(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 387 030**

(51) Int. CI.:
H04L 9/32 (2006.01)

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(96) Número de solicitud europea: **05808377 .5**
(96) Fecha de presentación: **11.11.2005**
(97) Número de publicación de la solicitud: **1810442**
(97) Fecha de publicación de la solicitud: **25.07.2007**

(54) Título: **Dispositivo y procedimiento para detectar una manipulación de una señal de información**

(30) Prioridad:
11.11.2004 DE 102004054549

(45) Fecha de publicación de la mención BOPI:
12.09.2012

(45) Fecha de la publicación del folleto de la patente:
12.09.2012

(73) Titular/es:
Fraunhofer-Gesellschaft zur Förderung der angewandten Forschung e.V.
Hansastrasse 27c
80686 München, DE

(72) Inventor/es:
KULESSA, Ralph;
PICKEL, Jörg;
KRÄGELOH, Stefan;
AICHROTH, Patrick;
SIEBENHAAR, Frank;
NEUBAUER, Christian y
SPINNLER, Wolfgang

(74) Agente/Representante:
Arizti Acha, Monica

DESCRIPCIÓN

Dispositivo y procedimiento para detectar una manipulación de una señal de información

La presente invención se refiere a la comprobación de la integridad de señales de información.

Con la continua expansión de los medios de comunicación modernos aumenta la importancia de conceptos que protegen las señales de información frente a una manipulación no permitida o descubren una manipulación.

Si en el caso de las señales de información se trata por ejemplo de señales de audio o de vídeo digitales, entonces a menudo se utilizan las denominadas marcas de agua, para proporcionar a los datos por ejemplo una protección frente al copiado. Las marcas de agua se "tejen" por ejemplo con la señal de información, de modo que una retirada de la marca de agua para, por ejemplo, eliminar la protección frente al copiado, puede dejar de por sí huellas digitales, que pueden detectarse. Para incluso en el caso de una retirada con éxito de la marca de agua evitar una reproducción de los datos, también es necesario comprobar la integridad de los datos, para detectar una posible manipulación.

Los enfoques conocidos para la comprobación de la integridad de las señales de información se basan en cifrar los datos completos mediante un procedimiento *hash* criptográfico. Los valores *hash* criptográficos se denominan a menudo suma de comprobación. Se calculan a partir de un valor de entrada con una longitud indeterminada y definen de manera unívoca un valor de salida determinado, el denominado *hash* (por ejemplo una cadena de 20 bytes). A este respecto la particularidad de la función *hash* consiste en determinar para cada valor de entrada aleatorio un valor de salida asociado de manera unívoca, a partir del que no puede volver a calcularse el valor de entrada.

La cantidad de datos completa se procesa en primer lugar con el algoritmo *hash*, es decir, se forma el *hash* de la cantidad de datos. Para la comprobación posterior de la integridad la cantidad de datos que va a someterse a prueba vuelve a procesarse por completo con el algoritmo *hash*. Si proporciona el mismo *hash* que en el caso de la pasada de referencia, entonces puede suponerse que no se realizaron modificaciones en el conjunto de datos.

Los requisitos con respecto a las funciones *hash* pueden determinarse esencialmente en tres puntos:

- cada valor *hash* debe aparecer con la misma frecuencia, es decir la probabilidad de valores *hash* no puede ser diferente con diferentes valores de entrada.

- Una modificación del valor de entrada debe llevar a un valor *hash* modificado.

- El esfuerzo para generar colisiones debe ser muy elevado, es decir, para un valor de entrada dado, debe ser difícil hallar un segundo con el mismo valor *hash*.

Una función *hash*, que cumple con los tres requisitos, también se denomina función *hash* criptográfica. Entre las funciones *hash* más importantes se encuentran SHA-1, MD4, MD5 así como RIPE-MD160.

La función *hash* criptográfica SHA-1 procesa bloques con una longitud de 512 bits y en este caso genera valores *hash* de 160 bits. Un papel importante lo desempeñan las variables de 532 bits (variables de cadena) así como la denominada función de compresión.

En primer lugar se divide el valor de entrada en bloques con una longitud de 512 bits. A continuación la función de compresión toma las cinco variables de cadena así como un bloque de 512 bits y lo reproduce sobre los siguientes valores de 532 bits. La función se desarrolla en cuatro pasadas con 20 operaciones idénticas en cada caso, en las que los bits individuales se desplazan según operaciones de cálculo predefinidas. Finalmente se emite el contenido de las cinco variables de cadena como valor *hash*. El uso del procedimiento *hash* para la comprobación de la integridad se describe por ejemplo en Open Mobil Alliance, OMA DRM especificación V2.0, borrador 2.0-10 de abril de 2004.

En los enfoques conocidos es desventajoso que por norma se someta a prueba un conjunto de datos completo, es decir, toda la señal de información, lo que va unido a una complejidad elevada. Además, de este modo, no puede realizarse ningún tipo de modificación posterior del conjunto de datos, por ejemplo la adición de una o varias marcas de agua, sin afectar a la integridad del conjunto de datos, incluso cuando sólo se modifican determinadas componentes del conjunto de datos.

