro tipo de información. En algunas aplicaciones, la clave utilizada para diseñar el patrón no puede revelarse a otras partes. En ese caso, puede adoptarse cualquier sistema para distribuir las claves que resulte útil, por ejemplo, el de las claves asimétricas o los pares de claves públicas-privadas.

El patrón puede combinarse con un logotipo, ya sea añadiendo el logotipo al patrón o viceversa. El logotipo puede ser cualquier imagen o documento existente, incluidas imágenes para otros fines (un código de barras 2D, una imagen con marca de agua, etc.). También es posible aplicar cualquier procedimiento, tal como un filtrado, al patrón o al logotipo, de tal forma que el logotipo interfiera al mínimo con la comparación entre el VAP registrado y la representación digital original del VAP.

Impresión del VAP

La calidad de la autenticación lograda por el VAP depende completamente de la fidelidad con la que se imprime el VAP en el documento. Los errores de autenticación se pueden reducir si se añade una etapa de "control de calidad" al final del procedimiento de impresión para garantizar la fidelidad del VAP:

1. Cada VAP impreso se someterá a un proceso de verificación automática para comprobar si el patrón de autenticación es de la calidad mínima necesaria para ser reconocido como original.

2. Si la calidad es inferior a la mínima, se generará una alerta y se reimprimirá el documento/embalaje que contiene el patrón de autenticación.

3. Dicha verificación puede servir asimismo como "control de calidad" para la calidad de impresión o los errores introducidos por la impresora.

La generación del VAP puede adaptarse a la tecnología de impresión. Por ejemplo, si se utiliza una impresora láser que imprime solo puntos binarios, puede generarse un VAP de puntos binarios para aprovechar mejor las prestaciones de la impresora. Asimismo, es posible generar e imprimir un VAP de forma más adecuada en el espacio de color de la impresora. Si una determinada impresora utiliza tintas específicas (por ejemplo, CMYK), puede resultar más eficaz generar el VAP en ese dominio que en el dominio RGB. Si el VAP se graba en metal con una grabadora láser capaz de generar solo puntos binarios, entonces tendría más sentido generar un VAP binario.

Utilización del VAP para transmitir otro tipo de información

A continuación, se describirán tres sistemas de utilización del VAP para transmitir otro tipo de información: reserva de determinadas áreas del VAP para almacenar información, utilización del resto de la información para generar la clave utilizada para crear el VAP original y adición de una marca de agua al VAP. La desventaja de la adición de una marca de agua es que reduce la capacidad del VAP de detectar formas analógicas no originales o modificaciones en el VAP.

Reserva de áreas del VAP para almacenar información

Pueden reservarse ciertas áreas (por ejemplo, bloques 8x8) del VAP para almacenar información. En esas áreas, la estructura y las características del VAP no se utilizan realmente para verificar su autenticidad, sino para almacenar algunos bits de información. Estas áreas pueden seleccionarse pseudoaleatoriamente mediante una clave, de tal forma que una entidad que no posea la clave no podrá determinar si un área del VAP se utiliza realmente para almacenar información o para determinar la autenticidad del VAP. En un área que se utiliza para almacenar información, cierta estructura y características del VAP pueden corresponder a cierto valor de bit ("0" o "1") de información. Esta estructura o características dependientes del valor de bit pueden, por supuesto, variar de conformidad con la clave. Debe tenerse en cuenta que las áreas reservadas y la información que estas contienen forman parte del VAP desde que se genera. Por lo tanto, no degradan la capacidad del VAP de detectar documentos no auténticos. Uno de los usos de las áreas reservadas es almacenar la clave utilizada para generar el VAP.

Utilización de la información para generar la clave del VAP

Se va a utilizar la terminología siguiente: el VAP se crea y detecta con una clave P; puede desearse utilizar una clave diferente *S* para incorporar un mensaje al patrón tal como se ha descrito anteriormente con referencia a las áreas reservadas o como se describe más adelante con referencia a las marcas de agua; se incorpora un mensaje M al VAP mediante la clave S y, por último, puede imprimirse información adicional I de forma visible en el documento (número de serie, código de barras, etc.), o de forma invisible mediante codificación UV, dentro del patrón o fuera de este, o puede obtenerse a partir de una fuente externa.

Clave de patrón fija

En una forma de realización, la clave de creación del VAP es una clave fija *P.* Esto es lo que sucede comúnmente en la tecnología de impresión offset estándar, donde la tecnología de impresión no tiene la capacidad de cambiar el patrón dinámicamente para cada embalaje/producto/documento. La clave se puede mantener en secreto como se ha descrito anteriormente o puede incorporarse a otras características de seguridad. Por ejemplo, podría imprimirse con tintas UV en el documento. La clave de patrón fija puede utilizarse para protección de marcas o protección de documentos en general.

Clave de patrón variable En otra forma de realización, la clave del VAP depende de una clave secreta *S* y otro tipo de información *I.* Este otro tipo de información *I* puede aparecer en el documento (dentro del patrón o fuera de este) u obtenerse a partir de una fuente externa. La información del documento puede ser, por ejemplo, un número de serie, un texto, un código de barras, etc. La información de la fuente externa puede ser, por ejemplo, un valor que está asociado al VAP y es conocido por la persona que verifica si el documento que contiene el VAP es auténtico. La clave del patrón puede ser cualquier función arbitraria *P=f(S,I)* de los parámetros constituidos por la clave secreta y la información *I.* Una función simple sería la de concatenar o sumar los dos parámetros, pero son posibles muchas otras funciones, tales como un valor hash de una combinación de los dos parámetros, etc. En el momento de la detección, la información impresa *I* se extrae con una tecnología adecuada: lector de códigos de barras, OCR, etc. A continuación, se genera la clave del patrón según *P=f(S,I)*, y se analiza el patrón. Los usos habituales comprenden la protección de marcas con impresión digital.

Marcas de agua en el VAP

Es posible incorporar una marca de agua visible o invisible al VAP mediante cualquier técnica de incorporación de marcas de agua. La marca de agua puede cumplir varios propósitos. Puede contener cualquier tipo de información, incluido un solo bit, tal como se ha indicado anteriormente, o facilitar el registro del patrón. La marca de agua puede detectarse con la clave utilizada para generar el VAP o con otra clave que limita su lectura a otro usuario o grupo de usuarios. Una tercera posibilidad, que se describe más adelante, es la de utilizar el mensaje contenido por la marca de agua para obtener la clave utilizada para generar el VAP.

