(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 426 256**

(51) Int. CI.:

H04L 29/06 (2006.01)
G06F 1/00 (2006.01)

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(96) Fecha de presentación y número de la solicitud europea: **26.03.2001 E 01107387 (1)**

(97) Fecha y número de publicación de la concesión europea: **31.07.2013 EP 1146714**

(54) Título: **Sistema y procedimiento para la protección de obras digitales**

(30) Prioridad:

24.03.2000 US 536089

(45) Fecha de publicación y mención en BOPI de la traducción de la patente:
22.10.2013

(73) Titular/es:

CONTENTGUARD HOLDINGS, INC. (100.0%)
103 FOULK ROAD, SUITE 200-M
WILMINGTON, DELAWARE 19803, US

(72) Inventor/es:

WANG, XIN

(74) Agente/Representante:

MILTENYI, Peter

DESCRIPCIÓN

Sistema y procedimiento para la protección de obras digitales

Esta invención se refiere a la gestión de derechos de documentos (*document rights management*), y más particularmente, a un procedimiento para la protección de obras digitales (*digital works*) que utiliza una encriptación que preserva el formato (*format-preserving encryption*) que permite transformaciones ocultas (*blind transformations*).

Una de las cuestiones más importantes que impiden una amplia distribución de documentos u obras digitales a través del comercio electrónico es la actual falta de protección de los derechos de propiedad intelectual de los propietarios de los contenidos durante la distribución y el uso de los documentos u obras digitales. Los esfuerzos para resolver este problema se han denominado "Gestión de Derechos de la Propiedad Intelectual" ("IPRM"- "*Intellectual Property Rights Management*"), "Gestión de Derechos de la Propiedad Digital" ("DPRM" - "*Digital Property Rights Management*"), "Gestión de la Propiedad Intelectual" ("IPM" - "*Intellectual Property Management*"), "Gestión de Derechos" ("RM" - "*Rights Management*"), "Gestión de Derechos Digitales" ("DRM" - "*Digital Rights Management*") y "Gestión Electrónica de Derechos de Autor" ("ECM" - "*Electronic Copyright Management*"). En el centro de la gestión de derechos digitales se encuentra el tema subyacente de asegurar que sólo los usuarios autorizados pueden realizar operaciones en los documentos u obras digitales que han adquirido. Una vez accedido, el contenido no debe ser distribuido o utilizado violando las especificaciones de los derechos del propietario del contenido.

Un documento u obra, según se usa el término en este documento, es cualquier unidad de información sujeta a distribución o transferencia, incluyendo pero no limitado a correspondencia, libros, revistas, diarios, periódicos, otros documentos, software, fotografías y otras imágenes, clips de audio y de vídeo, y otras presentaciones multimedia. Un documento puede estar realizado en forma impresa en papel, así como en datos digitales en un medio de almacenamiento, o de cualquier otra manera conocida en una variedad de medios. Una obra digital, según se usa el término en este documento, es cualquier documento, texto, audio, multimedia u otro tipo de obra o parte de la misma mantenida en un formato digital que puede ser reproducido o representado (*rendered*) por medio de un dispositivo o un programa de software.

En el mundo de los documentos impresos, una obra creada por un autor es generalmente proporcionada a un editor, que formatea e imprime varias copias de la obra. Las copias son entonces enviadas por un distribuidor a las librerías y otros puntos de venta, en los que los ejemplares son comprados por usuarios finales.

Mientras que la baja calidad del copiado y el alto coste de la distribución del material impreso han servido como elemento disuasorio para la copia ilegal de la mayoría de los documentos impresos, es demasiado fácil copiar, modificar y redistribuir documentos electrónicos no protegidos. En consecuencia, es necesario algún procedimiento de protección de documentos electrónicos para hacer que sea más difícil la copia ilegal de éstos. Esto servirá como elemento disuasorio para la copia, incluso si todavía es posible, por ejemplo, hacer copias impresas de documentos impresos y duplicarlos de manera tradicional.

