

19



OFICINA ESPAÑOLA DE
PATENTES Y MARCAS

ESPAÑA



11 Número de publicación: **2 383 100**

51 Int. Cl.:
G06F 21/00 (2006.01)

12

TRADUCCIÓN DE PATENTE EUROPEA

T3

- 96 Número de solicitud europea: **04783781 .0**
96 Fecha de presentación: **10.09.2004**
97 Número de publicación de la solicitud: **1692583**
97 Fecha de publicación de la solicitud: **23.08.2006**

54 Título: **Registro de la información de distribución del contenido en un adjunto al contenido**

30 Prioridad:
23.10.2003 US 692259

45 Fecha de publicación de la mención BOPI:
18.06.2012

45 Fecha de la publicación del folleto de la patente:
18.06.2012

73 Titular/es:
**Rovi Solutions Corporation
2830 De La Cruz Boulevard
Santa Clara, CA 95050 , US**

72 Inventor/es:
SHAVIT, Eyal

74 Agente/Representante:
Carpintero López, Mario

ES 2 383 100 T3

Aviso: En el plazo de nueve meses a contar desde la fecha de publicación en el Boletín europeo de patentes, de la mención de concesión de la patente europea, cualquier persona podrá oponerse ante la Oficina Europea de Patentes a la patente concedida. La oposición deberá formularse por escrito y estar motivada; sólo se considerará como formulada una vez que se haya realizado el pago de la tasa de oposición (art. 99.1 del Convenio sobre concesión de Patentes Europeas).

DESCRIPCIÓN

Registro de la información de distribución del contenido en un adjunto al contenido

Campo de la invención

5 La presente invención se refiere en general a la distribución de contenidos y en particular, al registro de la información de distribución del contenido en un adjunto al contenido para seguimiento de la distribución y otras finalidades útiles.

Antecedentes de la invención

10 La proliferación de ordenadores personales con dispositivos de lectura/escritura tales como CD-R/W y DVD-R/W y la amplia aceptación de Internet se han convertido tanto en beneficio como en perjuicio para los proveedores de contenidos. La distribución de contenidos sobre medios tangibles tales como CD y DVD se ha convertido en la práctica estándar desde hace algún tiempo para la copia y distribución autorizada, debido a su gran capacidad de almacenamiento y bajo coste del medio. Con la disponibilidad de conexiones a Internet de alta velocidad, la distribución a través de la descarga de contenidos está demostrando ser incluso más beneficiosa como un medio de distribución conveniente de bajo coste dado que elimina el coste del medio tangible, el coste de su envío al cliente y el tiempo que el cliente ha de esperar al producto comprado. Desafortunadamente, sin embargo, estos mismos medios han facilitado también la copia y distribución no autorizada del contenido.

15 Se han propuesto y/o implementado varios sistemas de control de copia tales como la Gestión de Derechos Digitales (“DRM”) con varios grados de éxito para controlar la copia de contenidos. En tales sistemas, se proporciona comúnmente una información del control de copias que indica si el contenido puede ser copiado y/o cuantas veces puede ser copiado, en un adjunto al contenido específicamente dedicado a la transmisión de derechos.

20 Además del control de la copia del contenido, sería también útil para la aplicación legal, análisis de mercado y otras finalidades conocer la información de distribución del contenido tales como un rastro de la información relativa al copiadore o un rastro de los nodos de la red que participan en la distribución del contenido. Por ejemplo, cuando la información de distribución del contenido es una información relativa al copiadore, entonces la información relativa al copiadore puede incluir información relacionada con la generación de una copia del contenido, tal como una cualquiera o más de las siguientes: información respecto a la identificación del copiadore (por ejemplo, una identificación de usuario de un usuario del copiadore o una dirección IP del copiadore), información respecto a cómo se generó la copia (por ejemplo, información sobre cuándo se generó la copia (por ejemplo, la hora de generación de la copia u otro procesamiento de acuerdo con una zona horaria especificada o la zona horaria asociada con el copiadore), qué plataforma de ordenador y sistema operativo se usó) e información respecto al formato en el que se generó la copia (por ejemplo, un archivo descargable que reside en la memoria del ordenador o un archivo almacenado en un medio tangible, extraíble).

25 La información relativa al copiadore para la cadena completa de copia que incluye cualquiera o más de quién (por ejemplo, dirección IP del copiadore), cuándo (por ejemplo, una hora de generación de la copia por el copiadore), cómo (por ejemplo, la plataforma del copiadore) y qué (por ejemplo, formato de la copia) se denomina como el “rastreo de la información relativa al copiadore” o “trayectoria de transformación del contenido” de los contenidos. La información sobre la trayectoria de transformación del contenido de una copia es útil para varias finalidades. Un uso es identificar “fugas” en los canales de distribución (por ejemplo, fuentes de copia no autorizada o ilegal). Por ejemplo, si hay múltiples copias del contenido en las que todas tienen una misma trayectoria de transformación del contenido, entonces la fuga se sigue directamente hasta la última transformación legítima en la trayectoria. Otro uso es analizar los canales de distribución a través de los que ha ido una copia con finalidades de comercialización de modo que los productores del contenido conocerán dónde y cómo distribuir su contenido más efectivamente.

30 Por otro lado, cuando la información de distribución del contenido es un rastro de los nodos de la red que participan en la distribución del contenido, por ejemplo a través de Internet, entonces la información de distribución del contenido puede incluir, para cada paquete de información, la dirección IP de cada nodo de la red que ha enviado el paquete hasta ese punto o su camino hasta su destino final. Esta información se puede usar entonces para determinar o al menos dar pistas sobre la topología de una red que incluya los nodos de la red y/o la forma en la que se propaga el contenido en dicha red. Por ejemplo, una información de esa clase puede ser especialmente útil en la determinación de la topología de red de una red entre iguales (“P2P”), y/o la forma en la que se propaga el contenido en una red P2P.

35 Un “adjunto” al contenido es algo que se asocia con el contenido, pero no necesariamente una parte de él. Los adjuntos contienen comúnmente información sobre el contenido y/o los derechos asociados con el contenido. Ejemplos de adjuntos incluyen metadatos incluidos en un portador que contiene derechos asociados con el contenido tal como un envoltorio de DRM, una marca de agua que se añade o embebe en el contenido o una firma tal como una Firma Digital o boletín de mensaje o valor de codificación relacionado con el contenido que se añade a, se une con, o se asocia de otra forma al contenido. En aplicaciones comunes de un adjunto al contenido, la información en el adjunto se extrae y se usa para activar alguna acción mediante un sistema de exploración cuando el contenido ha de ser reproducido o copiado o consumido en otra forma.

5 En resumen, el adjunto establece un enlace entre el contenido y la información correspondiente. Se incluye comúnmente en cada copia del contenido independientemente del formato físico de la copia. A veces, sin embargo, se almacena remotamente (es decir, no se almacena en la misma localización física que el contenido), pero asociada con el contenido. Según se propaga el contenido a través de diversos canales de distribución en copias del contenido, el contenido se puede transformar repetidamente en esas copias (es decir, con el formato cambiado). El adjunto, sin embargo, en general no se cambia de forma que capture cuáles fueron esas transformaciones o las identidades de los copiadores. Por ello, los adjuntos convencionales son en modo figurado sin memoria, dado que son completamente no informativos sobre la secuencia de transformaciones a la que se sometió el contenido o las identidades de las entidades que realizan esas transformaciones.

10 Si los adjuntos tuvieran memoria, entonces podrían proporcionar información dinámica tal como información de la distribución del contenido así como la información estática proporcionada convencionalmente tal como el control de copia, origen y propietario del contenido. Por ejemplo, en el caso en que la información de distribución del contenido incluya información relativa al copiadore, el término "dinámico" significa que el adjunto al contenido se modifica en el nivel de archivo u objeto cada vez que se genera una copia del contenido de modo que incluya información relativa al copiadore para la generación de esa copia.

15 De ese modo, podría estar contenido en el adjunto al contenido actual un rastro de la información relativa al copiadore para una cadena de copias desde una copia original hasta la copia actual. En el caso en que la información de distribución del contenido incluya un rastro de los nodos de la red que participan en la distribución del contenido, tales como en una red P2P, el término "dinámico" significa que el adjunto al contenido se modifica a nivel del paquete cada vez que se renvia un paquete a través de un nodo de la red en su camino a su destino final. La modificación en este caso puede incluir la dirección IP del nodo de la red que realiza el renvio y la información que indica la hora de tal renvio.