Cuando se incorpora una marca de agua digital a un VAP, el VAP puede sufrir ligeras modificaciones. Como consecuencia, si se utiliza el mismo VAP para la verificación de la autenticidad, su fiabilidad para este propósito puede reducirse. Como alternativa, la marca de agua digital puede incorporarse a áreas del VAP que están reservadas para almacenar información tal como se ha indicado anteriormente.

Marcas de agua y claves

En otra forma de realización, la clave de creación del patrón *P* se obtiene a partir de la clave secreta *S* y el mensaje *M* incorporado como una marca de agua digital al patrón de detección de copia. En este caso, *M* ocupa el lugar de la información *I* utilizada para crear la clave de patrón variable descrita anteriormente. En el momento de su creación, la clave del patrón *P* puede ser cualquier función de la clave secreta *S* y el mensaje *M, g*(*M,S*). El patrón se genera de la manera habitual y, a continuación, se inserta a este una marca de agua que codifica el mensaje *M* utilizando la clave secreta *S* como parámetro. En el momento de la detección, primero debe leerse el mensaje de la marca de agua *M* del patrón con la clave secreta *S.* Una vez que se conoce *M*, se obtiene la clave del patrón *P=g*(*M,S*) y se analiza el patrón.

En este marco de aplicación, no se necesitaría ninguna tecnología auxiliar para extraer más información impresa en el embalaje. Sin embargo, también es posible utilizar de varias maneras la información *I* impresa en el embalaje dentro del principio descrito en la presente memoria. Por ejemplo, la clave secreta *S*, puede utilizarse junto con la información *I* para generar una clave de marca de agua *W*, es decir*, h(S,I)=W,* que se utiliza para incorporar el mensaje al patrón. A continuación, se genera la clave del patrón de la misma manera que antes, *P=f(M,W)=f(M,h(S,I)).* En general, los VAP pueden combinarse con la tecnología de marcas de agua y otras tecnologías de lectura (lectores OCR o de códigos de barras, por ejemplo), para ofrecer distintos niveles de verificación.

Comparación de VAP

La manera de comparar los VAP registrados con las representaciones digitales de los VAP dependerá de cómo se ha creado el VAP y cuál es su función. Algunas variantes de aplicación general comprenden la evaluación independiente de ciertas áreas, ya sea para obtener más indicaciones sobre qué procedimiento se ha aplicado al documento, o bien por cuestiones de seguridad. Tal como se ha descrito anteriormente, un VAP puede contener más de un patrón de autenticación, y los diferentes patrones pueden ser analizados por diferentes grupos.

Para poder comparar significativamente los VAP, tal vez sea necesario "entrenar" el programa de comparación con unos VAP registrados a partir de documentos originales, tal como se ha descrito anteriormente para los CDP. El entrenamiento establece los umbrales para determinar si un VAP registrado a partir de un documento cuya autenticidad se examina es auténtico o no. El significado del umbral dependerá, por supuesto, de la clase de alteración que se pretende detectar con el VAP. Es necesario efectuar un reentrenamiento cada vez que varía la manera en que se imprimen los documentos originales de una forma que afecta a la comparación de los VAP. El entrenamiento puede tener lugar de forma automática imprimiendo una serie de VAP en una hoja de papel, escaneando la hoja y facilitando la hoja escaneada al software de entrenamiento.

En otra forma de realización, en lugar de comparar el registro digital de un VAP de prueba con una correspondiente representación digital para medir su índice de calidad, es posible comparar el registro digital con un registro digital de otro VAP (normalmente, un VAP original que se ha escaneado).

Entornos en los que se realiza un análisis de VAP

Lo que se necesita para analizar un VAP es un dispositivo que pueda registrar el VAP a partir del documento con el cual se va a crear el VAP registrado, una copia de la representación digital original del VAP y un procesador que pueda comparar el VAP registrado con la representación digital original del VAP. El registrador y el procesador pueden hallarse en el mismo entorno local o estar conectados por una red. La red puede ser una red de área local (LAN) o una red de área extensa (WAN). Un ejemplo de entorno local es un procesador de un PC provisto de un escáner, una copia del código de análisis y una copia de la representación digital original del VAP. La copia de la representación digital original del VAP puede descargarse o generarse localmente mediante una clave. Los resultados de los análisis se facilitan al dispositivo de pantalla del PC.

En un entorno de red, el escaneo, el análisis y la representación digital original del VAP pueden distribuirse por la red de cualquier manera. Una de las distribuciones que mantiene la seguridad de la representación digital original del VAP y simplifica el equipo necesario a nivel local es una en la que el escaneo se realiza en un dispositivo que está conectado a una WAN. Cuando el VAP del documento se ha escaneado para generar el VAP registrado, el VAP registrado se envía a una ubicación de la WAN donde están disponibles tanto el código de análisis como una representación digital original del VAP. La representación digital original se puede almacenar o regenerar según las necesidades. El análisis se efectúa en esa ubicación, y solo se presenta el resultado del análisis a través de la WAN al dispositivo utilizado para escanear. Generalmente, en los entornos de red, la información transmitida o enviada con el VAP registrado puede utilizarse para recuperar información que se va a utilizar en el análisis. Por ejemplo, el documento puede contener un número de serie, y el número de serie puede enviarse con el VAP registrado a la ubicación donde se realiza el análisis. Si existe una asociación entre los VAP y los números de serie, el número de serie podría aplicarse a una base de datos de la ubicación o a cualquier otro lugar de la red para recuperar la clave para la representación digital original del VAP que debe compararse con el VAP registrado o una copia de la representación digital original del VAP. Como se ha descrito anteriormente, el número de serie podría especificarse en un código de barras que contiene el VAP, podría aparecer como una marca de agua visible en el VAP, podría someterse a OCR a partir del documento o incluso podría ser introducido por la persona que realiza el escaneo.

Puede utilizarse también una cámara (cámara web, videocámara, etc.) para captar imágenes del VAP. En este caso, el detector de VAP, no solo recibe una imagen como entrada, sino una secuencia constante de imágenes. La información adicional aportada por varias imágenes puede ser potencialmente muy útil para el análisis. Sin embargo, como el tiempo necesario para analizar una imagen puede superar de manera sustancial el tiempo entre dos imágenes consecutivas, el uso de la secuencia de imágenes puede mejorarse. Por ejemplo, las imágenes de la secuencia que parecen presentar las propiedades adecuadas para una correcta lectura (buena nitidez, VAP completamente abarcado por la imagen), pueden seleccionarse y utilizarse para el análisis.