En relación a los documentos impresos, hay una etapa adicional de digitalizar el documento antes de que pueda ser redistribuido electrónicamente, lo cual sirve como elemento disuasorio. Por desgracia, se ha reconocido ampliamente que no hay forma viable de evitar que la gente haga distribuciones no autorizadas de documentos electrónicos por medio de los sistemas actuales de comunicaciones y de representación de propósito general, tales como ordenadores personales, estaciones de trabajo (*workstations*), y otros dispositivos conectados a través de redes de área local (LANs - *Local Area Networks*), intranets e Internet. Muchos intentos de proporcionar soluciones basadas en hardware para evitar la copia no autorizada han demostrado no tener éxito.

Se han usado dos esquemas básicos para tratar de resolver el problema de la protección de documentos: contenedores seguros (*secure containers*) (sistemas que se basan en mecanismos criptográficos) y sistemas de confianza (*trusted systems*).

Los mecanismos criptográficos encriptan (*encrypt*) (o "cifran" - "*encipher*") documentos que después se distribuyen y almacenan públicamente, y en última instancia son desencriptados (*decrypted*) en privado por usuarios autorizados. Los mecanismos criptográficos proporcionan una forma básica de protección durante la entrega de documentos desde un distribuidor de documentos a un usuario previsto a través de una red pública, así como durante el almacenamiento de documentos en un medio inseguro. Muchas de las soluciones de gestión de derechos digitales se basan en el encriptado de la obra digital y la distribución de tanto el mensaje encriptado como la clave de desencriptación al sistema del consumidor. Aunque se utilizan diferentes esquemas para ocultar la clave de desencriptación a los consumidores, el hecho es que toda la información necesaria está disponible para que un usuario malicioso rompa la protección de la obra digital. Teniendo en cuenta que los ordenadores de propósito general actuales y los sistemas operativos del consumidor proporcionan poco en cuanto a mecanismos de seguridad sofisticados, la amenaza es real y evidente.

Un "contenedor seguro" (o simplemente un documento encriptado) ofrece una forma de mantener encriptado el contenido del documento hasta que se cumplan una serie de condiciones de autorización y se satisfagan algunos términos de los derechos de autor (por ejemplo, pago por uso). Después de verificar con el proveedor del documento las diversas condiciones y términos, el documento es entregado al usuario en un formato no encriptado (*clear form*). Los productos comerciales tales como los *Cryptolopes* de IBM y los *Digiboxes* de InterTrust pertenecen a esta categoría. Claramente, el enfoque de contenedor seguro proporciona una solución para proteger el documento durante la entrega a través de canales inseguros, pero no proporciona ningún mecanismo para evitar que los usuarios legítimos obtengan el documento no encriptado (*clear document*) y a continuación lo usen y redistribuyan violando la propiedad intelectual de los propietarios del contenido.

Los mecanismos criptográficos y contenedores seguros se centran en la protección de la obra digital durante su transferencia al usuario/comprador autorizado. Sin embargo, una obra digital debe ser protegida de su uso por parte de usuarios maliciosos y programas de software maliciosos. Incluso si un usuario es una persona de confianza, el sistema del usuario puede ser susceptible de ser atacado. Un problema importante con el que se enfrenta el comercio electrónico en cuanto a obras digitales es el de garantizar que la obra está protegida en el dispositivo del consumidor de destino. Si la protección de la obra digital se ve comprometida, se pierde información valiosa y sensible. Para complicar las cosas, los ordenadores de propósito general actuales y los sistemas operativos del consumidor son deficientes en las áreas de seguridad e integridad. La protección de la obra en todo su uso es un tema mucho más complejo que permanece en gran medida sin resolverse.

En el enfoque del "sistema de confianza", el sistema en su totalidad se encarga de impedir el uso y la distribución no autorizada del documento. La construcción de un sistema de confianza por lo general implica la introducción de un nuevo hardware tal como un procesador seguro, almacenamiento seguro y dispositivos de representación (*rendering*) segura. Esto también requiere que todas las aplicaciones que se ejecutan en los sistemas de confianza estén certificadas como de confianza. Aunque la construcción de sistemas de confianza a prueba de manipulación (*tamper-proof*) sigue siendo un verdadero desafío para las tecnologías existentes, las tendencias actuales del mercado sugieren que los sistemas abiertos y no confiables, tales como PC's y estaciones de trabajo, serán los sistemas dominantes que se utilizarán para acceder a los documentos con derechos de autor. En este sentido, los entornos informáticos existentes tales como PC's y estaciones de trabajo equipados con sistemas operativos populares (por ejemplo, Windows y UNIX) y aplicaciones de representación (*render*) (por ejemplo, Microsoft Word) no son sistemas de confianza y no se puede hacer que sean de confianza sin alterar significativamente sus arquitecturas.