20 Si se usa un enfoque "directo" para añadir información de distribución del contenido a un adjunto al contenido tal como la adición en serie o la concatenación de información adicional de distribución del contenido al adjunto cada vez que su contenido asociado se copia o renvia o se somete en otra forma a una transformación, entonces el tamaño del adjunto crece según la trayectoria de distribución del contenido se hace más larga. Esto puede dar como resultado un deterioro cuestionable en la calidad del contenido subyacente cuando, por ejemplo, el adjunto es una marca de agua embebida en el contenido, así como un incremento en la complejidad de embebido de la información en cada copia sucesiva y/o la extracción para recuperación de nuevo de dicha información de copias sucesivas.

25 El documento US2002/0059238 describe un procedimiento de seguimiento de la distribución de productos digitales. El documento US 2003/125964A1 describe un procedimiento de seguimiento de la distribución de productos digitales usando un código de identificación de usuario para cada usuario registrado. Un paquete de datos asociado con el producto digital incluye una marca de agua que almacena el ID de usuario que se actualiza con cada transferencia del paquete para incluir el ID del usuario que transfirió el paquete.

30 Los aspectos de la presente invención se exponen en las reivindicaciones adjuntas.

35 Se escoge un enfoque "indirecto" cuando la información de distribución del contenido no se incluye explícitamente en el adjunto como una "lista". En tal enfoque indirecto, la información de distribución del contenido se manifiesta preferentemente en su lugar en un conjunto de transformaciones reversibles que se embeben como una función en el adjunto al contenido.

40 Una realización de la presente invención proporciona adicionalmente un procedimiento para registrar la información de distribución del contenido en un adjunto al contenido que no incrementa sustancialmente el tamaño del adjunto cuando la trayectoria de distribución del contenido se hace más larga.

45 Las características adicionales y ventajas de los varios aspectos de la presente invención serán evidentes a partir de la siguiente descripción de su realización preferida, cuya descripción se debe tomar en conjunto con los dibujos adjuntos.

Breve descripción de los dibujos

50 La FIG. 1 ilustra un diagrama de bloques de una cadena de unidades de procesamiento que registran la información de distribución del contenido en un adjunto al contenido, de acuerdo con una realización de la presente invención.

La FIG. 2 ilustra un diagrama de flujo de un procedimiento realizado preferentemente por un copiadore como parte de un sistema de control de copia para proporcionar información de distribución del contenido en un adjunto al contenido cuando se genera una copia del contenido, de acuerdo con una realización de la presente invención.

55 La FIG. 3 ilustra un diagrama de bloques y la cadena de copiadores para el registro de la información de distribución del contenido en copias del contenido generado en medios tangibles, extraíbles por la cadena de copiadores, de acuerdo con una realización de la presente invención.

La FIG. 4 ilustra un diagrama de bloques del sistema que incluye una cadena de copiadores para el registro

de la información de distribución del contenido en copias del contenido generadas en archivos descargables y al menos un ordenador para la extracción de la información de distribución del contenido desde unas copias seleccionadas, de acuerdo con una realización de la presente invención.

5 La **FIG. 5** ilustra un diagrama de flujo de un procedimiento realizado preferentemente por un nodo de la red para proporcionar información de distribución del contenido en un adjunto al contenido recibido en un paquete de datos, de acuerdo con una realización de la presente invención.

La **FIG. 6** ilustra un diagrama de flujo de un procedimiento para la extracción de la información de distribución del contenido desde un adjunto al contenido, de acuerdo con una realización de la presente invención.

10 La **FIG. 7** ilustra un ejemplo de la realización de modo sucesivo de una transformación funcional de un adjunto al contenido original para almacenar información de distribución del contenido en el adjunto, de acuerdo con una realización de la presente invención.

La **FIG. 8** ilustra un ejemplo de la realización de modo sucesivo de una transformación inversa en un adjunto al contenido para extraer la información de distribución del contenido desde el adjunto, de acuerdo con una realización de la presente invención.

15 **Descripción detallada de la realización preferida**

La **FIG. 1** ilustra, como un ejemplo, un diagrama de bloques de una cadena de N unidades de procesamiento (incluyendo las unidades **101-104**) que registra la información de distribución del contenido en una forma preferida en un adjunto al contenido según se está distribuyendo el contenido a través de las N unidades. El resultado de cada una de las N unidades en este caso puede ser del mismo formato o formatos diferentes.

20 Aunque en la descripción siguiente se supone que cada una de las N unidades es un copiador que genera una copia del contenido como se describe, por ejemplo, en referencia a las **FIGS. 2-4**, varias enseñanzas que se describen con referencia al diagrama de bloques son también aplicables al caso en que cada una de las N unidades es un nodo de la red que transmite un paquete que contiene contenido como se describe, por ejemplo, con referencia a la **FIG. 5**.

25 En el ejemplo, "A(0)" es el adjunto original al contenido recibido en una copia original del contenido por el copiador **101** y "E(1)" es la información relativa al copiador para la generación de una primera copia autorizada por el copiador **101**. La copia original en este caso es la primera copia en una sucesión de copias, la primera copia autorizada es la segunda copia en la sucesión de copias, y el copiador **101** es el primer copiador en la cadena de copiadores. Mediante la aplicación de una transformación funcional "T" al adjunto original "A(0)", se genera un adjunto modificado "A(1)":

$$A(1) = T(A(0), E(1)) \tag{1}$$

35 Una "transformación funcional", tal como se entiende en general la expresión en matemáticas, es un mapa (es decir, función) cuyo dominio es algún conjunto de funciones. Así, las transformaciones funcionales son funciones que actúan sobre funciones. Un ejemplo bien conocido de una transformación funcional es la derivada. La derivada se aplica a una función y el resultado es otra función.

La transformación funcional usada en el presente documento tiene varias características importantes. Primero, se caracteriza porque tiene una transformación inversa que permite volver a extraer la información relativa al copiador desde el adjunto modificado. Por ello, se denomina en el presente documento como una "transformación reversible". Segundo, preferentemente preserva el tamaño del adjunto independientemente del número de veces que se realice sobre él una transformación funcional, tal como por las copias sucesivas del contenido por una cadena de copiadores. Con el mantenimiento del tamaño del adjunto, la transformación funcional no reduce la robustez del adjunto o la eficiencia de su embebido y extracción a y desde el contenido.

45 El adjunto A(1) es ahora el adjunto al contenido en la copia recibida por el copiador **102** (es decir, el segundo copiador en la cadena de copiadores que recibe la segunda copia en la sucesión de copias). Dado que "E(2)" es la información relativa al copiador para la generación de una copia por el copiador **102**, se genera un adjunto modificado "A(2)" mediante la aplicación de la transformación funcional "T" al adjunto "A(1)" como sigue:

$$A(2) = T(A(1), E(2)) \tag{2}$$

Mediante la sustitución de "A(1)" con la ecuación (1), "A(2)" se puede expresar también como:

$$A(2) = T(T(A(0), E(1)), E(2)) \tag{3}$$

50 Este es ahora el adjunto al contenido en la copia recibida por el copiador **103** (es decir, el tercer copiador en la cadena de copiadores que recibe la tercera copia en la sucesión de copias). Dado que "E(3)" es la información relativa al copiador para la generación de una copia por el copiador **103**, se genera un adjunto modificado "A(3)" mediante la aplicación de la transformación funcional "T" al adjunto "A(2)" como sigue:

$$A(3) = T(A(2), E(3)) \tag{4}$$

Mediante la sustitución de “A(2)” con la ecuación (3), “A(3)” se puede expresar también como:

$$A(3) = T(T(T(A(0), E(1)), E(2)), E(3)) \quad (5)$$

Este proceso continúa para cada copiado en la cadena de copiadores hasta que el copiado **104** recibe una copia del contenido (es decir., el eNésimo copiado en la cadena de copiadores que recibe la eNésima copia del contenido en la sucesión de copias). La extensión directa de las ecuaciones (1), (2) y (4) indica un adjunto modificado de:

$$A(N) = T(A(N-1), E(N)) \quad (6)$$

para la copia del contenido generado por el copiado **104**, en la que “E(N)” es la información relativa al copiado para la generación de una copia por el copiado **104** y “A(N-1)” es el adjunto al contenido de la copia recibida por el copiado **104**.

La **FIG. 2** ilustra, como un ejemplo, un diagrama de flujo de un procedimiento realizado en este caso por un copiado como parte de un sistema de control de copia para proporcionar información de distribución del contenido en un adjunto al contenido cuando el copiado genera una copia del contenido. Si se genera una copia posterior a partir de la copia generada por el mismo copiado o uno diferente, entonces el procedimiento descrito a continuación con referencia a **202-210** se realiza también para esa copia posterior de modo que se proporciona un registro de la información de distribución del contenido para la sucesión de copias en el adjunto al contenido en la copia posterior.