Combinación de VAP con otras tecnologías de seguridad

Un VAP puede combinarse con otras tecnologías utilizadas para hacer más seguras las formas analógicas. Por ejemplo, el VAP puede utilizarse con técnicas de ocultación de información, tales como las marcas de agua digitales, con información legible por máquina, tal como los códigos de barras 1D o 2D, con hologramas o con cualquier otra tecnología que se pueda aplicar a una forma analógica. La relación entre las tecnologías puede ser muy variada; por ejemplo, un código de barras 2D puede contener información independiente o la clave secreta necesaria para el análisis de los patrones o, a la inversa, el VAP puede contener la clave necesaria para decodificar el código de barras 2D, o el código de barras 2D puede contener el VAP.

Conclusión

La anterior *Descripción detallada* ha dado a conocer a los expertos en las correspondientes tecnologías las técnicas de los inventores para determinar si una forma analógica de un objeto es una forma analógica original o una forma analógica no original, sus técnicas para utilizar los VAP en comprobaciones de la autenticidad de las formas analógicas y sus técnicas para utilizar los VAP en la ocultación de mensajes en las formas analógicas, y además ha dado a conocer a los expertos en las tecnologías pertinentes el mejor modo conocido actualmente por los inventores de llevar a la práctica las técnicas. Como apreciarán de inmediato los expertos en las correspondientes tecnologías, son posibles muchas formas de realización de las técnicas de los solicitantes, aparte de las dadas a conocer en la presente memoria. Por ejemplo, el tamaño, la forma y el patrón de un VAP vendrán determinados por la naturaleza de la forma analógica con la cual se utiliza el VAP y por la función del VAP. La manera en que un VAP transmite información adicional y la composición de esa información también vendrá determinada por la naturaleza de la forma analógica y por la función del VAP. En general, los VAP pueden utilizarse en cualquier situación en la que deban detectarse los cambios realizados tras haberse creado la forma analógica original. Si bien la aplicación da a conocer VAP impresos en documentos, es posible insertar unos elementos análogos a estos VAP impresos en las formas analógicas de otros medios.

Por todas las razones expuestas, la *Descripción detallada* no debe considerarse restrictiva, sino ejemplificativa en todos los sentidos, y el alcance de la presente invención dada a conocer en la presente memoria no debe determinarse a partir la *Descripción detallada,* sino a partir de las reivindicaciones interpretadas en toda la amplitud permitida por la legislación de patentes.

REIVINDICACIONES

1. Procedimiento para determinar si una forma analógica de un objeto es una forma analógica original, comprendiendo el procedimiento las etapas siguientes:

generar una representación digital original de un patrón de autenticación, siendo el patrón de autenticación un patrón de autenticación visible;

producir posteriormente por lo menos una forma analógica original que incluye el patrón de autenticación a partir de la representación digital original, que provoca una primera pérdida de información en dicha por lo menos una forma analógica original;

realizar un registro digital a partir del patrón de autenticación de dicha por lo menos una forma analógica original o de otro patrón de otra forma analógica derivada de dicha por lo menos una forma analógica original, que provoca una segunda pérdida de información en el registro digital;

comparar el registro digital con la representación digital original para determinar el grado de disimilitud entre el registro digital realizado y la representación digital original; y

utilizar el grado de disimilitud que es igual a la suma de la primera y segunda pérdidas de información para determinar que el registro digital se realizó a partir de dicha por lo menos una forma analógica original y utilizar el grado de disimilitud que es superior a la suma de la primera y segunda pérdidas de información para determinar que el registro digital se realizó a partir de la otra forma analógica.

2. Procedimiento según la reivindicación 1, en el que:

el procedimiento se lleva a la práctica en un nodo de una red y el procedimiento comprende además las etapas siguientes:

recibir el registro digital desde otro nodo de la red, realizándose el registro digital a partir de dicha por lo menos una forma analógica original o de la otra forma analógica.

3. Procedimiento según la reivindicación 1, en el que:

el procedimiento se lleva a la práctica en un nodo de una red y el procedimiento comprende además las etapas siguientes:

devolver una indicación a otro nodo que indica si se ha determinado que el registro digital se ha realizado a partir de dicha por lo menos una forma analógica original o de la otra forma analógica.

4. Procedimiento según la reivindicación 1, en el que:

el procedimiento se lleva a la práctica en un procesador al que están unidos un dispositivo de registro digital y un dispositivo de salida; y comprendiendo además el procedimiento las etapas siguientes:

realizar el registro digital a partir de la entrada recibida desde el dispositivo de registro digital; y

proporcionar una indicación que indica si se ha determinado que el registro digital se ha realizado a partir de dicha por lo menos una forma analógica original al dispositivo de salida.

5. Procedimiento según la reivindicación 1, en el que:

en la etapa de determinación de un grado de disimilitud, lo que se determina es la disimilitud de las características en el registro digital y la representación digital original, siendo causada la disimilitud por operaciones que comprenden el registro digital y la impresión implicadas en la realización de una forma analógica no digital.

6. Procedimiento según la reivindicación 1, en el que:

la representación digital original presenta un patrón con ruido perceptible por humanos en la forma analógica.

7. Procedimiento según la reivindicación 6, en el que:

el patrón con ruido se realiza utilizando una clave y el procedimiento comprende además la etapa siguiente:

utilizar la clave para generar la representación digital original.

8. Procedimiento según la reivindicación 6, en el que:

el patrón con ruido presenta una función en la forma analógica, además de la de permitir determinar si la forma analógica es dicha por lo menos una forma analógica original.

9. Procedimiento según la reivindicación 8, en el que:

un mensaje es derivado a partir del patrón con ruido.

10. Procedimiento según la reivindicación 9, comprendiendo además el procedimiento las etapas siguientes:

utilizar el mensaje para derivar una clave; y
utilizar la clave para generar la representación digital original.

11. Procedimiento según la reivindicación 9, en el que:

el mensaje se halla en unas partes del patrón con ruido reservadas para este propósito.