En consecuencia, a pesar de que se pueden desplegar ciertos componentes de confianza, los usuarios deben seguir confiando en diversos elementos y sistemas desconocidos y no confiables. En estos sistemas, aunque se espera que sean seguros, frecuentemente se detectan y experimentan errores y debilidades inesperadas.

Los procedimientos de encriptado simétrico y asimétrico convencionales tratan los mensajes a encriptar como cadenas binarias básicamente. La aplicación de procedimientos de encriptado convencionales a los documentos tiene algunos inconvenientes. Los documentos son típicamente mensajes relativamente largos; el encriptado de mensajes largos puede tener un impacto significativo en el rendimiento de cualquier aplicación que necesita desencriptar el documento antes de usarlo. Más importante aún, los documentos son mensajes formateados que se basan en aplicaciones de representación adecuadas para visualizarlos, reproducirlos, imprimirlos e incluso editarlos. Puesto que el encriptado de un documento generalmente destruye información de formato, la mayoría de las aplicaciones de representación requieren que el documento sea desencriptado a un formato no encriptado (*clear form*) antes de ser procesado. El desencriptado previo a la representación abre la posibilidad de que el documento sea divulgado en un formato no encriptado (*in the clear*) después de la etapa de desencriptación a cualquiera que quiera interceptarlo.

Hay una serie de problemas en la gestión de los derechos: autenticación, autorización, contabilización, pago y compensación financiera, especificación de los derechos, verificación de los derechos, aplicación de los derechos y protección de los documentos. La protección de los documentos es una cuestión particularmente importante. Después de que un usuario haya satisfecho (*honored*) los derechos del propietario del contenido y se le haya permitido llevar a cabo una operación en particular con un documento (por ejemplo, imprimirlo, verlo en pantalla, reproducir la música o ejecutar el software), el documento es de suponer que está en un formato no encriptado (*in the clear*), o desencriptado. En pocas palabras, el problema de la protección de documentos es evitar que se vean comprometidos los derechos de los propietarios del contenido cuando el documento se encuentra en su estado más vulnerable: almacenado, en un formato no encriptado (*in the clear*), en una máquina bajo el control del usuario.

Aun cuando el documento es entregado de forma segura (por lo general en formato encriptado) por parte de un distribuidor al usuario, éste debe ser representado (*rendered*) en un formato de representación de datos antes de que el usuario pueda ver o manipular de otro modo el documento. En consecuencia, para lograr el nivel más alto posible de protección, es importante proteger el contenido del documento tanto como sea posible, al mismo tiempo que es revelado al usuario en una etapa posterior y de una forma que sea difícil recuperarlo en un formato útil.

En los enfoques conocidos de distribución de documentos electrónicos que utilizan el encriptado, un documento encriptado es procesado en varias etapas diferentes. En primer lugar, el documento encriptado es recibido por el usuario. En segundo lugar, el usuario utiliza su clave privada (en un sistema criptográfico de clave pública) para desencriptar los datos y derivar el contenido no encriptado (*clear content*) del documento. Finalmente, el contenido no encriptado (*clear content*) es pasado entonces a una aplicación de representación, que convierte el documento legible por ordenador en el documento acabado, ya sea para su visualización en la pantalla del ordenador del usuario o para imprimir una copia en papel. Se requiere el contenido no encriptado (*clear content*) para su representación, ya que, en la mayoría de los casos, la aplicación de representación es un producto de terceros (como Microsoft Word o Adobe Acrobat Reader) que requiere que el documento de entrada esté en un formato específico. Se debe apreciar, entonces, que entre las etapas segunda y tercera, el documento previamente protegido es vulnerable. Se ha desencriptado, pero todavía está almacenado en un formato electrónico no encriptado (*clear electronic form*) en el ordenador del usuario. Si el usuario es descuidado o de lo contrario está motivado en cuanto a minimizar gastos, el documento puede ser fácilmente redistribuido sin adquirir los permisos necesarios del propietario del contenido.