En **202**, el copiado recibe una solicitud para generar una copia del contenido de un usuario del copiado. El término “copiado” como se usa en el presente documento incluye ordenadores personales y otros dispositivos que se configuran a través tanto de hardware como de software para generar una copia autorizada del contenido de acuerdo con este procedimiento. El término “contenido” como se usa en el presente documento incluye material que puede tener copyright (tal como audio, video, audiovisual, texto, imágenes gráficas y programas de ordenador), así como material que en general no puede tener copyright tal como datos. El término “autorizado” como se usa en el presente documento significa autorizado por el propietario del contenido o bien directamente o bien indirectamente a través de agentes, representantes o licenciarios del propietario. El término “usuario” como se usa en el presente documento significa el operador que usa o controla en otra forma el copiado.

En **203**, el copiado recibe la información relacionada con la copia tal como información de un identificador del usuario asociado con el usuario del copiado o una dirección IP asociada con el copiado o información de un dispositivo de copia si se usa en la generación de una copia del contenido por el copiado. La expresión “dispositivo de copia” como se usa en el presente documento incluye escritores digitales tales como unidades de lectura/escritura de CD y DVD, así como dispositivos de grabación analógicos y otros.

En **204**, se descifra la copia actual del contenido en una forma convencional por el copiado usando una clave proporcionada al mismo o ya presente en el copiado. En **205**, se lee una indicación del número de copias autorizadas a ser generadas a partir de la copia actual desde una localización predefinida en la copia descifrada del contenido. La expresión “copia del contenido” como su se usa en el presente documento significa una copia del contenido así como su adjunto al contenido. En **206**, el copiado determina si la copia solicitada está permitida comprobando la indicación del número de copias autorizadas leída en **205**. Si la indicación del número de copias es una o más, entonces se permite o autoriza a realizar la copia solicitada y el procedimiento prosigue a **207**. Por otro lado, si la indicación del número de copias es cero, entonces el procedimiento salta a **201**, lo que coloca al copiado de vuelta a su estado inactivo.

En **207**, se lee un adjunto al contenido. En **208**, se modifica el adjunto mediante la realización de una transformación funcional (tal como se describe con referencia a la **FIG. 1**) sobre el adjunto usando la información relativa al copiado recibida en **203**. Después de modificar el adjunto mediante la adición a él de información relativa al copiado, en **209**, se disminuye la indicación del número de copias autorizadas a ser generadas a partir de la copia actual y el valor disminuido se escribe de nuevo en la localización predefinida en la copia descifrada del contenido de modo que sobrescriba el número original leído en **205**. Finalmente, en **210**, se genera una nueva copia del contenido mediante el cifrado del contenido descifrado previamente (junto con el adjunto modificado y el número disminuido de copias autorizadas). El procedimiento salta entonces a **201** para colocar al copiado de nuevo en su estado inactivo.

Aunque descrito como usado en conjunto con un sistema de control de copia, se apreciará que el procedimiento para registrar la información de distribución del contenido descrito el presente documento se puede realizar también sin las funciones del sistema de control de copia **205**, **206** y **209** y sin las funciones de descifrado y cifrado **204** y **210** y, por lo tanto, el procedimiento y alcance de cualesquiera reivindicaciones dirigidas al procedimiento no se han de restringir de ninguna manera como que requieren tales funciones.

La **FIG. 3** ilustra, como un ejemplo, un diagrama de bloques de una cadena de copiadores no conectados **301** y **302** que registran la información de distribución del contenido en sus copias del contenido generadas respectivamente en medios tangibles, extraíbles **320** y **330**. En cada una de las copias generadas, la información de distribución del contenido registrada en ella incluye información relativa al copiado para una cadena de copiadores usada en la generación de una sucesión de copias que conducen hasta la copia actualmente generada. Los copiadores **301** y **302** se denominan como que son “copiadores conformes” dado que responden a la información de control de copia

almacenada en las copias recibidas (tales como la **310** y **320**, respectivamente) para generar solamente copias autorizadas o legales (tales como la **320** y **330**, respectivamente) del contenido. El copiator **303**, por otro lado, se denomina como que es un “copiator no conforme” dado que ignora tal información de control de copia almacenada en una copia recibida (tal como la **330**), permitiendo de este modo que se generen copias no autorizadas o ilegales (tales como **351-359**).

Cada uno de los operadores **301**, **302** y **303** comprende dos componentes de hardware primario: un dispositivo de usuario (es decir, **311**, **312** y **313**, respectivamente) tales como un ordenador personal y un reproductor/grabador u otro dispositivo de reproducción de escritura digital (es decir, **312**, **322** y **332**, respectivamente) tal como una unidad de disco de CD o DVD. Los dispositivos de usuario **311** y **321** se configuran con módulos de control conformes **312** y **322** que hacen que sus copiatores respectivos actúen como copiatores conformes. El dispositivo de usuario **331**, por otro lado, se configura con un módulo de control no conforme **332** que permite a su copiator actuar como un copiator no conforme.

Las copias **310**, **320** y **330** se denominan como que son una “sucesión de copias” dado que la copia **330** se genera a partir de la copia **320** y la copia **320** se genera a su vez a partir de la copia **310** (tal como se indica por las líneas de puntos en la **FIG. 3**). Los copiatores **301** y **302** se denominan como que son una “cadena de copiatores” dado que generan una sucesión de copias. Aunque se muestran como copiatores diferentes en este ejemplo, una cadena de copiatores puede incluir el mismo copiator más de una vez en la cadena. Se ha de observar que las copias **351-359** no son una sucesión de copias dado que no se genera una de la siguiente. Cada una estas copias se genera ilegalmente a partir de la misma copia de origen **330**. Dado que la copia de origen **330** era una copia legal en este ejemplo, cada una de las copias ilegales **351-359** incluirá la información relativa al copiator incluida en la copia **330**, indicando de ese modo que el usuario del copiator **302** era la parte que “fugaba” o pasaba el contenido al usuario que operaba el copiator no conforme **303**.

La **FIG. 4** ilustra, como un ejemplo, un diagrama de bloques del sistema que incluye un servidor de contenidos **401**, un número de dispositivos de usuario (por ejemplo, **411**, **421**, **431** y **441**) y un ordenador de extracción **403** que comunican entre sí a través de Internet **402**. Cada uno de los dispositivos de usuario incluye una unidad de procesador para la ejecución de un módulo de control que controla el uso y copia del contenido. Un ejemplo típico de tal dispositivo de usuario es un ordenador personal.

Los dispositivos de usuario **411** y **421** incluyen respectivamente módulos de control conformes **412** y **422** que sólo permiten copias autorizadas del contenido en respuesta a la información de control de copia almacenada junto con o embebida en el contenido. El dispositivo de usuario **441**, por otro lado, incluye un módulo de control no conforme que no responde a tal información de control de copia, permitiendo de ese modo la copia no autorizada del contenido. El dispositivo de usuario **431** incluye tanto un módulo de control conforme como un módulo de control no conforme.

En este ejemplo, el dispositivo de usuario **411** descarga legalmente una copia original del contenido **414** desde el servidor de contenidos **401** a través de Internet **402** después de que el usuario o el operador del dispositivo del usuario **411** tramite su pago en cualquiera de las varias formas convencionales tales como en el sistema de Gestión de Derechos Digitales. Para las finalidades de este ejemplo, la copia **414** viene junto con un derecho para realizar y distribuir dos copias adicionales del contenido. La información de este derecho se almacena en la copia **414** en una localización secreta conocida para los módulos de control conformes, pero no conocida necesariamente para los módulos de control no conformes.

Cuando el dispositivo de usuario **421** es autorizado a descargar una copia **424** del contenido a través de Internet **402** desde el dispositivo de usuario **411**, tal descarga se gestiona preferentemente por los módulos de control conformes **412** y **422** en comunicación y cooperación entre sí. Antes de descargar la copia **424** al dispositivo de usuario **421**, se genera la copia **424** como un archivo descargable y se almacena en la memoria del dispositivo de usuario **411**. La copia original **414** se modifica también para indicar cualquier derecho que se retenga en la realización y distribución de copias adicionales más allá de la copia **424**.

La copia **424** se genera de modo que incluya información relativa al copiator en su adjunto mediante la modificación del adjunto incluido en la copia **414** con la información relativa al copiator en la misma forma en general que la descrita con referencia a **203-208** de la **FIG. 2**. Además de la información del copiator (es decir, información del copiator o dispositivo de usuario **411** en este caso y/o información de su usuario u operador), se incluye también preferentemente en el adjunto modificado al contenido incluido en la copia **424** información del dispositivo de usuario receptor **421** (tal como su dirección IP) y/o su usuario.