12. Procedimiento según la reivindicación 8, en el que:

por lo menos una parte del patrón con ruido se halla en una imagen de fondo o en un código de barras.

13. Procedimiento según cualquiera de las reivindicaciones 1 a 12, que comprende además la etapa siguiente:

utilizar el resultado de la etapa de comparación para llevar a cabo una comprobación de autenticidad en un autenticador.

14. Procedimiento según la reivindicación 13, en el que:

el resultado de la etapa de comparación indica una parte del patrón de autenticación registrado que se ha destruido en la forma analógica registrada.

15. Procedimiento según la reivindicación 13, en el que:

el resultado de la etapa de comparación indica una parte del patrón de autenticación registrado que procede de dicha por lo menos una forma analógica original.

16. Procedimiento según la reivindicación 13, en el que:

el patrón de autenticación contiene además un mensaje.

17. Procedimiento según la reivindicación 13, en el que:

el resultado de la etapa de comparación indica una parte del patrón de autenticación que se ha sobreescrito con texto escrito.

18. Procedimiento según la reivindicación 1, en el que:

la representación digital original es una imagen, y la etapa de producción de por lo menos una forma analógica original comprende la impresión de la imagen en el objeto.

19. Procedimiento según la reivindicación 18, en el que:

la representación digital original es una imagen en escala de grises o una imagen en color.

20. Procedimiento según la reivindicación 1, en el que:

la creación de una representación digital original comprende la creación de una representación digital original de un documento;

comprendiendo además:

la impresión del documento para generar dicha por lo menos una forma analógica original.

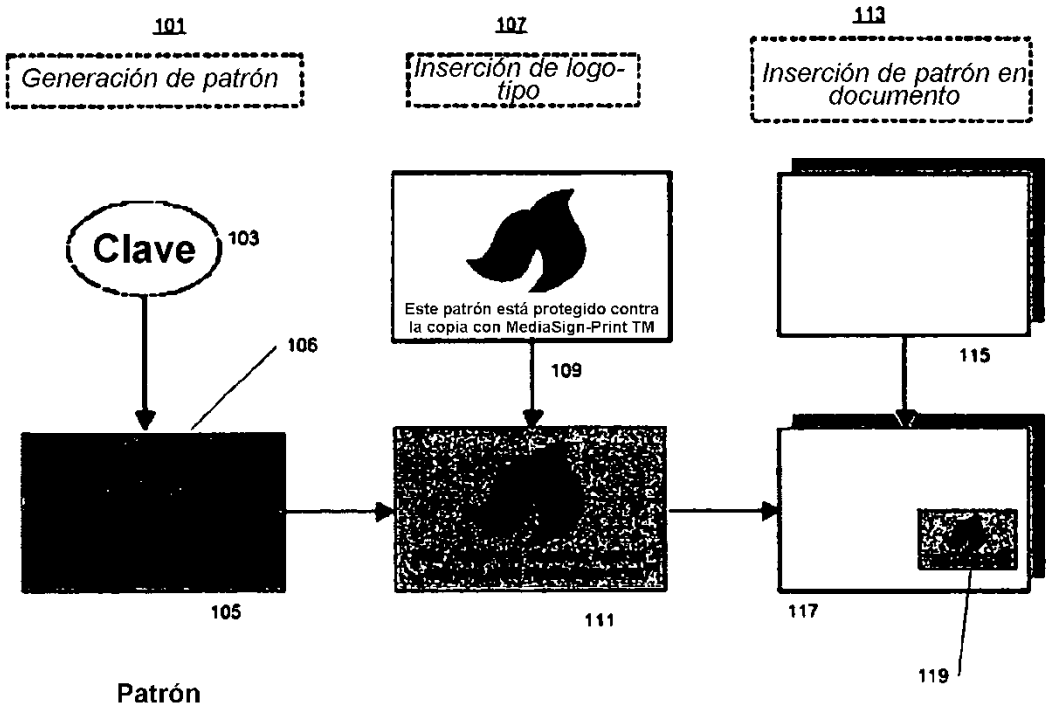

101
Generación de patrón
107
Inserción de logo-tipo
113
Inserción de patrón en documento
Clave
103
106
Este patrón está protegido contra la copia con MediaSign-Print TM
109
115
105
111
117
119
Patrón