La publicación especializada de Schneider *et al.* "A Robust Content Based Digital Signature for Image Authentication", 16 de septiembre de 1996, Proceedings of the International Conference on Image Processing (ICIT), Lausanne, 16 a 19 de septiembre de 1996 da a conocer para la generación de una firma basada en contenido una extracción de contenido y una siguiente formación de *hash* del resultado de la extracción con un cifrado siguiente, para obtener una firma digital basada en contenido. Para la verificación se lleva a cabo la misma extracción de contenido de una imagen de prueba, de nuevo se realiza un *hash* y a continuación este *hash* se compara con una

firma descifrada, que se proporciona junto con la imagen, para una verificación. Para la extracción de contenido se utiliza un histograma de intensidad para cada bloque de una pluralidad de bloques, en los que se divide una imagen.

La publicación de patente estadounidense 2002/0178368 A1 da a conocer un sistema de marca de agua semifrágil para una autentificación de vídeo MPEG. Una marca de agua semifrágil comprende una componente de marca de agua semifrágil y una componente de marca de agua robusta. Para generar la marca de agua frágil se extraen características a partir del flujo de vídeo y a continuación se someten a un procesamiento *hash*. La marca de agua frágil es el resultado cifrado de un procesamiento *hash* de coeficientes DCT cuantificados.

La publicación de patente estadounidense US 2004/- 0128511 A1 da a conocer procedimientos y sistemas para generar una firma multimedia. Para ello se extraen características invariables a partir del contenido multimedia y se calculan determinados atributos. Para ello se cuantifica el contenido multimedia y se extraen las características invariables a partir del contenido multimedia cuantificado. Las características invariables extraídas así como los datos multimedia cuantificados se cifran, para generar una firma digital. Las características extraídas son vértices, valores medios de bloques e histogramas, que deben extraerse a partir de imágenes, para generar firmas robustas.

El objetivo de la presente invención es crear un concepto para la comprobación de la integridad de datos, que presente una complejidad reducida y que permita una comprobación de la integridad de los datos también después del procesamiento de las componentes de datos.

Este objetivo se soluciona mediante un dispositivo según la reivindicación 1 o mediante un dispositivo según la reivindicación 13 o mediante un dispositivo según la reivindicación 15 o mediante un procedimiento según la reivindicación 18 o mediante un procedimiento según la reivindicación 19 o mediante un procedimiento según la reivindicación 20 o mediante un programa informático según la reivindicación 21.

La invención se basa en el conocimiento de que una pluralidad de señales de información, que están relacionadas con diferentes aplicaciones, por ejemplo señales de vídeo o audio, presentan una información característica de la señal de información, a la que puede recurrirse para proteger un conjunto de datos frente a la manipulación permitiendo simultáneamente modificaciones no características del conjunto de datos.

Si en el caso de la señal de información se trata por ejemplo de un archivo codificado en MP3, así durante la comprobación del archivo de audio codificado en MP3 de la integridad, para por ejemplo poder descubrir manipulaciones, el archivo aún debe considerarse como sin modificar, cuando por ejemplo por medio de la formación de marcas de agua en el flujo de bits se ha añadido una marca de agua. Las manipulaciones en un archivo, que modifican la característica de la pieza o incluso dan como resultado un cambio de la pieza (o de partes de la pieza) deben reconocerse sin embargo de manera unívoca. Según la presente invención, para por ejemplo permitir una adición posterior de marcas de agua, se utiliza como sensor una información característica e inherente a la señal de información, en este ejemplo el archivo de audio codificado en MP3.

Sin embargo, en primer lugar, debe determinarse la información característica de un conjunto de datos, es decir de una señal de información. Esta etapa puede definirse en función de un tipo y una aplicación del conjunto de datos y en el caso más sencillo requiere un enmascaramiento de partes no características, eventualmente también un filtrado o transformación del conjunto de datos, para obtener la información característica. En el caso de una pieza de música codificada en MP3, por ejemplo, es suficiente extraer la información secundaria o sólo parte de la información secundaria, sin considerar los datos espectrales, que forman la información principal, estando relacionada la información secundaria con la información principal y comprendiendo por ejemplo factores de escala para los datos espectrales. Si por ejemplo se añade a los datos espectrales una marca de agua, entonces esto no cambia nada de la información característica. La integridad de la señal de información se no ve afectada, en el sentido según la invención.

Entonces, en una segunda etapa se asegura o somete a prueba la integridad de exclusivamente la información característica con un procedimiento criptográfico, pudiendo recurrir para el procedimiento criptográfico por ejemplo al procedimiento *hash* ya mencionado.

En el ejemplo del flujo de datos de MP3, por ejemplo, los factores de escala, que están relacionados con los datos espectrales, pueden aprovecharse como información característica, de modo que por ejemplo, el procedimiento *hash* sólo se aplique a los factores de escala, es decir que el valor *hash* sólo se calcule mediante los factores de escala. Si ahora se aplica la formación de marcas de agua en el flujo de bits, entonces se modifican los valores espectrales, aunque no los factores de escala (parámetros de escala). Una comprobación posterior del *hash* proporciona por tanto una coincidencia, en caso de que no exista una manipulación del conjunto de datos (de la señal de información). Esto es suficiente, por ejemplo, para evitar que pueda meterse otra pieza.