El derecho almacenado para realizar copias adicionales se modifica también en la copia **414**. Si el derecho a realizar una segunda copia se mantiene por el dispositivo de usuario **411**, entonces se modifica la copia **414** para indicar que solamente se puede realizar y distribuir una copia adicional a partir de ella y se genera la copia **424** de modo que indique que no se pueden realizar ninguna copia a partir de ella. Por otro lado, si el derecho a realizar una segunda copia se transfiere junto con la copia **424** al dispositivo de usuario **421**, entonces se modifica la copia **414** para indicar que no se pueden realizar más copias a partir de ella y se genera la copia **424** de modo que indique que sólo se puede realizar y distribuir una copia a partir de ella.

Suponiendo que el derecho para realizar y distribuir una copia más se transfiere junto con la copia **424** al dispositivo de usuario **421**, entonces cuando el dispositivo de usuario **431** está autorizado a descargar una copia **434** del contenido a través de Internet **402** desde el dispositivo de usuario **421**, tal descarga se gestiona preferentemente por los módulos de control conformes **422** y **432** en comunicación y cooperación entre sí. Antes de la descarga de la copia **434** al dispositivo de usuario **431**, se genera la copia **434** como un archivo descargable sin derechos para realizar copias adicionales indicados en él y se almacena en la memoria del dispositivo de usuario **421**. La primera copia **424** se modifica también para indicar que ya no quedan derechos restantes para realizar o distribuir ninguna copia a partir de la copia **424**.

Se genera la copia **424** de modo que incluya una información relativa al copiator en su adjunto al contenido mediante la modificación del adjunto incluido en la copia **424** con información relativa al copiator en general de la misma manera que se ha descrito con referencia a la **FIG. 1** para copias sucesivas. Además de la información del copiator (es decir, información del copiator o dispositivos de usuario **421** en este caso y/o información de su usuario u operador), se incluye también preferentemente información del dispositivo de usuario receptor **431** (tal como su dirección IP) y/o su usuario en el adjunto modificado incluido en la copia **434**.

En este caso, la sucesión de copias incluye la copia original **414**, la primera copia **424** y la segunda copia **434** del contenido y la cadena de copiatores incluye los dispositivos de usuario **411** y **421**. Si el usuario del dispositivo de usuario **431** realiza posteriormente una copia ilegal **438** de la segunda copia legal **434**, la copia ilegal **438** incluiría información relativa al copiator en su adjunto al contenido indicando al menos la cadena de copiatores e información del dispositivo de usuario receptor **431** de la segunda copia **434** si esa información estuviese también incluida en el adjunto por el dispositivo de usuario **421** durante la generación de la segunda copia legal **434**. En consecuencia, cualesquiera copia de la copia ilegal **438**, tal como la copia **444** que reside en el dispositivo de usuario **441**, tendría también tal información relativa al copiator incluida en su adjunto al contenido.

Ahora, suponiendo que el derecho para realizar y distribuir una copia más es retenido por el dispositivo de usuario **411**, entonces cuando el dispositivo de usuario **431** está autorizado para descargar una copia **434** del contenido a través de Internet **402** desde el dispositivo de usuario **411**, tal descarga se gestiona preferentemente por los módulos de control conformes **412** y **432** que comunican y cooperan entre sí. Antes de la descarga de la copia **434** al dispositivo de usuario **431**, se genera la copia **434** como un archivo descargable sin derechos para la realización de copias adicionales indicados en él y almacenados en la memoria en el dispositivo de usuario **411**. La copia original **424** se modifica también para indicar que ya no quedan derechos para realizar o distribuir ninguna copia más de la copia original **414**.

La copia **434** se genera de modo que incluya información relativa al copiator en su adjunto mediante la modificación del adjunto al contenido incluido en la copia **414** con su información relativa al copiator en general de la misma manera que el adjunto incluido en la copia **424**. Además de la información del copiator (es decir, información del copiator o dispositivo de usuario **411** en este caso y/o información de su usuario u operador), se incluye también preferentemente información del dispositivo de usuario receptor **431** (tal como su dirección IP) y/o su usuario en el adjunto modificado incluido en la copia **434**.

En este segundo caso, hay dos sucesiones de copias. La primera incluye la copia original **414** y la primera copia **424** y la segunda incluye la copia original **414** y la segunda copia **434**. En ambos casos, la cadena de copiatores incluye sólo el dispositivo de usuario **411** dado que el realiza ambas copias **424** y **424** y las distribuye a los dispositivos de usuario **421** y **431**. Si el usuario del dispositivo de usuario **431** realiza posteriormente una copia ilegal **438** de la segunda copia legal **434**, la copia ilegal **438** incluiría la información relativa al copiator en su adjunto señalando al dispositivo de usuario **411** como el último en su cadena de copiatores y señalando al dispositivo de usuario **431** como el receptor de la última copia autorizada o legal **434** si esa información estuviese también incluida en el adjunto por el dispositivo de usuario **411** durante la generación de la segunda copia legal **434**. En consecuencia, cualesquiera copias de la copia ilegal **438**, tal como la copia **444** que reside en el dispositivo de usuario **441**, tendría también tal información relativa al copiator incluida en su adjunto al contenido.

Si se detecta una copia ilegal o se pone a disposición en otra forma del ordenador de extracción **403**, el ordenador de extracción **403** puede realizar una sucesión de transformaciones inversas sobre el adjunto al contenido en la copia de modo que extraiga la información relativa al copiator almacenada en él por los módulos de control de conformidad tales como el **412** y **422**. A partir de esta información, el usuario del ordenador de extracción **403** puede identificar al menos el usuario y/o el dispositivo de usuario que generó la última copia autorizada de la copia ilegal y el receptor de esa última copia autorizada si esa información se incluye en la información relativa al copiator almacenada en el adjunto.

Además de las disposiciones descritas con referencia la **FIG. 3** en la que se generaron una sucesión de copias cada una en un medio tangible y con referencia la **FIG. 4** en la que se generaron una sucesión de copias cada una como un archivo de ordenador, se contemplan totalmente otras disposiciones que incluyen híbridos de estas dos como aplicables a y utilizables con el procedimiento reivindicado para el registro de información de distribución del contenido en un adjunto al contenido. En particular, en una disposición entre iguales ("P2P"), se puede proporcionar una copia original del contenido en un medio tangible tal como un CD o DVD y se pueden generar copias posteriores como archivos descargables compartidos en Internet. La copia original en este caso, así como todas las otras

descritas en el presente documento, pueden o no estar protegidas contra copia. Alternativamente, en otra disposición P2P, la copia original se puede descargar por una compañía de cable u otra compañía de distribución de medios a un decodificador digital de usuario que puede realizar entonces una copia de seguridad en un medio tangible y/o conectarse a una red doméstica a través de la que se pueden generar copias posteriores como archivos descargables compartidos en Internet.

La **FIG. 5** ilustra, como un ejemplo, un diagrama de flujo de un procedimiento realizado preferentemente dentro de un nodo de la red de una red tal como una red P2P en Internet para el registro de información de distribución del contenido en un adjunto al contenido que se recibe en un paquete de datos. En **501**, el procedimiento está inicialmente en un estado inactivo. En **502**, se recibe un paquete de datos de o bien una fuente o bien un nodo de la red previo en la red. En **503**, se lee un adjunto al contenido incluido en el paquete. En **504**, se realiza una transformación funcional tal como la descrita con referencia a la **FIG. 1**, sobre el adjunto que incluye información que identifica al nodo de la red tal como su dirección IP. Si el nodo de la red es parte de una red dinámicamente cambiante (por ejemplo, en la que cada nodo está representado por un ordenador operado por un usuario final y los usuarios finales están uniéndose y saliendo constantemente de la red), tal como el de una red Kazaa, se incluye también preferentemente una marca de tiempos u otra información que indique la hora en la que está siendo recibido y/o reenviado un paquete por el nodo de la red en el adjunto modificado por la transformación funcional. En **505**, el paquete con el adjunto modificado se transmite o envía a continuación en la red o bien al siguiente nodo de la red o bien a su destino final.

Si todos los nodos de la red que el paquete recorre entre un nodo de origen y el nodo de destino final ejecutan **501-505** sobre el paquete, entonces el paquete recibido en el destino final contendrá un rastro completo de identificadores de nodos de la red que indican la trayectoria de distribución del contenido a través de la que ha viajado el paquete. Dado que otros paquetes asociados con el mismo contenido pueden viajar a través de diferentes trayectorias de distribución incluyendo diferentes nodos de origen, se puede determinar una indicación de la topología de la red entre los nodos de origen y destino final mediante el análisis de la información de distribución del contenido contenida en los adjuntos de tales paquetes.

Si no está disponible el acceso al destino final, por ejemplo, debido a que está participando en un acto inapropiado recibiendo contenido no autorizado desde el origen, entonces los paquetes en tránsito se pueden descubrir o ser interceptados en otra forma mediante, por ejemplo, un BOT o un rastreador de la red que se usa para peinar la red, recoger paquetes, analizar la información de distribución del contenido contenida en los adjuntos al contenido incluidos en los paquetes y a continuación enviar los paquetes a lo largo de su camino a su o a sus destinos finales. Este tipo de acción no requerirá la cooperación ni del origen ni del destino final y podría conducir a una información valiosa de la topología de la red que conduce de vuelta al origen de la transmisión del paquete.