Fig. 1

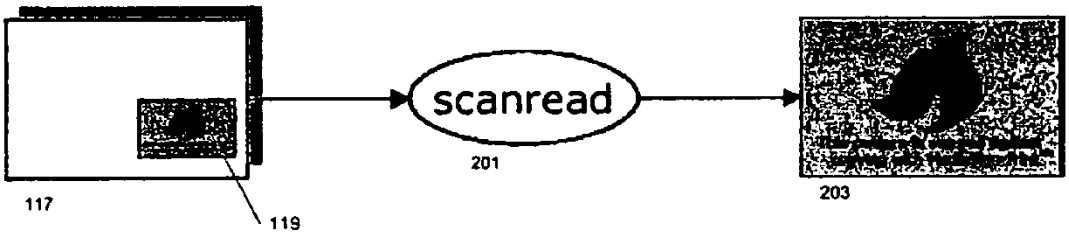


Fig. 2

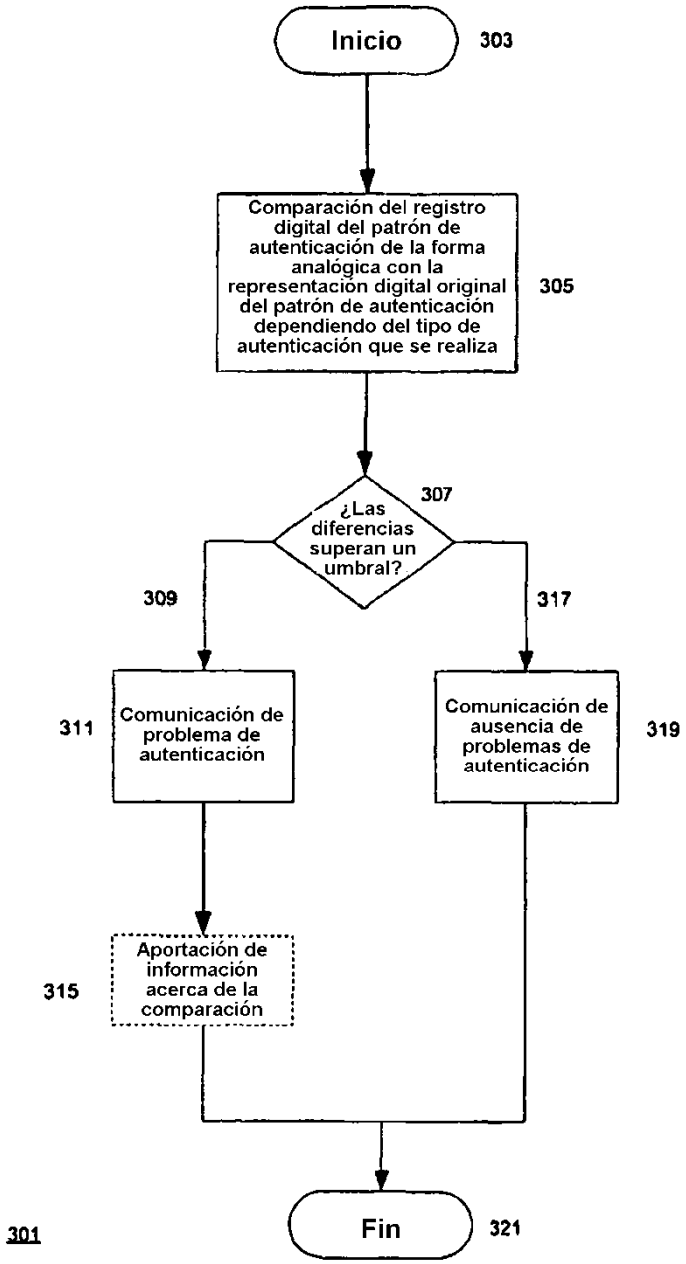
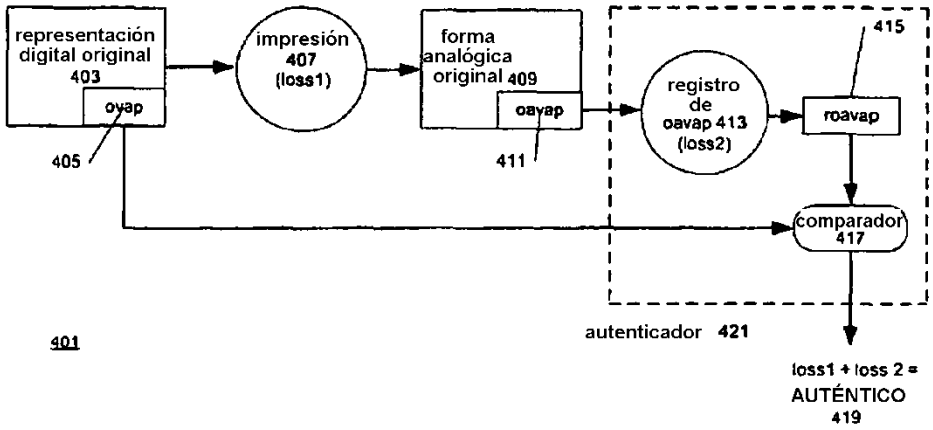

Inicio
303
Comparación del registro digital del patrón de autenticación de la forma analógica con la representación digital original del patrón de autenticación dependiendo del tipo de autenticación que se realiza
305
¿Las diferencias superan un umbral?
307
309
317
Comunicación de problema de autenticación
311
Comunicación de ausencia de problemas de autenticación
319
Aportación de información acerca de la comparación
315
Fin
321
301

Fig. 3

Situación hipotética 1:
impresión y autenticación de una forma analógica original



Situación hipotética 2:
impresión y autenticación de una forma analógica no original

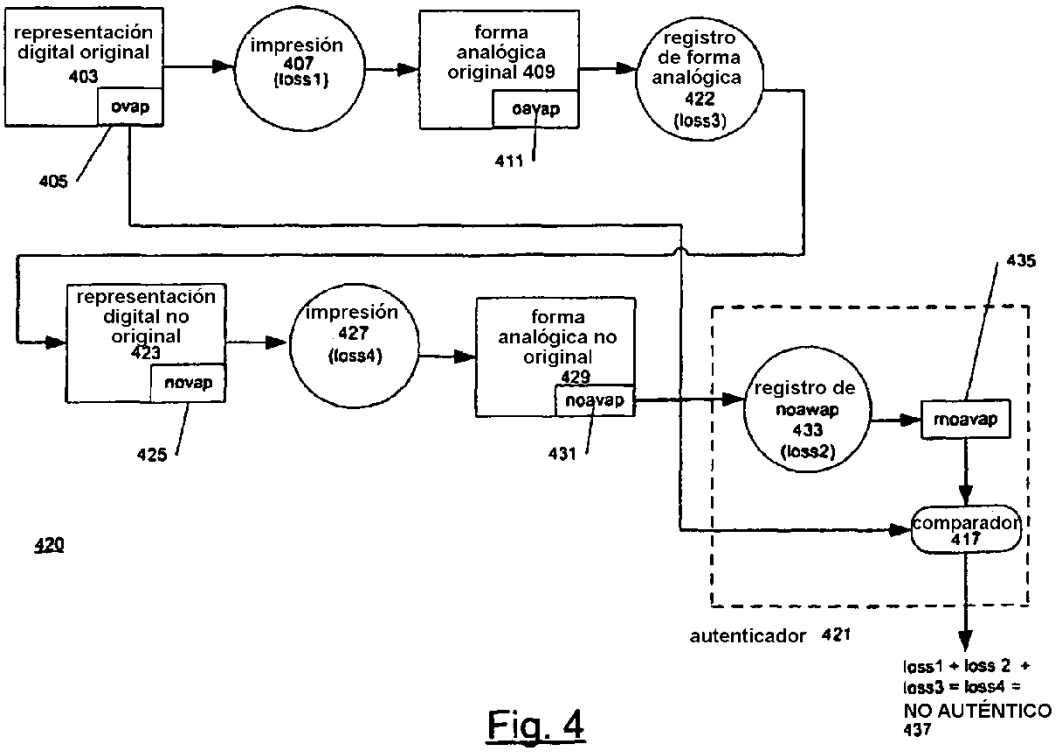
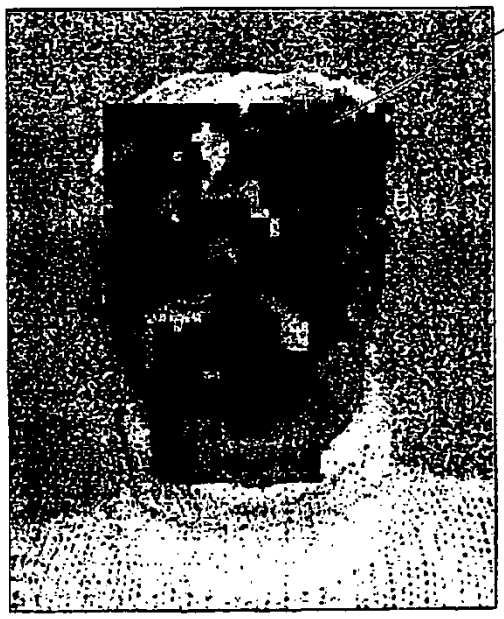