A diferencia del estado de la técnica, en el que una comprobación de la integridad del archivo completo se realiza mediante un procedimiento *hash* criptográfico sin tener en cuenta información característica, la presente invención se basa en proteger un conjunto de datos frente a la manipulación de su información característica permitiendo simultáneamente modificaciones no características del conjunto de datos.

Para la comprobación de la integridad de un conjunto de datos puede utilizarse, por ejemplo un procedimiento *hash* criptográfico, por ejemplo SHA-1. Sirve para comprobar una coincidencia de uno a uno entre una referencia (original) y un conjunto de datos que va a compararse (copia). El resultado de la comprobación es o bien “idéntico” o bien “difiere de algún modo”.

Como ya se ha mencionado, a veces es deseable permitir modificaciones específicas en un conjunto de datos, por ejemplo mediante la adición de una marca de agua, y aún así poder comprobar, que la información característica está presente sin modificar, es decir, que esencialmente sigue tratándose del conjunto de datos original, es decir del conjunto de datos original, no manipulado. Según la invención se comprueba la integridad de la información característica de un conjunto de datos. Lo que es “información característica” puede definirse según el caso de aplicación. Un ejemplo de esto es una pieza de música codificada en MP3, a la que, como se ha descrito anteriormente, tras una determinación de la información de integridad, por medio de la formación de marcas de agua en el flujo de bits se añadirá una marca de agua. Los valores espectrales de la pieza se modifican (ligeramente), los factores de escala y otra información secundaria permanecen sin embargo iguales y diferencian la pieza de otras piezas de música. Así se conserva la información característica.

Según la invención, por tanto, una pieza de música codificada en MP3 todavía puede considerarse como sin modificar cuando se ha tratado con formación de marcas de agua en el flujo de bits. Se comprueba la integridad de la información característica de un conjunto de datos, sin embargo se permiten las modificaciones del conjunto de datos, que no modifican la información característica.

En piezas de música codificadas en MP3 mediante la utilización de la formación de marcas de agua en el flujo de bits no se ve afectada la integridad de las partes de señal de información características, que comprenden la información característica. De este modo se consigue que el original no pueda sustituirse por otra pieza o partes de otra pieza, lo que por ejemplo es importante para aplicaciones DRM, pudiendo modificarse aún así la información no característica.

Mediante la posibilidad de poder comprobar de manera dirigida la integridad de la información característica de un conjunto de datos, puede modificarse así una información no característica, sin modificar la integridad. Así, por ejemplo, en el caso de un archivo codificado en MP3 puede añadirse una marca de agua por medio de la formación de marcas de agua en el flujo de bits, sin que se modifique la integridad del archivo en el sentido según la invención, es decir por ejemplo sin que el procedimiento *hash* según la invención indique una diferencia con respecto al original.

Ejemplos de realización adicionales de la presente invención se describen mediante la figura 1, que muestra un diagrama de bloques de un dispositivo para detectar una manipulación de una señal de información según un ejemplo de realización de la presente invención.

El dispositivo representado en la figura 1 comprende un equipo 101 para la extracción, cuya salida está acoplada con una entrada de un equipo 103 para el cifrado. El equipo 103 para el cifrado comprende una salida, que está acoplada con una entrada de un equipo 105 para la comparación.

Tal como se representa en la figura 1, la señal de información comprende una componente de señal de información, que es característica de la señal de información. El equipo 101 para la extracción está configurado para extraer la componente de señal de información, y para poner la componente de señal de información a disposición del equipo 103 para el cifrado. El equipo 103 para el cifrado está configurado para cifrar la componente de información por ejemplo utilizando un procedimiento criptográfico, para obtener una señal cifrada.

El equipo 105 para la comparación está configurado para recibir la señal cifrada desde el equipo 103 para el cifrado, y para comparar la señal cifrada con una señal de referencia, siendo la señal de referencia una representación cifrada de una componente de señal de referencia no manipulada de una señal de información de referencia, para detectar la manipulación de la señal de información, en caso de que la señal de información se haya manipulado.

En caso de una manipulación detectada, el equipo 105 para la comparación a través de una salida puede proporcionar una señal de control, que indica una manipulación de la señal de información existente en una entrada del equipo 101 para la extracción.

Según la invención el equipo 101 para la extracción puede estar configurado para no filtrar una componente de señal de información adicional o componentes de señal de información adicionales de la señal de información, de modo que no pueda detectarse una modificación de las componentes de información adicionales. Si, por ejemplo, se añade una marca de agua a los otros componentes de la señal de información, entonces esta modificación de la señal de información según la invención no debe conducir a que se detecte una manipulación, porque las modificaciones permitidas según la invención del conjunto de datos no deberían poder detectarse para no afectar a la comprobación de la integridad.

Para que la señal de información tras una comprobación de la integridad pueda tratarse sin modificaciones, cuando no existe ninguna manipulación, en el caso de la señal de información, que procesa el equipo 101 para la extracción,

se trata por ejemplo de una copia de la señal de información, que en primer lugar se genera por el equipo 101 para la extracción. Así las componentes de señal de información adicionales pueden enmascararse o suprimirse por el equipo 101 para la extracción, de modo que sólo se dejen pasar las componentes de señal de información con la información característica, sin afectar a la propia señal de información.