En una red dinámicamente cambiante tal como una red distribuida con control descentralizado, la determinación de la topología de la red debería ser para un momento específico (o periodo de tiempo) dado que la topología de la red cambia a lo largo del tiempo. La topología de la red en este caso puede ser considerada como un gráfico de red dinámicamente cambiante con los identificadores de nodos de la red e información de tiempo relacionada extraída de los adjuntos al contenido de paquetes de datos que indican trayectorias específicas en el tráfico de la red. Si hay grandes tendencias de larga duración en la topología de la red que se convierten en no tan dinámicas, entonces esta información se puede usar para formar heurísticas sobre búsquedas y acciones que se toman en la utilización de la red. Además de la determinación de la topología de la red, se pueden identificar "súper nodos" (es decir, nodos centralizados con prioridades y niveles de actividad más altos) así como nodos duplicados o no importantes en el gráfico de la red. Esta información permite búsquedas mejoradas en la red mediante la eliminación de los nodos duplicados o no importantes del gráfico de la red y que proporcionan una guía en dónde mirar primero (es decir, los súper nodos identificados). Además, tal conocimiento de la topología de la red se puede usar también para "simular" la red.

La **FIG. 6** ilustra, como un ejemplo, un diagrama de flujo de un procedimiento para la extracción de la información de distribución del contenido de un adjunto al contenido incluido en una copia actual generada como una de una sucesión de copias tal como se ha descrito con referencia a la **FIG. 1**. Aunque el ejemplo se describe con referencia a la extracción de información relativa al copiador en el nivel de archivo u objeto, la técnica de extracción descrita en el presente documento es igualmente aplicable con la modificación apropiada para la extracción de identificadores de red u otra información contenida en adjuntos en el nivel de paquetes.

La copia en este caso se denomina como la copia actual, debido a que es la copia que actualmente se está procesando por el procedimiento. El procedimiento se realiza mediante un programa de extracción que reside, por ejemplo, en un ordenador tal como el ordenador de extracción **403** de la **FIG. 4**, un dispositivo electrónico de consumo tal como un reproductor DVD o un decodificador. Aunque no es una parte esencial del procedimiento, el programa de extracción puede tener también la capacidad y autoridad para descifrar antes de la lectura el adjunto al contenido tal como se describe con referencia al módulo de control de conformidad **312** en la **FIG. 3** y **412** en la **FIG. 4**.

En **602**, el programa de extracción se inicia cuando recibe una solicitud por parte de un usuario del programa de extracción para extraer información relativa al copiador desde el adjunto al contenido en la copia actual. En **603**,

descifra, si es necesario, la copia actual en una forma similar a la descrita con referencia a **204** en la **FIG. 2**.

En **604**, el programa de extracción comprueba si la copia actual es una copia original del contenido, tal como las copias originales descritas con referencia a **310** en la **FIG. 3** para una copia "hard" (es decir, en un medio tangible) del contenido y **414** en la **FIG. 4** para una copia "soft" (es decir, en una forma intangible tal como un archivo descargable en la memoria) del contenido. Para determinar si la copia actual es la copia original, se incluye preferentemente en el adjunto una indicación de ello. La indicación puede ser un número de copia en la sucesión de copias, comenzando, por ejemplo, con el número de copia cero para la copia original e incrementada en uno para cada copia posterior en la sucesión de copias por el módulo de control de conformidad que genera la copia. Por otro lado, la indicación puede ser simplemente un patrón de bits que indican que la copia actual es una copia original del contenido que el programa de extracción reconoce o puede buscar en otra forma a través de algunos recursos tales como el servidor de contenidos descrito con referencia a **401** en la **FIG. 4**, un ejemplo del cual es un código de ID conectado a una lista almacenada en una base de datos de soporte.

Si la copia actual es la copia original, entonces en **605**, el resultado se notifica el usuario del ordenador de extracción y el procedimiento salta hacia atrás a **601** para volver a entrar en el estado inactivo. Por otro lado, si la copia actual no es la copia original, entonces en **606**, el procedimiento realiza una transformación inversa del adjunto y, en **607**, extrae la información relativa al copiador que corresponde a la generación de la copia actual desde el adjunto. La información relativa al copiador se almacena entonces preferentemente para una notificación posterior después de la extracción de toda la información relativa al copiador del adjunto. La transformación inversa en este caso se refiere a la transformación funcional que modifica el adjunto para incluir la información relativa al copiador tal como se describe con referencia a **208** en la **FIG. 2**. Después de realizar la transformación inversa, el adjunto para la copia previa del contenido se extrae junto con la información relativa al copiador en la generación de la copia actual. El procedimiento salta hacia atrás a **604** para determinar si el adjunto para la copia previa indica la copia original del contenido y continúa en un bucle a través de **604-607** hasta que se halla una indicación en uno de los adjuntos transformados inversamente que indican que se ha alcanzado la copia original. Después de dicha determinación, a continuación en **605**, el resultado de la información relativa al copiador para la pista completa de copias se notifica al usuario del ordenador de extracción y el procedimiento salta hacia atrás a **601** para volver a entrar en el estado inactivo.

Se sigue ahora un ejemplo para proporcionar una mejor apreciación de una transformación funcional y su transformación inversa tal como se usa en el presente documento. En el ejemplo, sea la forma general de una transformación funcional sobre el adjunto:

$$T(A, E, K) = \{T(A, E) | T(E, K)\} \tag{7}$$

en la que "T" es la transformación funcional, "A" es el adjunto al contenido, "E" es la información relativa al copiador, "K" es una clave maestra para asegurar el adjunto contra manipulación no autorizada y el símbolo "|" indica la operación de concatenación.

Para simplificar la descripción siguiente, se puede suponer que la clave maestra "K" sea una clave secreta que se comparte por un módulo de control de conformidad que realiza la transformación funcional para incluir información relativa al copiador en el adjunto y un programa de extracción que extrae la información relativa al copiador desde el adjunto. En la implementación real, sin embargo, se puede usar un mecanismo en base a la clave pública de la aplicación de reproducción o exploración del contenido, como es común en las aplicaciones de seguridad convencionales.

Si la transformación funcional es una función O exclusiva, "XOR", que se realiza sobre un adjunto original "A(0)" usando la información relativa al copiador "E(1)" para la generación de la primera copia autorizada, entonces el adjunto modificado "A(1)" resultante de la transformación funcional y a ser incluido en la primera copia autorizada del contenido es igual al siguiente:

$$A(1) = \{XOR(A(0), E(1)) | XOR(E(1), K)\} \tag{8}$$

que se puede expresar también como sigue con finalidades de simplificación:

$$A(1) = B1 | B2 \tag{9}$$

en la que,

$$B(1) = XOR(A(0), E(1)) \tag{10}$$

$$B(2) = XOR(E(1), K) \tag{11}$$

La **FIG. 7** ilustra un ejemplo de cálculos usando las ecuaciones (10) y (11) para la determinación de las partes "B1" y "B2" del primer adjunto modificado transformado "A(1)", en el que el adjunto original "A(0)", la primera información relativa al copiador "E(1)" y la clave maestra "K" tienen los siguientes valores:

$$A(0) = muestra_A \tag{12}$$

$$E(1) = id1 \quad (13)$$

$$K = m \quad (14)$$

5 Yendo en la dirección inversa, si un ordenador de extracción recibe la primera copia que incluye el adjunto modificado "A(1)", entonces la información relativa al copiador "E(1)" asociada con la generación de esa primera copia y el adjunto original "A(0)" al contenido en la copia original se pueden extraer a partir del adjunto "A(1)" en la copia actual mediante la aplicación de una transformación inversa usando la función O exclusiva, "XOR", como sigue:

$$E(1) = XOR(B2, K) \quad (15)$$

$$A(0) = XOR(B1, E(1)) \quad (16)$$

10 La **FIG. 8** ilustra un ejemplo de cálculos usando las ecuaciones (15) y (16) para la extracción de "E(1)" y "A(0)" desde el adjunto "A(1)" en la primera copia autorizada del contenido, en la que los valores para "B2" y "B1" son los calculados como se muestra en la **FIG. 7**. Como se puede ver fácilmente a partir del ejemplo, la información relativa al copiador "E(1)" asociada con la generación de la primera copia autorizada y el adjunto original "A(0)" se muestran como siendo extraídos con éxito de vuelta desde el adjunto "A(1)".