Aunque ningún sistema es completamente a prueba de suplantación de identidad o inmune a los ataques, algunas técnicas recientes protegen las obras digitales limitando el uso de la obra digital a un dispositivo físico específico de usuario. Estas técnicas requieren que el usuario proporcione información privada o información de estado del sistema desde el sistema o dispositivo físico que el usuario pretende utilizar para procesar la obra digital. La información del estado del sistema se define generalmente como la información de configuración del sistema, tales como parámetros del sistema, identificador de CPU, identificadores de dispositivos, identificadores de centro de información de red (NIC - *Network Information Center*), configuración de controladores, etc. En estas técnicas, el contenido digital se encripta mediante una clave de sesión, entonces la clave de sesión, en lugar de utilizar la clave de encriptado del usuario, es encriptada utilizando una combinación de la información del sistema o de su estado y las credenciales del usuario. Entonces, tanto el contenido encriptado como la clave son transmitidos al repositorio de destino. Con el fin de utilizar la obra encriptada recibida, el usuario debe ponerse en contacto con una entidad autorizadora de confianza (por lo general un programa de software en una ubicación remota) que verifica la identidad y credenciales del usuario, entonces, junto con el estado del sistema, se desencripta la clave de sesión y finalmente se desencripta el contenido para que pueda ser usado.

Aplicaciones comerciales tales como el lector seguro de Adobe Acrobat y el reproductor seguro Microsoft MediaPlayer validan el uso de la obra digital validando un comprobante (*voucher*) de licencia para las credenciales de usuario y derechos de uso apropiados. Entre las credenciales de usuario están los identificadores de dispositivos del sistema, tales como el identificador de CPU o ciertos números de serie de los dispositivos. En el momento en que el usuario invoca una operación sobre la obra digital, la aplicación verifica si el dispositivo especificado está presente. Esto proporciona la seguridad de que la obra digital no ha sido transmitida a un usuario no autorizado (en realidad a un dispositivo no autorizado). Mientras la verificación programática proporciona un nivel mínimo de seguridad, ésta depende de la seguridad del secreto, que reside en el dispositivo del usuario. No sólo se puede violar la clave de desencriptado, sino que también los propios identificadores de dispositivos son particularmente susceptibles a la amenaza de suplantación de identidad.

Los esquemas de protección de Acrobat Reader y MediaPlayer funcionan permitiendo que la aplicación de representación identifique los dispositivos requeridos en el sistema del usuario según se especifica en el comprobante de licencia emitido para la obra digital. Esto proporciona un nivel de protección adecuado en muchas circunstancias (es decir, si el usuario es de confianza y el dispositivo de representación especificado del usuario no es susceptible al ataque). La debilidad de los esquemas es que se basan en la suposición de que no se verán comprometidos la protección de la clave criptográfica ni la integridad del comprobante de licencia.

Estas técnicas son realmente más una técnica de autenticación que una técnica de protección, en la que una vez que la identidad del usuario y la información de credenciales, la información de estado del sistema se ha verificado o se ha recibido un comprobante de licencia, el contenido es desencriptado a su estado no encriptado (*clear state*) y entonces se vuelve vulnerable al ataque. No se ofrece ninguna protección de la obra digital a lo largo de su uso. Además, el enfoque de información del usuario es problemático en el sentido de que supone que el usuario estará suficientemente disuadido de distribuir su información personal. En otras palabras, para que el enfoque de la información del usuario tenga éxito, tendría que haber consecuencias graves para los usuarios que puedan revelar su identidad privada e información de credenciales.

Un inconveniente importante de los esquemas que vinculan la autorización a un dispositivo específico es que requieren que el usuario divulgue información sensible (por ejemplo, el número de CPU o cualquier otra información personal) lo cual plantea una preocupación por cuestiones de privacidad. Aunque el usuario divulga la información voluntariamente (la única opción para el usuario si éste no desea divulgar esta información es no recibir la obra digital) sería deseable proporcionar un esquema de protección que podría asegurar una obra digital en el dispositivo del usuario sin que se requiera información privada. También sería deseable proporcionar una solución DRM que no

se base en la protección de la clave criptográfica o la integridad del comprobante de licencia. Sería deseable proporcionar una solución DRM que retrase la desencriptación del contenido digital al último momento posible.

Por consiguiente, sería beneficioso proporcionar un esquema de distribución de documentos electrónicos que minimice las desventajas de los sistemas conocidos. Este esquema evitaría que los usuarios obtengan un formato útil de un documento distribuido electrónicamente durante los procesos de descodificación y representación.