Según un aspecto adicional de la presente invención, el equipo 101 para la extracción está configurado para detectar la componente de señal de información en la señal de información, y para extraer una copia de la componente de señal de información, para obtener la componente de señal de información.

Como ya se ha mencionado, la señal de información puede comprender una componente de señal de información adicional. Por ejemplo la componente de señal de información adicional comprende una información principal, por ejemplo datos útiles. Como información característica puede tratarse por ejemplo de una información secundaria, que está relacionada con la información principal, estando contenida la información secundaria en la componente de señal de información, que debe extraerse por el equipo 101.

Según un aspecto de la presente invención, la componente de señal de información y la componente de señal de información adicional pueden estar dispuestas en diferentes segmentos de la señal de información. En caso de que la señal de información esté presente por ejemplo en forma de una trama de datos, entonces la componente de señal de información puede estar dispuesta por ejemplo en otro lugar de la trama de datos que la componente de señal de información adicional. Dicho de otro modo, las dos componentes están separadas entre sí dentro de la señal de información. En este caso el equipo 101 para la extracción está configurado para extraer el segmento de la señal de información, en el que está dispuesta la componente de señal de información.

Sin embargo, si un espectro de la componente de señal de información presenta valores espectrales diferentes que un espectro de la componente de señal de información adicional, entonces el equipo 101 para la extracción puede estar configurado para filtrar los valores espectrales de la componente de señal de información, para obtener la componente de señal de información. Los valores espectrales de la componente de señal de información adicional pueden suprimirse, por ejemplo. Para ello, el equipo 101 para la extracción puede comprender un filtro estar configurado en sí mismo como un filtro para extraer los valores espectrales, que están relacionados con la componente de señal de información. Además, el equipo 101 para la extracción puede estar configurado para realizar un análisis espectral, para filtrar los valores espectrales del espectro de la componente de señal de información. Por ejemplo el equipo 101 para la extracción comprende para ello un transformador de Fourier, que está configurado para formar una transformada de Fourier de la señal de información, para poner los valores espectrales de la componente de señal de información adicional en la transformación de Fourier a cero y para volver a transformar el resultado en el dominio de tiempo, para obtener la componente de señal de información.

En este momento ha de indicarse que un filtrado tanto puede realizarse cuando la componente de señal de información y la componente de señal de información adicional están solapadas, como cuando la componente de señal de información y la componente de señal de información adicional están separadas entre sí y ocupan diferentes intervalos espectrales.

Si en el caso de la señal de información se trata, por ejemplo, de una señal de audio, por ejemplo una señal MPEG, entonces la componente de señal de información adicional como información principal puede comprender valores espectrales de audio, que por ejemplo estén codificados, estando comprendidos los parámetros de escala asociados a los valores espectrales de audio como información secundaria (información característica) en la componente de señal de información.

Sin embargo, en el caso de la información secundaria puede tratarse de una información sobre un número de los valores espectrales de audio, es decir de una información con respecto a la distribución de la longitud de bloque (información de conmutación de bloques), que proporciona una distribución entre bloques cortos y bloques largos (*Short-Blocks, Long-Blocks*).

Si en el caso de la señal de información se trata de una señal de vídeo, entonces la componente de señal de información adicional puede comprender como información principal información de vídeo, comprendiendo la componente de señal de información como información adicional por ejemplo valores de luminancia para la información de vídeo.

La componente de señal de información se pone a disposición del equipo 103 para el cifrado, para mediante el cifrado de la componente de señal de información utilizando procedimientos criptográficos obtener una señal cifrada. El equipo 103 para el cifrado puede estar configurado por ejemplo para formar un valor *hash* relativo a la componente de señal de información, para obtener la señal cifrada. El equipo 103 para el cifrado puede estar configurado además para formar una suma de comprobación relativa a la componente de señal de información.

Según un aspecto adicional, el equipo 103 para el cifrado puede estar configurado para cifrar la componente de señal de información utilizando, por ejemplo, el algoritmo RSA recurriendo a una clave privada o pública. El equipo 103 para el cifrado puede estar configurado, sin embargo, para utilizar cualquier otro procedimiento de cifrado simétrico o no simétrico conocido, para obtener la señal cifrada.

Según la invención la señal cifrada se compara con una señal de referencia. La señal de referencia puede estar comprendida, por ejemplo, en la señal de información. En este caso el equipo 101 para la extracción está configurado además para extraer la señal de referencia a partir de la señal de información. Si la señal de referencia está dispuesta en un lugar determinado de la señal de información, entonces se extrae el segmento correspondiente de la señal de información, que comprende la señal de referencia. Sin embargo, la señal de referencia puede comprender un espectro con valores espectrales de referencia específicos, de modo que el equipo 101 para la extracción, de manera análoga a las realizaciones anteriores, pueda filtrar los valores espectrales de referencia, para extraer la señal de referencia.