15 El ejemplo se puede extender adicionalmente para incluir la generación de un segundo adjunto modificado "A(2)" al contenido incluido en una segunda copia autorizada del contenido. Suponiendo la información relativa al copiador "E(2)" para la generación de la segunda copia autorizada, el adjunto modificado "A(2)" a ser incluido en la segunda copia autorizada del contenido es igual a lo siguiente:

$$A(2) = \{ XOR(A(1), E(2)) \mid XOR(E(2), K) \} \quad (17)$$

20 que se puede expresar también como sigue con finalidades de simplificación:

$$A(2) = C1 \mid C2 \quad (18)$$

en la que,

$$C1 = XOR(A(1), E(2)) \quad (19)$$

$$C2 = XOR(E(2), K) \quad (20)$$

25 Suponiendo ahora que sólo se recibe la segunda copia autorizada con el segundo adjunto transformado "A(2)" para el procesamiento de la extracción, entonces se usan las ecuaciones siguientes en secuencia para extraer la información relativa al copiador, "E(2)" y "E(1)", para la segunda y primera copias y los adjuntos primero modificado y original, "A(1)" y "A(0)":

$$E(2) = XOR(C2, K) \quad (21)$$

30 $A(1) = XOR(C1, E(2)) = B1 \mid B2 \quad (22)$

$$E(1) = XOR(B2, K) \quad (23)$$

$$A(0) = XOR(B1, E(1)) \quad (24)$$

35 La extensión del ejemplo anterior para la realización de transformaciones funcionales adicionales que corresponden a copias adicionales en una sucesión de copias es directa. De la misma manera, la extensión del ejemplo anterior para la realización de transformaciones inversas adicionales sobre el adjunto para copias posteriores en una sucesión de copias para extraer el adjunto original y la información relativa al copiador para una cadena de copiadores que generan la sucesión de copias es también directa.

40 Aunque se han descrito los varios aspectos de la presente invención con respecto a una realización preferida, se entenderá que la invención tiene el derecho a una protección completa dentro del alcance íntegro de las reivindicaciones adjuntas.

REIVINDICACIONES

1. Un procedimiento de operación de un copiator (311, 321) para el registro de la distribución del contenido en un adjunto al contenido, **caracterizado por** las etapas realizadas por el copiator que comprenden:
 - 5 cuando el copiator realiza una copia autorizada (320) a partir de un original (310) que tiene un contenido y un adjunto original, A(0),
la formación (208) de un adjunto al contenido modificado, A(1), mediante:
 - el cálculo de una primera parte B1 mediante la realización de una operación O exclusiva entre el adjunto original A(0) y la información relativa al copiator, E(1), asociada con el copiator;
 - 10 el cálculo de una segunda parte B2 mediante la realización de una operación O exclusiva entre la información relativa al copiator, E(1), y la clave, K, y
el cálculo del adjunto modificado, A(1), mediante la concatenación de la primera parte B1 con la segunda parte B2;
 - la generación (210) de la copia autorizada para incluir el contenido y el adjunto modificado, A(1), y la repetición de las etapas de formación y generación cuando se generan copias autorizadas adicionales usando los copiatores respectivos para formar los adjuntos modificados adicionales respectivos A(2), A(3),... para incluir información relativa al copiator E(2), E(3),... asociada con los respectivos copiatores.
2. El procedimiento de acuerdo con la reivindicación 1, en el que el adjunto es una marca de agua embebida en el contenido o metadatos asociados con el contenido o una firma relativa al contenido.
3. El procedimiento de acuerdo con la reivindicación 2, en el que la firma es un boletín de mensaje o valor de codificación calculado usando el contenido.
4. El procedimiento de acuerdo con la reivindicación 1, en el que el contenido es un material que puede disponer de protección.
5. El procedimiento de acuerdo con la reivindicación 1, en el que la información relativa al copiator incluye información de una identificación de usuario asociada con un usuario de un copiator usado para la generación de una copia autorizada del contenido o información de una dirección IP asociada con un copiator usado para la generación de una copia autorizada del contenido o información del copiator usado para la generación de la copia autorizada del contenido.
6. Un procedimiento de funcionamiento de un ordenador de extracción (403) para extraer información relativa al copiator a partir de un adjunto al contenido modificado A(1) proporcionado por un procedimiento tal como se reivindica en la reivindicación 1 en la que el adjunto modificado A(1) está compuesto de una primera parte B1 concatenada con una segunda parte B2,
en la que la primera parte B1 es el resultado de realizar la operación O exclusiva entre un adjunto original A(0) y una información relativa al copiator E(1) asociada con un copiator,
en la que la segunda parte B2 es el resultado de la realización de una operación O exclusiva entre la información
35 relativa al copiator E(1) y una clave K,
las etapas realizadas por el ordenador de extracción **caracterizadas porque** comprenden:
 - una etapa de extracción (607) que comprende:
 - 40 la realización de una operación O exclusiva entre la segunda parte B2 y la clave K para obtener la información relativa al copiator E(1),
la realización de una operación O exclusiva entre la primera parte B1 y la información relativa al copiator E(1) para obtener un adjunto A(0);
y la repetición de la etapa de extracción en el caso de una sucesión de adjuntos que se hayan generado hasta que se detecte un adjunto original.
7. El procedimiento de acuerdo con la reivindicación 6, en el que el adjunto es una marca de agua embebida en el contenido o metadatos asociados con el contenido o una firma relativa al contenido.
8. El procedimiento de acuerdo con la reivindicación 6, en el que el contenido es un material que puede disponer de protección.
9. El procedimiento de acuerdo con la reivindicación 6, en el que la información relativa al copiator incluye información de una identificación de usuario asociado con un usuario de un copiator o información de una dirección IP asociada con un copiator o información de un dispositivo de copia usado en la generación de una copia del contenido por un copiator.
10. Aparato (311, 321) para el registro de la distribución del contenido en un adjunto al contenido, comprendiendo el aparato un copiator configurado, cuando el copiator realiza una copia autorizada (320) a partir de un original (310) que tiene contenido y un adjunto original, A(0); para formar (208) un adjunto al contenido modificado, A(1), mediante:

- el cálculo de una primera parte B1 mediante la realización de una operación O exclusiva entre el adjunto original A(0) y la información relativa al copiadore, E(1), asociada con el copiadore;
- el cálculo de una segunda parte B2 mediante la realización de una operación O exclusiva entre la información relativa al copiadore, E(1), y la clave, K, y
- 5 el cálculo del adjunto modificado, A(1), mediante la concatenación de la primera parte B1 con la segunda parte B2; para generar la copia autorizada para incluir el contenido y el adjunto modificado, A(1), y repetir la formación y generación cuando se generan copias autorizadas adicionales usando los copiadore respectivos para formar los adjuntos modificados adicionales respectivos A(2), A(3),... para incluir información relativa al copiadore E(2), E(3),... asociada con los respectivos copiadore.
- 10 11. El aparato de acuerdo con la reivindicación 10, en el que el copiadore es un ordenador, o un dispositivo electrónico de consumo, o un decodificador.
12. El aparato de acuerdo con la reivindicación 10, en el que el adjunto es una marca de agua embebida en el contenido o metadatos asociados con el contenido o una firma relativa al contenido.
- 15 13. El aparato de acuerdo con la reivindicación 10, en el que el contenido es un material que puede disponer de protección.
14. El aparato de acuerdo con la reivindicación 10, en el que la información asociada con el copiadore incluye información de una identificación de usuario asociada con un usuario del copiadore o información de una dirección IP asociada con el copiadore o información de un dispositivo de copia usado en la generación de la copia por el copiadore.
- 20 15. El aparato de acuerdo con la reivindicación 10, en el que el copiadore se configura además para hacer que la copia se genere sobre un medio tangible o un archivo descargable.
16. Un aparato (403) para la extracción de información de distribución del contenido a partir de una copia del contenido, en la que un adjunto modificado A(1) está compuesto de una primera parte B1 concatenada con una segunda parte B2, comprendiendo el aparato:
- 25 un medio de extracción que comprende:
- medios para la realización de una operación O exclusiva entre la segunda parte B2 y la clave K para obtener la información relativa al copiadore E(1),
- medios para la realización de una operación O exclusiva entre la primera parte B1 y la información relativa al copiadore E(1) para obtener un adjunto A(0);
- 30 y configurado para repetir la extracción en el caso de una sucesión de adjuntos que se hayan generado hasta que se detecte un adjunto original.
17. El aparato de acuerdo con la reivindicación 16, en el que el adjunto es una marca de agua embebida en el contenido o metadatos asociados con el contenido o una firma relativa al contenido.
- 35 18. El aparato de acuerdo con la reivindicación 16, en el que el contenido es un material que puede disponer de protección.
19. El aparato de acuerdo con la reivindicación 16, en el que la información relativa al copiadore incluye información de una identificación de usuario asociada con un usuario de un copiadore usado para generar una de las copias autorizadas o información de una dirección IP asociada con un copiadore usado para generar una de las copias autorizadas.
- 40 20. El aparato de acuerdo con la reivindicación 19, en el que una de las copias autorizadas es un archivo descargable.