Fig. 4

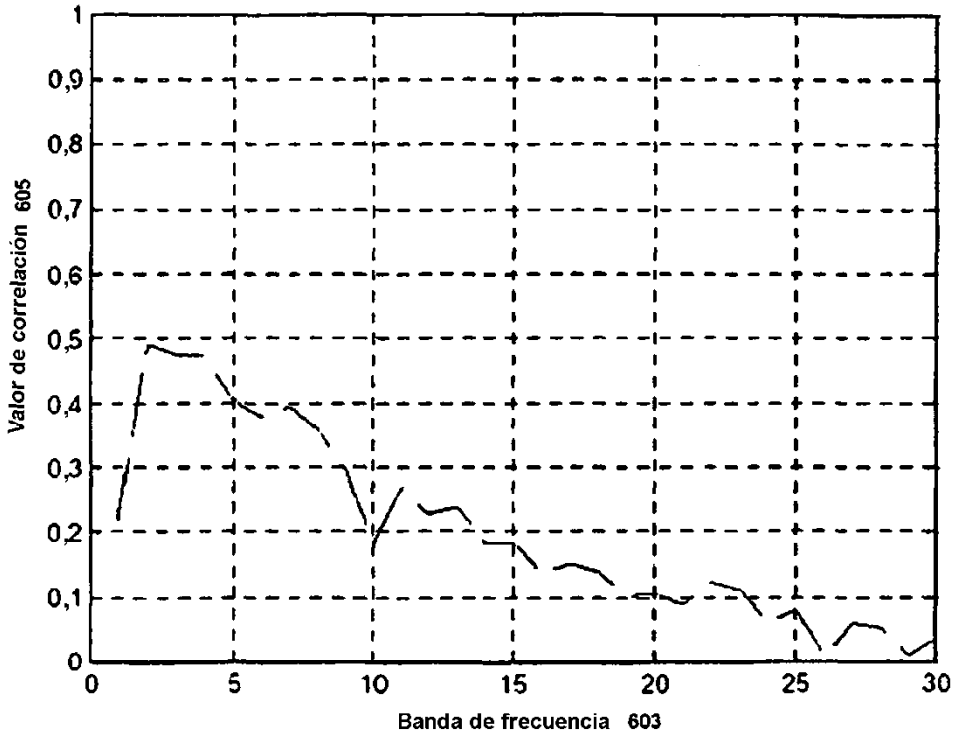
501

502



503

Fig. 5


1
0,9
0,8
0,7
0,6
0,5
0,4
0,3
0,2
0,1
0
Valor de correlación 605
0
5
10
15
20
25
30
Banda de frecuencia 603

601

Fig. 6

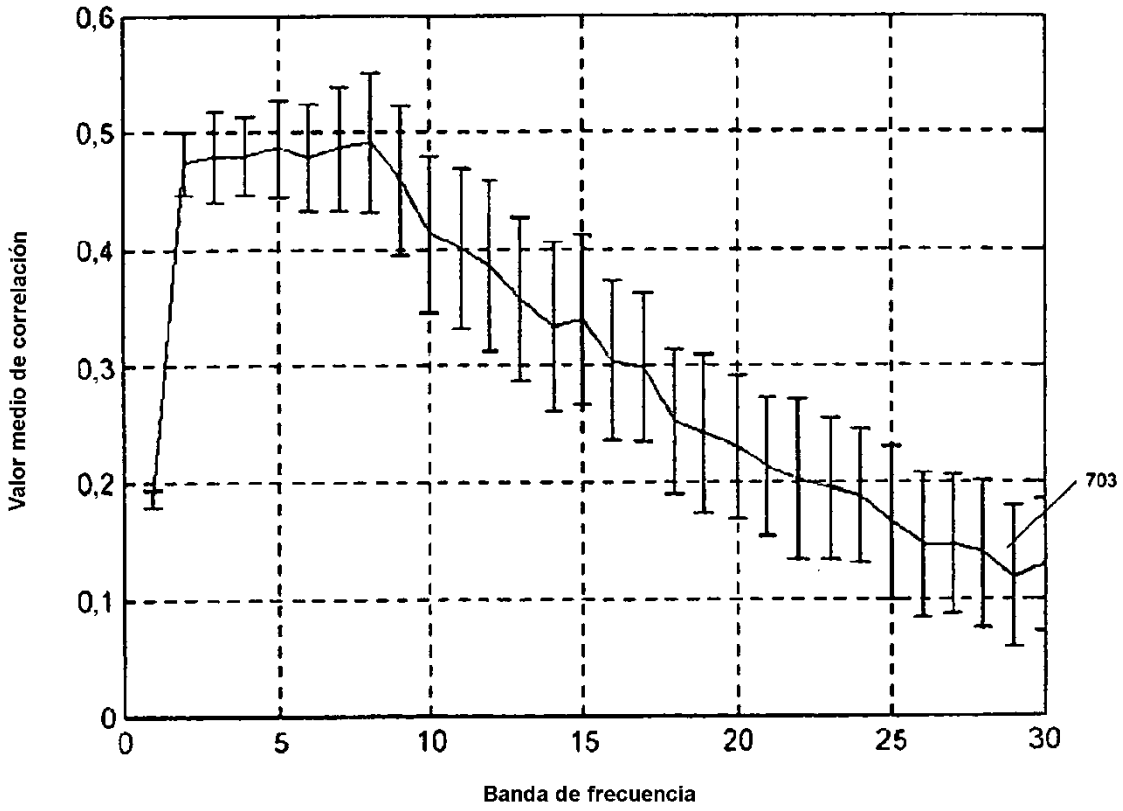

0,6
0,5
0,4
0,3
0,2
0,1
0
0
5
10
15
20
25
30
Valor medio de correlación
Banda de frecuencia
703
701