Si la señal de referencia no está contenida en la señal de información, entonces el equipo para la extracción puede estar configurado para seleccionar una señal de referencia, que está asociada a la componente de señal de información, a partir de una pluralidad de señales de referencia. Las señales de referencia puede estar depositadas por ejemplo para cualquier componente de señal de información concebible en una memoria, de modo que mediante la componente de señal de información extraída, que comprende la información característica, se selecciona una señal de referencia, que por ejemplo está unida con la información característica y por tanto relacionada con la misma.

En el caso de la señal de referencia puede tratarse de un valor *hash* o de una suma de comprobación relativa a una componente de señal de información no manipulada. En general, en el caso de la señal de información, puede tratarse de un resultado de un cifrado criptográfico de una componente de señal de referencia no manipulada, recurriéndose por ejemplo al procedimiento criptográfico mencionado anteriormente.

La componente de señal de referencia no manipulada es por ejemplo idéntica a la componente de señal de información original. De manera análoga la señal de referencia puede ser idéntica a la señal de información original, es decir, no manipulada.

Los ejemplos de realización anteriores se refieren al caso en que la componente de señal de información se cifre para comprobar la integridad de los datos. Sin embargo, según la invención es concebible que la componente de señal de información, que es característica de la señal de información, se compare con una señal descifrada, para comprobar la integridad de la señal de información, desprendiéndose la señal descifrada de un descifrado criptográfico de una señal de referencia.

Según un aspecto adicional la invención proporciona un dispositivo para detectar una manipulación de una señal de información con un equipo para extraer una componente de señal de información, que es característica de la señal de información a partir de la señal de información, pudiendo el equipo para la extracción ser idéntico al equipo 101 para la extracción ya descrito.

El dispositivo comprende además un equipo para descifrar una señal de referencia, siendo la señal de referencia una representación cifrada de una componente de señal de referencia no manipulada de una señal de información de referencia, para obtener una señal descifrada.

El dispositivo comprende además un equipo para comparar la señal descifrada con la componente de señal de información.

En el caso de la señal de referencia, que por ejemplo está comprendida en la señal de información y que también se extrae por el equipo para la extracción, se trata por ejemplo de una representación cifrada de la componente de señal de información original de una señal de información original.

Si en el caso de la señal de información se trata por ejemplo de una firma digital generada utilizando una clave privada relativa a la componente de señal de información, entonces el equipo para el descifrado puede estar configurado para descifrar la firma con una clave pública, que está relacionada con la clave privada, para obtener la señal descifrada.

Según un aspecto adicional, en el caso de la señal de referencia puede tratarse de una señal, que se ha cifrado utilizando un procedimiento de cifrado simétrico o no simétrico cualquiera, habiendo utilizado en el caso de un procedimiento no simétrico una clave privada. La señal de referencia puede descifrarse ahora en el lado de recepción con una clave pública, para obtener una versión descifrada de la componente de señal de información. Tras una comparación de la componente de señal de información recibida con la versión descifrada, ahora puede determinarse si existe una manipulación de la señal de información.

Según un aspecto adicional, la presente invención proporciona un dispositivo para generar una señal de información a partir de una señal de entrada, comprendiendo la señal de entrada una componente de señal de entrada y una componente de señal de entrada adicional, comprendiendo la componente de señal de entrada adicional una información principal y comprendiendo la componente de señal de entrada una información secundaria, que está relacionada con la información principal. La componente de señal de entrada corresponde por ejemplo a la componente de señal de información ya mencionada y la componente de señal de entrada adicional corresponde por ejemplo a la componente de señal de información adicional.

El dispositivo para generar la señal de información comprende un equipo para cifrar la componente de señal de entrada, para obtener una señal de referencia. Además el dispositivo para la generación comprende un equipo para componer la componente de señal de recepción, la componente de señal de recepción adicional y la señal de referencia, para generar la señal de información.

Según un aspecto de la presente invención el equipo para el cifrado está configurado para cifrar la componente de señal de entrada, que por ejemplo comprende la información característica de la señal de información o del tipo de señal de información, utilizando un procedimiento criptográfico, tal como por ejemplo se han mencionado anteriormente. Por ejemplo, el equipo para el cifrado puede estar configurado para cifrar la componente de señal de entrada con ayuda de un procedimiento de cifrado no simétrico utilizando una clave privada, pudiendo descifrarse la señal de referencia, tal como se ha descrito anteriormente, por ejemplo utilizando la clave pública.

El equipo para el cifrado puede estar configurado sin embargo para formar un valor *hash* o una suma de comprobación relativa a la componente de señal de entrada, para obtener la señal de referencia.

El equipo para la composición puede estar configurado por ejemplo para adjuntar la señal de referencia a la señal de entrada, para generar la señal de información. El equipo para la composición puede estar configurado sin embargo para solapar la señal de referencia a la señal de entrada, por ejemplo, presentando la señal de referencia y la señal de entrada preferiblemente diferentes intervalos espectrales. El equipo para la composición puede estar configurado sin embargo para disponer la señal de referencia en un lugar aleatorio de la señal de entrada.