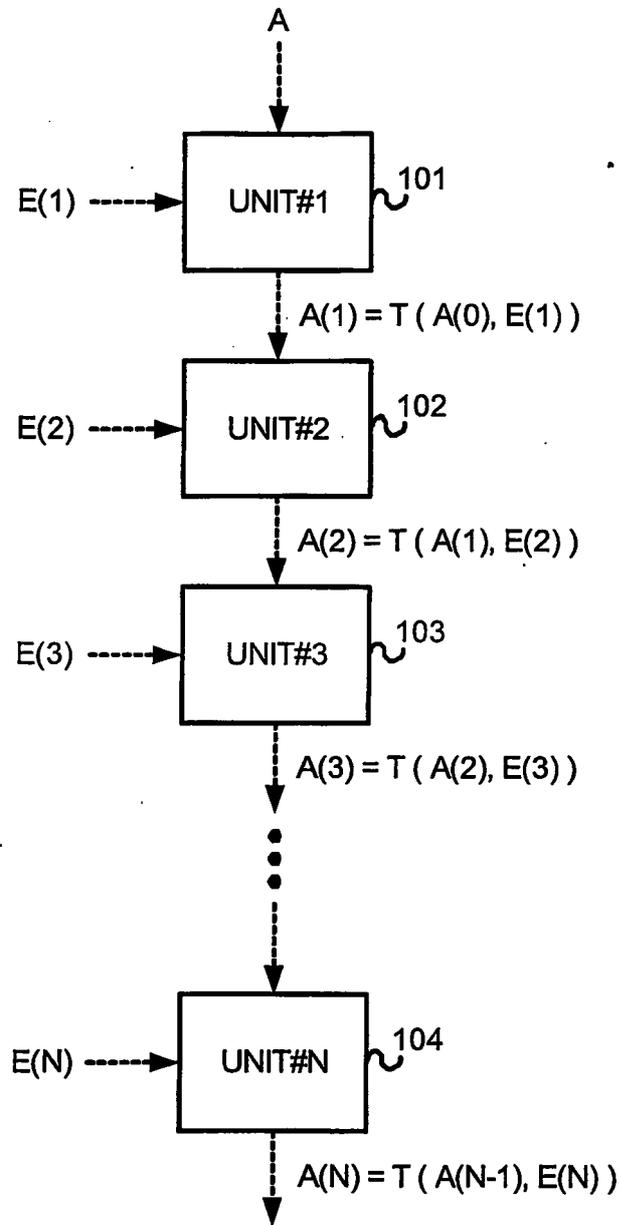


FIG.1

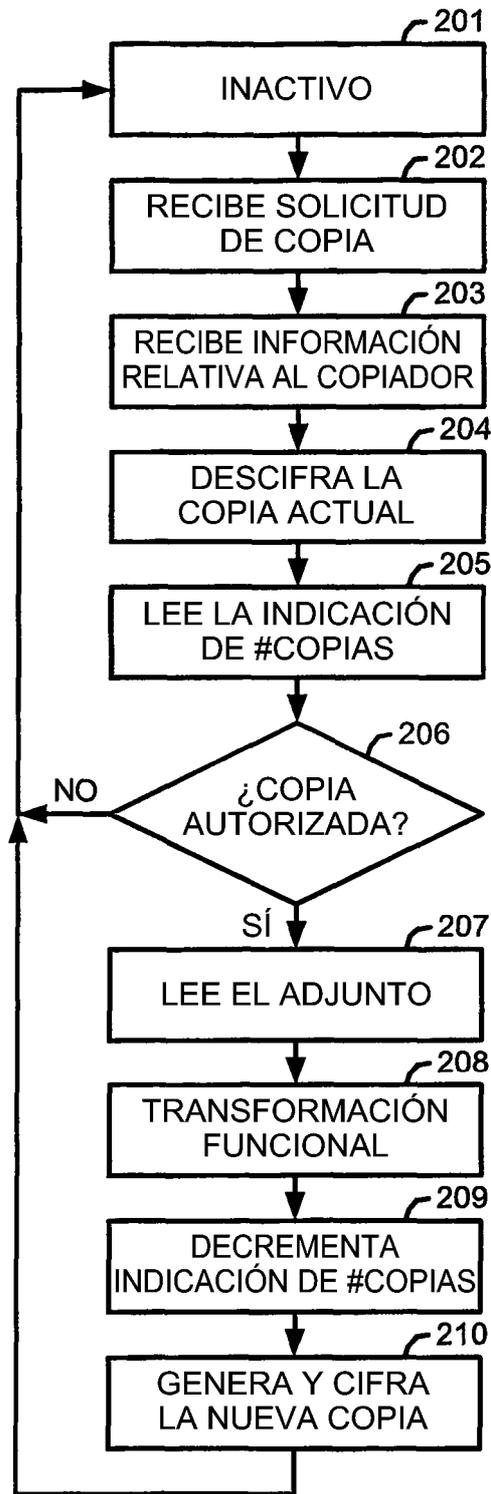


FIG.2

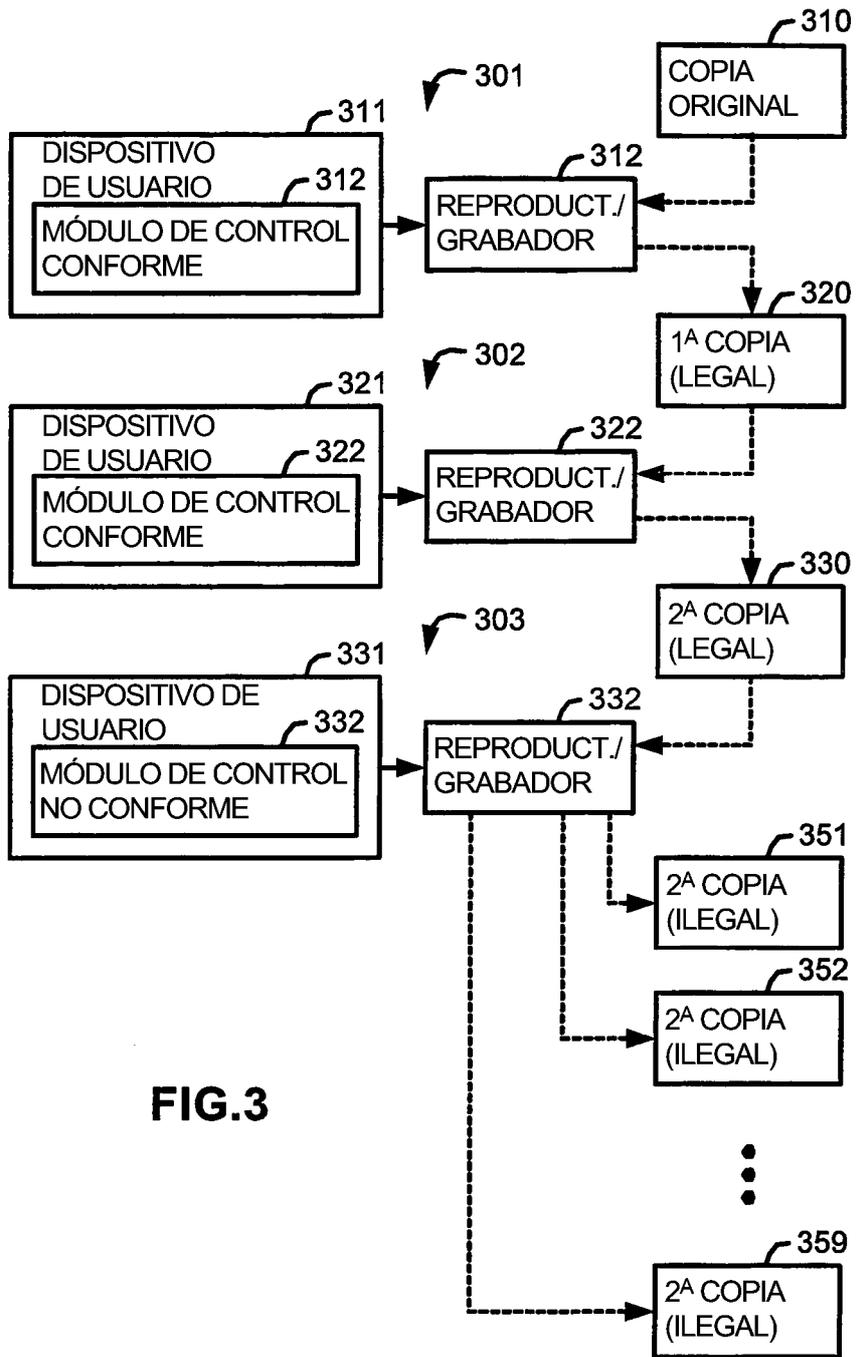


FIG.3

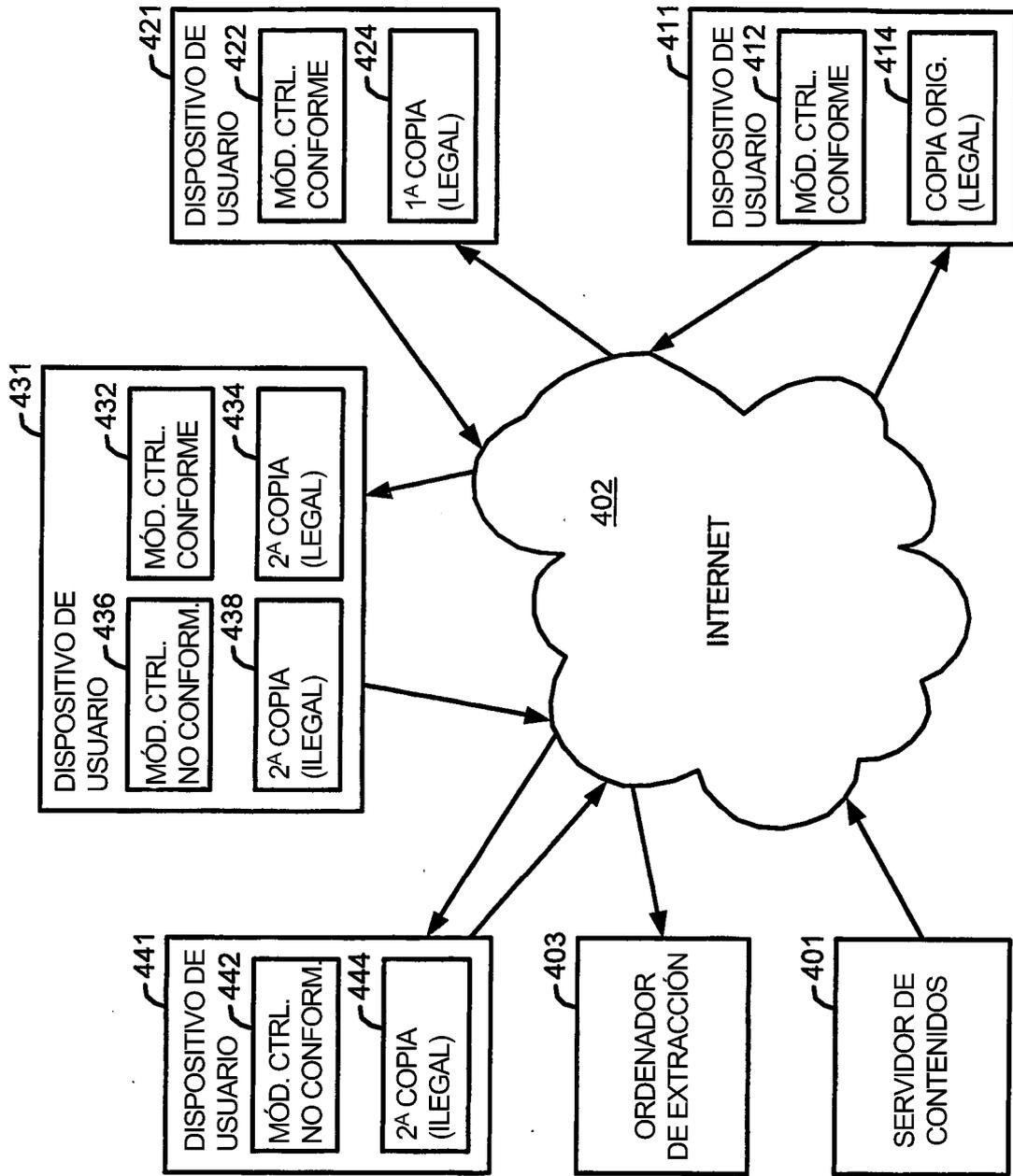


FIG.4

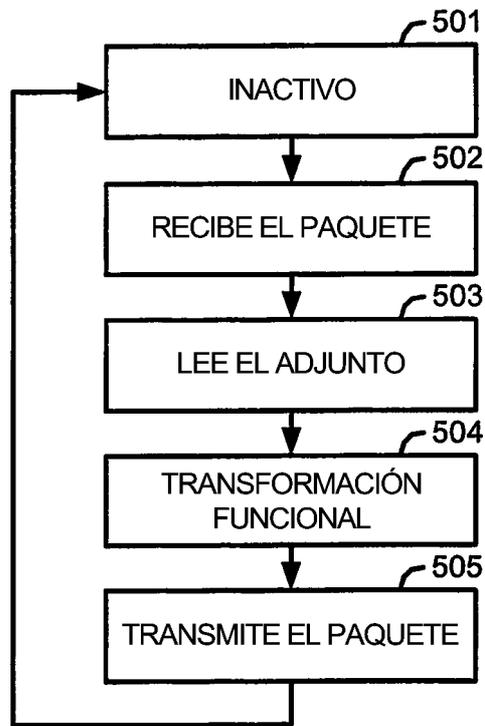


FIG.5

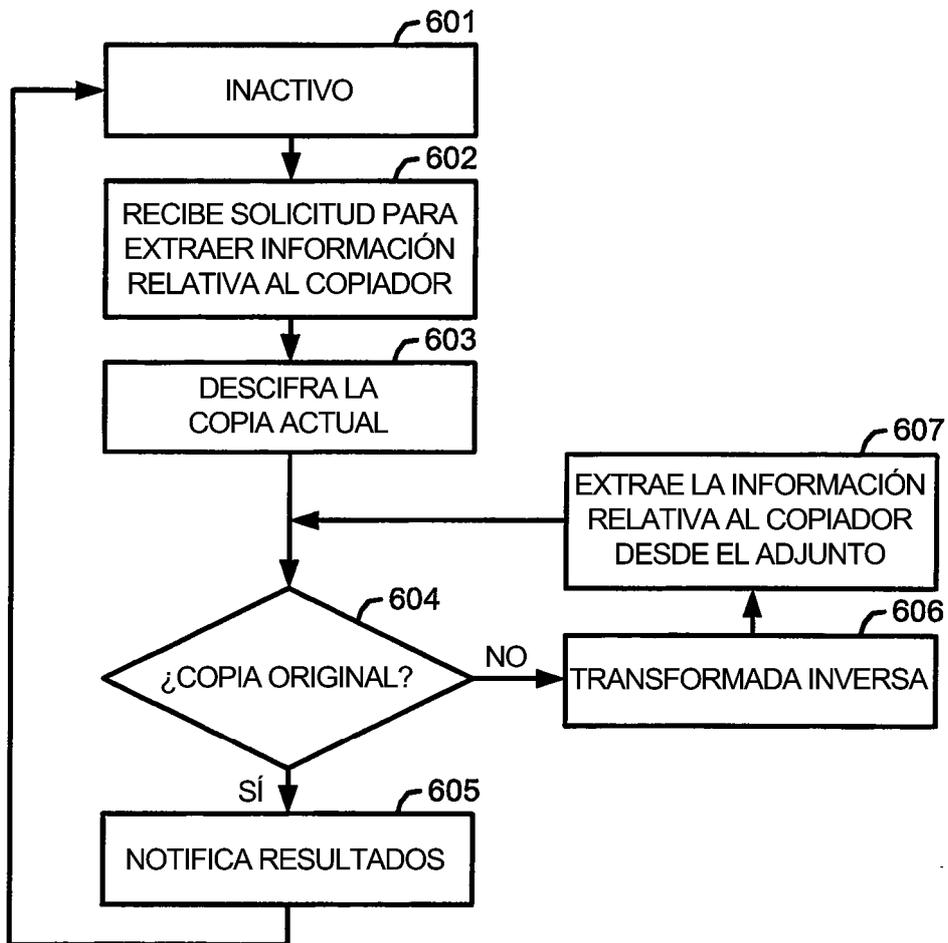


FIG.6

A(0)	s	a	m	p	i	e	-	A
	01110011	01100001	01101101	01110000	01101100	01100101	01011111	01000001
E(1)	i	d	1	i	d	1	i	d
	01101001	01100100	00110001	01101001	01100100	00110001	01101001	01100100
B1	00011010	00000101	01011100	00011001	00001000	01010100	00110110	00100101
	%1a	%05	\	%19	%08	T	6	%
E(1)	i	d	1					
	01101001	01100100	00110001					
K	m	m	m					
	01101101	01101101	01101101					
B2	00000100	00001001	01011100					
	%04	%09	\					

FIG.7