Fig. 7

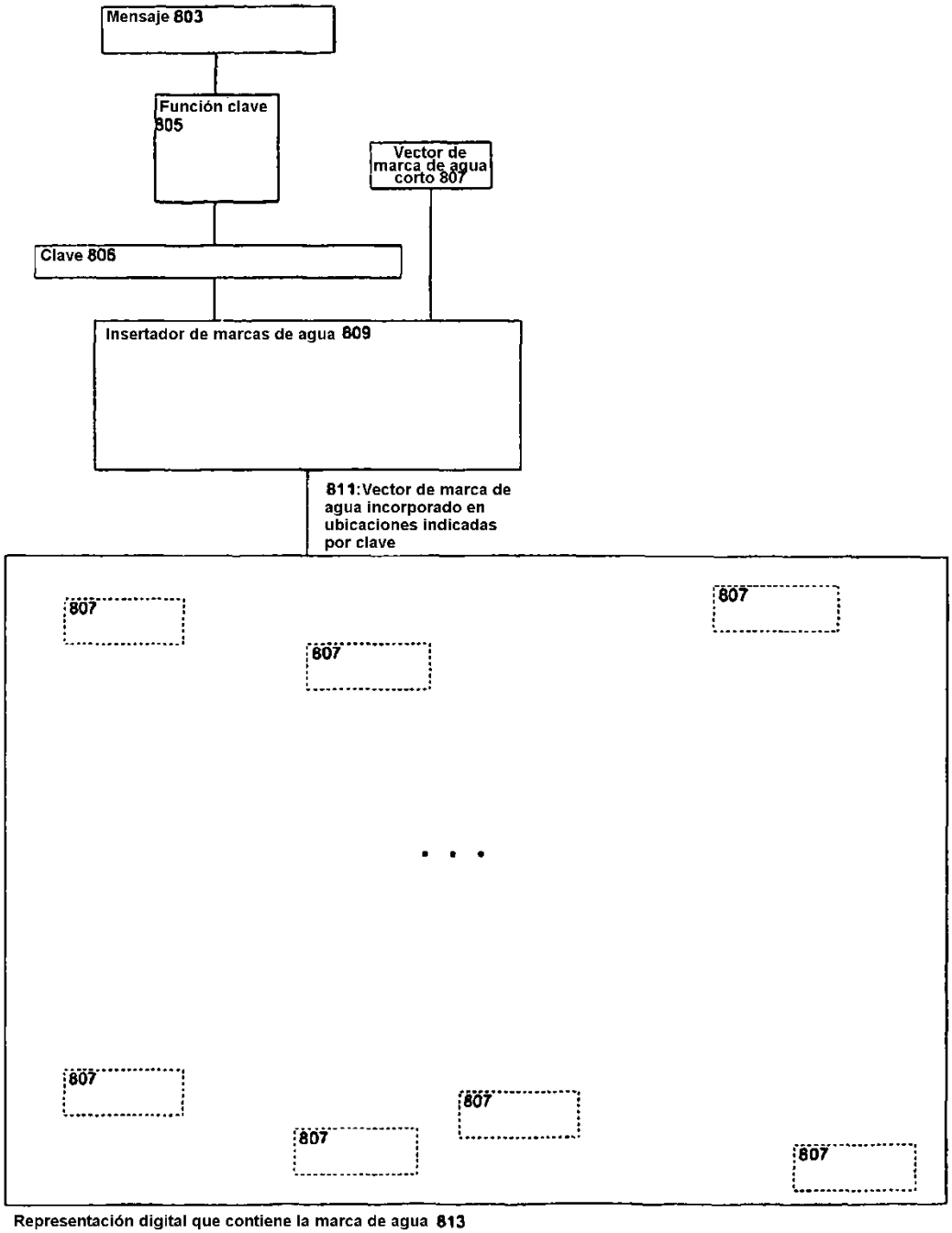

Mensaje 803
Función clave 805
Vector de marca de agua corto 807
Clave 806
Insertador de marcas de agua 809
811:Vector de marca de agua incorporado en ubicaciones indicadas por clave
807
807
807
807
807
807
807
Representación digital que contiene la marca de agua 813
801