Según la invención ahora es posible someter a prueba la integridad de la información característica de un conjunto de datos. Si ahora se realizan modificaciones en la información no característica de un conjunto de datos, entonces la prueba de integridad sigue proporcionando el mensaje de idéntico. Así, por ejemplo, la información principal mencionada anteriormente puede haberse tratado adicionalmente, sin que se modifique la componente de señal de información o componente de señal de entrada. Por ejemplo a la componente de señal de información adicional o la componente de señal de entrada adicional se le pueden añadir marcas de agua, sin que esto influya en la integridad de los datos.

Tal como se ha descrito anteriormente, en una primera etapa se extrae la información característica del caso de aplicación deseado, por ejemplo, con ayuda de un filtro. En el caso de señales codificas en MP3, este filtro puede enmascarar por ejemplo todos los valores de código de Hoffmann (líneas espectrales, valores espectrales), es decir, dejar pasar otros bits. Son concebibles filtros de diferentes tipos, tanto los que enmascaran las partes sencillas como los que realizan operaciones de filtro complicadas. Así por ejemplo, en el caso de un documento de texto puede filtrarse sólo texto sin edición. Si se trata de una imagen, entonces por ejemplo sólo se extrae la luminancia y nada de color, etc.

En una etapa adicional la información característica obtenida (el resultado del filtro) se procesa/somete a prueba con un procedimiento criptográfico habitual, por ejemplo con un procedimiento *hash* criptográfico.

Si en el caso de la señal de información o señal de entrada se trata de una señal codificada en MP3, entonces ésta se descodifica hasta que puede determinarse la zona en la que están almacenados factores de escala como información secundaria. El algoritmo *hash* se aplica ahora a los factores de escala del conjunto de datos y se almacena el valor *hash* producido como referencia, no teniendo en cuenta los valores espectrales.

Ahora a la señal se le puede añadir con cualquier frecuencia una marca de agua por medio de un procedimiento de formación de marcas de agua en el flujo de bits adecuado. Para ver si la información característica se ha modificado, vuelve a determinarse la zona de los factores de escala (parámetros de escala) (componente de señal de información), se calcula el *hash* relativo a los factores de escala y se compara con la referencia, tal como se describió anteriormente. Si la información característica no tiene modificaciones, el *hash* es igual.

Otras posibilidades de definir información característica de señales codificadas en MP3 son, por ejemplo, la información secundaria completa, una parte determinada de los valores espectrales, en caso de que se utilice la formación de marcas de agua sólo para la parte complementaria, o la información de conmutación de bloques (distribución bloques cortos, bloques largos)ya mencionada.

Los valores espectrales pueden estar ajustados a escala por ejemplo con factores de escala. Además los valores espectrales pueden estar codificados, por ejemplo estar cifrados mediante Huffman.

Así, la presente invención proporciona entre otros también la posibilidad de proporcionar un *hash* compatible con marcas de agua.

La presente invención proporciona además de los dispositivos descritos también procedimientos con la funcionalidad correspondiente. Además todas las funcionalidades de los diferentes ejemplos de realización pueden combinarse entre sí, para obtener efectos ventajosos adicionales de la presente invención.

En función de las circunstancias los procedimientos según la invención pueden implementarse en hardware o en software. La implementación puede realizarse en un medio de almacenamiento digital, en particular un disquete o

CD con señales de control legibles de manera electrónica, que pueden actuar conjuntamente con un sistema informático programable, de modo que se realiza el procedimiento correspondiente. En general la invención también consiste por tanto en un producto de programa informático con un código de programa almacenado en un soporte legible a máquina para la realización de al menos uno de los procedimientos según la invención, cuando el producto de programa informático se ejecuta en un ordenador. Dicho de otro modo, la invención puede realizarse por tanto como un programa informático con un código de programa para la realización de los procedimientos, cuando el programa informático se ejecuta en un ordenador.

REIVINDICACIONES

1. Dispositivo para detectar una manipulación de una señal de información, caracterizado porque la señal de información presenta una componente de señal de información con información secundaria y una componente de señal de información adicional con información principal, estando relacionada la información secundaria con la información principal, y porque el dispositivo presenta las características siguientes:

un equipo (101) para extraer la componente de señal de información con información secundaria, que es característica de la señal de información, a partir de la señal de información;

un equipo (103) para cifrar la componente de señal de información extraída con información secundaria, para obtener una señal cifrada; y

un equipo (105) para comparar la señal cifrada con una señal de referencia, siendo la señal de referencia una representación cifrada de una componente de señal de referencia no manipulada con información secundaria de una señal de información de referencia, para detectar la manipulación.

2. Dispositivo según la reivindicación 1, estando configurado el equipo (101) para la extracción para no filtrar la componente de señal de información con información principal, de modo que no puede detectarse una modificación de la componente de señal de información con información principal.

3. Dispositivo según la reivindicación 1, estando dispuestas la componente de señal de información con información secundaria y la componente de señal de información con información principal en diferentes segmentos de la señal de información, y estando configurado el equipo (101) para la extracción para extraer el segmento de la señal de información, en el que está dispuesta la componente de señal de información con información secundaria, para obtener la componente de señal de información extraída.

4. Dispositivo según la reivindicación 1, presentando un espectro de la componente de señal de información y un espectro de la componente de señal de información adicional diferentes valores espectrales, y estando configurado el equipo (101) para la extracción para filtrar los valores espectrales de la componente de señal de información, para obtener la componente de señal de información.