FIG. 8

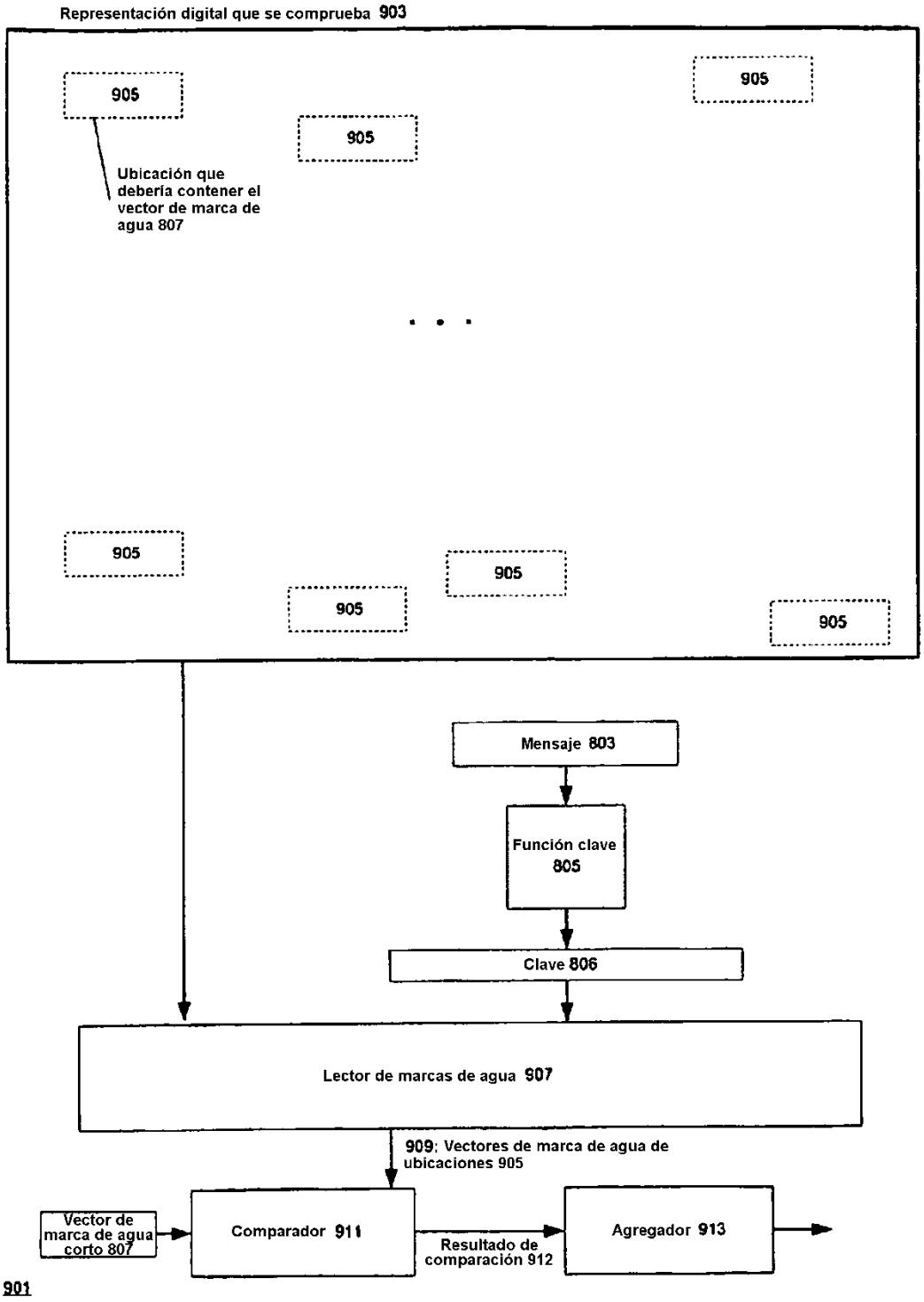

Representación digital que se comprueba 903
905
905
905
905
905
905
905
905
Ubicación que debería contener el vector de marca de agua 807
Mensaje 803
Función clave 805
Clave 806
Lector de marcas de agua 907
909: Vectores de marca de agua de ubicaciones 905
Vector de marca de agua corto 807
Comparador 911
Resultado de comparación 912
Agregador 913
901

Fig. 9

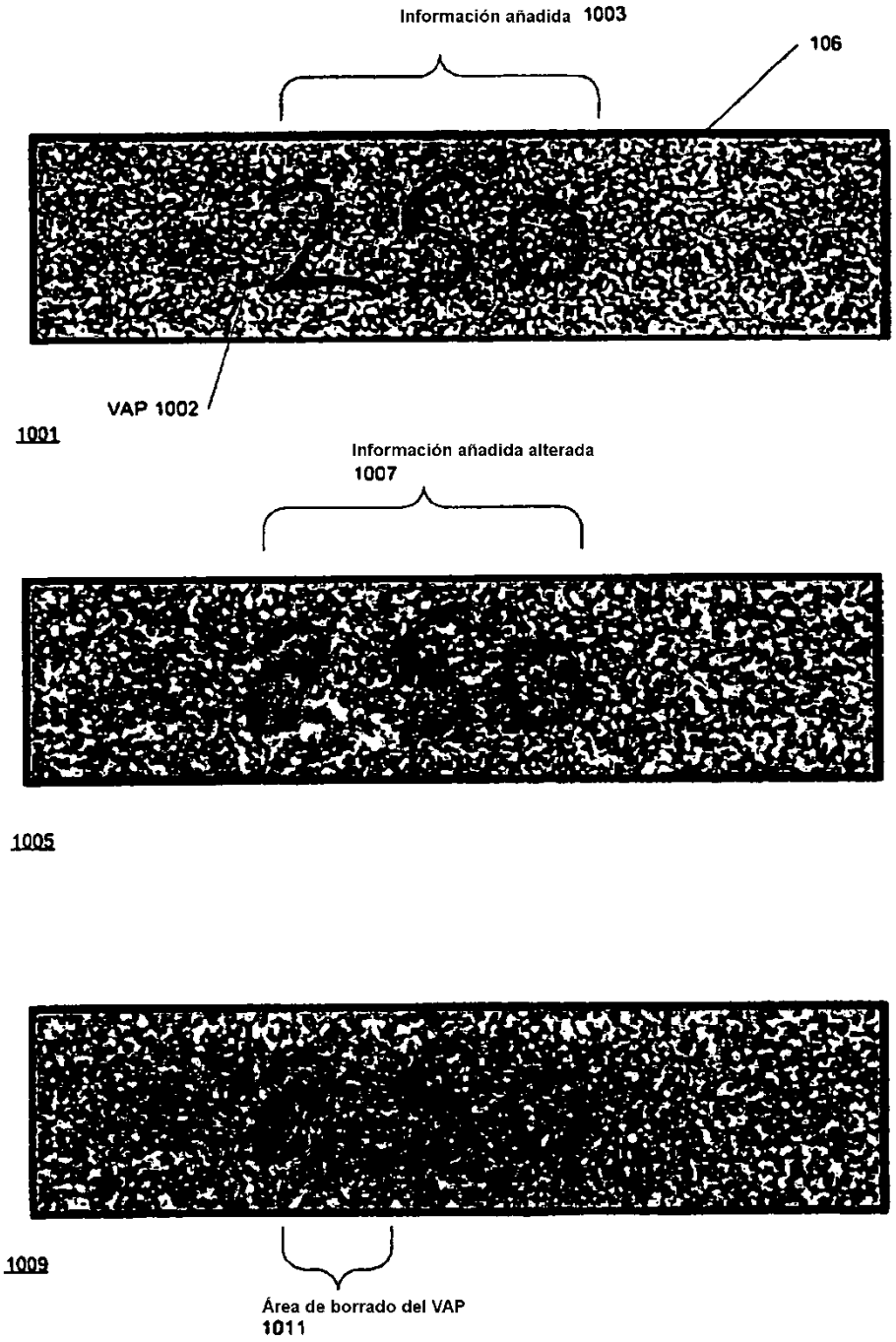

Información añadida 1003
106
VAP 1002
1001
Información añadida alterada
1007
1005
1009
Área de borrado del VAP
1011

Fig. 10

1101

1103

Fig. 11