5. Dispositivo según una de las reivindicaciones 1 a 4, siendo la señal de información una señal de audio, comprendiendo la componente de señal de información adicional como información principal valores espectrales de audio, y comprendiendo la componente de señal de información como información secundaria parámetros de escala para los valores espectrales de audio.

6. Dispositivo según una de las reivindicaciones 1 a 4, siendo la señal de información una señal de audio, y comprendiendo la componente de señal de información adicional valores espectrales de audio, y comprendiendo la componente de señal de información, información sobre un número de valores espectrales de audio.

7. Dispositivo según una de las reivindicaciones 1 a 4, siendo la señal de información una señal de vídeo, comprendiendo la componente de señal de información adicional como información principal información de vídeo, y comprendiendo la componente de señal de información como información secundaria valores de luminancia para la información de vídeo.

8. Dispositivo según una de las reivindicaciones 1 a 7, estando configurado el equipo (103) para el cifrado para formar un valor *hash* o para formar una suma de comprobación relativa a la componente de señal de información, para obtener la señal cifrada.

9. Dispositivo según una de las reivindicaciones 1 a 8, comprendiendo la señal de información además la señal de referencia, estando configurado el equipo (101) para la extracción para extraer la señal de referencia a partir de la señal de información.

10. Dispositivo según la reivindicación 9, estando configurado el equipo (101) para la extracción para seleccionar una señal de referencia, que está asociada a la componente de señal de información, a partir de una pluralidad de señales de referencia.

11. Dispositivo según la reivindicación 9 u 10, siendo la señal de referencia un valor *hash* o una suma de comprobación relativa a la componente de señal de referencia no manipulada.

12. Dispositivo según una de las reivindicaciones 1 a 11, siendo la componente de señal de referencia no manipulada idéntica a la componente de señal de información original, y siendo la señal de referencia idéntica a la señal de información original.

13. Dispositivo para detectar una manipulación de una señal de información, caracterizado porque la señal de información presenta una componente de señal de información con información secundaria y una componente de

señal de información adicional con información principal, estando relacionada la información secundaria con la información principal, y porque el dispositivo presenta las características siguientes:

un equipo para extraer la componente de señal de información con información secundaria, que es característica de la señal de información, a partir de la señal de información;

un equipo para descifrar una señal de referencia, siendo la señal de referencia una representación cifrada de una componente de señal de referencia no manipulada con información secundaria de una señal de información de referencia, para obtener una señal descifrada, presentando la señal de referencia una componente de señal de información adicional con información principal, estando relacionada la información secundaria con la información principal; y

un equipo para comparar la señal descifrada, que representa información secundaria descifrada de la señal de referencia, con la componente de señal de información con información secundaria, para detectar la manipulación de la señal de información.

14. Dispositivo según la reivindicación 13, siendo la señal de referencia una firma digital generada utilizando una clave privada relativa a la componente de señal de información, y estando configurado el equipo para el descifrado para descifrar la firma con una clave pública, que está relacionada con la clave privada, para obtener la señal descifrada.

15. Dispositivo para generar una señal de información a partir de una señal de entrada, caracterizado porque la señal de entrada comprende una componente de señal de entrada, que es característica de la señal de información, y una componente de señal de entrada adicional, comprendiendo la componente de señal de entrada adicional información principal, y comprendiendo la componente de señal de entrada información secundaria, que está relacionada con la información principal, y porque el dispositivo presenta las características siguientes:

un equipo para cifrar la componente de señal de entrada, que comprende la información secundaria, para obtener una señal de referencia; y

un equipo para componer la componente de señal de entrada, que comprende la información secundaria, de la componente de señal de entrada adicional, que comprende la información principal, y de la señal de referencia, que comprende la información secundaria en forma cifrada, para generar la señal de información.

16. Dispositivo según la reivindicación 15, estando configurado el equipo para el cifrado para formar un valor *hash* o para formar una suma de comprobación relativa a la componente de señal de entrada, para obtener la señal de referencia.

17. Dispositivo según la reivindicación 15 o 16, estando configurado el equipo para la composición para adjuntar la señal de referencia a la señal de entrada, para generar la señal de información.

18. Procedimiento para detectar una manipulación de una señal de información, caracterizado porque la señal de información presenta una componente de señal de información con información secundaria y una componente de señal de información adicional con información principal, estando relacionada la información secundaria con la información principal, y porque el procedimiento presenta las etapas siguientes:

extraer la componente de señal de información con información secundaria, que es característica de la señal de información, a partir de la señal de información;

cifrar la componente de señal de información extraída con información secundaria, para obtener una señal cifrada; y

comparar la señal cifrada con una señal de referencia, siendo la señal de referencia una representación cifrada de una componente de señal de referencia no manipulada con información secundaria de una señal de información de referencia, para detectar la manipulación.

19. Procedimiento para detectar una manipulación de una señal de información, caracterizado porque la señal de información presenta una componente de señal de información con información secundaria y una componente de señal de información adicional con información principal, estando relacionada la información secundaria con la información principal, y porque el procedimiento presenta las etapas siguientes:

extraer la componente de señal de información con información secundaria, que es característica de la señal de información, a partir de la señal de información;

descifrar una señal de referencia, siendo la señal de referencia una representación cifrada de una componente de señal de referencia no manipulada con información secundaria de una señal de información de referencia, para obtener una señal descifrada, presentando la señal de referencia una componente de señal de información adicional con información principal, estando relacionada la información secundaria con la información principal; y

comparar la señal descifrada, que representa información secundaria descifrada de la señal de referencia, con la componente de señal de información con información secundaria, para detectar la manipulación.

20. Procedimiento para generar una señal de información a partir de una señal de entrada, caracterizado porque la señal de entrada comprende una componente de señal de entrada, que es característica de la señal de información, y una componente de señal de entrada adicional, comprendiendo la componente de señal de entrada adicional información principal, y comprendiendo la componente de señal de entrada información secundaria, que está relacionada con la información principal, y porque el procedimiento presenta las etapas siguientes:

cifrar la componente de señal de entrada, que comprende la información secundaria, para obtener una señal de referencia; y

componer la componente de señal de entrada, que comprende la información secundaria, de la componente de señal de entrada adicional, que comprende la información principal, y de la señal de referencia, que comprende la información secundaria en forma cifrada, para generar la señal de información.

21. Programa informático para llevar a cabo el procedimiento según la reivindicación 18 o el procedimiento según la reivindicación 19 o el procedimiento según la reivindicación 20, cuando el programa informático se ejecuta en un ordenador.

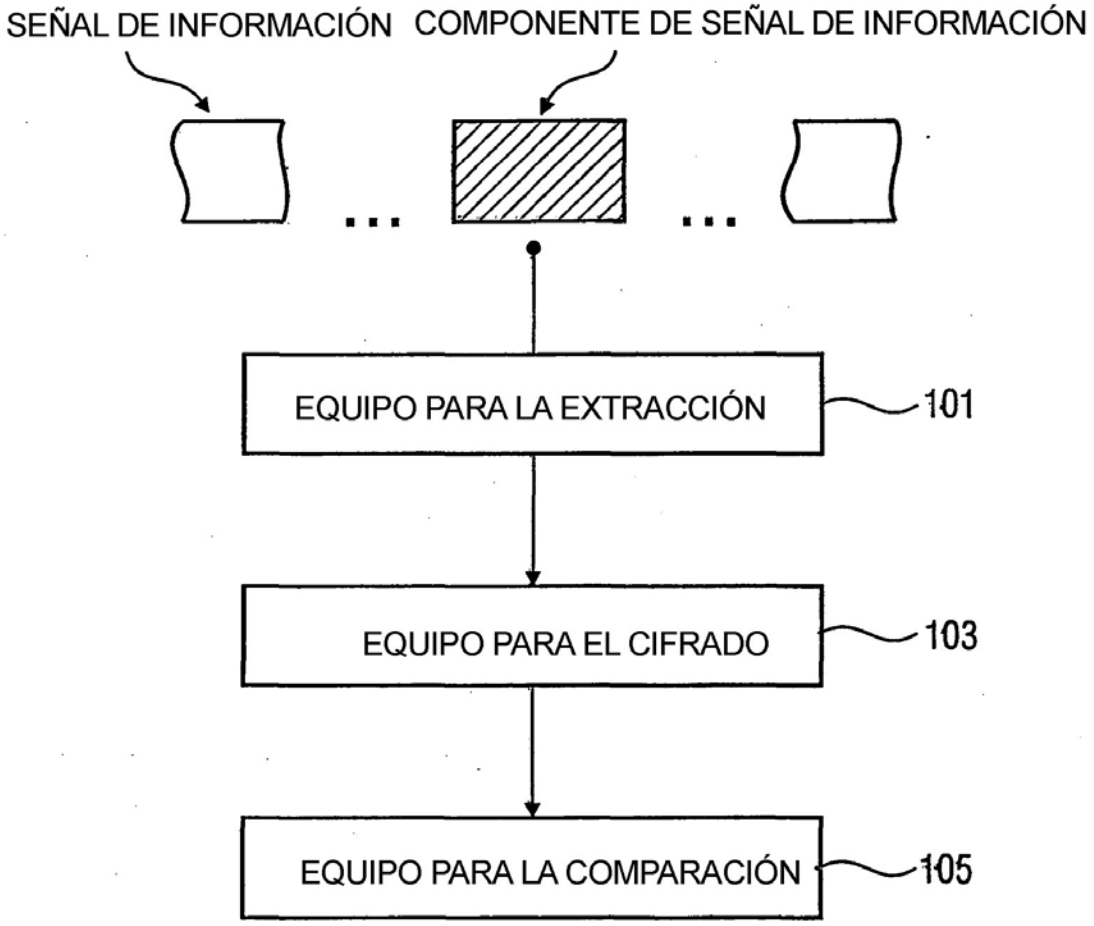
SEÑAL DE INFORMACIÓN
COMPONENTE DE SEÑAL DE INFORMACIÓN
EQUIPO PARA LA EXTRACCIÓN
101
EQUIPO PARA EL CIFRADO
103
EQUIPO PARA LA COMPARACIÓN
105

FIG. 1