Ramanujapuram, A. et al., "Digital Content & Intellectual Property Rights: A specification language and tools for rights management," Dr. Dobb's Joumal, M&T Publ., Redwood City, CA, US, vol. 23, no. 12, Diciembre 1998, páginas 20-22, 24, 26-27 se refiere a documentos con auto-protección (SPD - *self-protecting documents*) y sugiere que experimentan cuatro etapas de transformación durante su ciclo de vida. En primer lugar, la preparación del SPD, en la que el documento original es convertido a un formato intermedio. En segundo lugar, la creación del SPD, en la que se crea un SPD genérico usando el formato intermedio del documento y la especificación de derechos, marcaje (*watermark*) y políticas. En tercer lugar, la personalización del SPD, en la que el SPD es transformado en un SPD personalizado usando las credenciales del usuario final y el conjunto de permisos adquiridos para este documento. En cuarto lugar, el uso del SPD, en el que el SPD es procesado de forma segura en la pantalla o la impresora.

US-A-5 768 390 divulga un sistema criptográfico con enmascaramiento para transformar una secuencia de bloques de input de texto plano o datos de texto encriptado en una correspondiente secuencia de bloques de output de datos al mismo tiempo que proporciona una protección mejorada contra ataques criptográficos.

EP-A-0 932 298 divulga un procedimiento de marcaje (*watermarking method*) electrónico, un sistema de distribución de información electrónica y un medio de almacenamiento para intercambiar datos a través de una red en que una primera entidad realiza un primer proceso de encriptación de los datos originales, una segunda entidad gestiona o distribuye los datos proporcionados por la primera entidad de encriptación e incorpora (*embeds*) una marca (*watermark*) electrónica en los datos y una tercera entidad realiza un segundo proceso de encriptación de los datos en los que se ha incorporado la marca electrónica.

WO 99/16205 A divulga un procedimiento y sistema de transformación dinámica de material encriptado que habilita software bajo demanda y servicios de subscripción a software a través de un filtro de transformación para regular, medir y cobrar por el uso de productos de software.

US-A-5 586 186 divulga un procedimiento y sistema para controlar el acceso no autorizado a información distribuida a usuarios permitiendo la encriptación del software mediante una única clave de encriptación y su desencriptación mediante una multiplicidad de claves de "desencriptación", en que cada una de las cuales es única para un usuario en particular.

Es un objeto de la presente invención proporcionar un procedimiento y correspondiente sistema mejorados de protección de una obra digital durante los procesos de desencriptación y representación.

Este objeto es solucionado por la materia de las reivindicaciones independientes. Se definen realizaciones preferidas en las reivindicaciones dependientes.

Un documento con auto-protección ("SPD"), de acuerdo con la invención, no está sujeto a las desventajas de la técnica anterior anteriormente indicadas. Mediante la combinación de un documento encriptado con un conjunto de permisos y un segmento de código ejecutable que incluye la mayor parte del software necesario para extraer y usar el documento encriptado, el documento con auto-protección cumple con la protección del contenido del documento sin necesidad de hardware y software adicionales.

El sistema SPD se divide en un creador de contenido (similar al autor y editor del modelo tradicional) y un distribuidor de contenido. El autor/editor crea el documento original, y decide qué derechos deben ser permitidos. El distribuidor entonces personaliza el documento para su uso por parte de varios usuarios, garantizando a través de la personalización que los usuarios no exceden los permisos que han comprado.

En el sistema del usuario, el documento con auto-protección es desencriptado en el último momento posible. En una forma de realización de la invención, también se proporcionan varias funciones (*facilities*) de representación (*rendering*) dentro del SPD, de manera que el uso del SPD no necesita depender de aplicaciones externas que podrían no ser de confianza (y que podrían invitar a un uso no autorizado). En una realización alternativa, se especifican las interfaces y protocolos para que una aplicación de representación de terceros interactúe con el SPD para proporcionar una representación (*rendering*) de confianza.

En una forma de realización de la invención, el documento encriptado es desencriptado por el sistema del usuario, mientras que al mismo tiempo es "polarizado" con una clave que depende, al menos en parte, del estado del sistema del usuario. La polarización puede ser criptográficamente menos segura que la encriptación que se utiliza para la

distribución, pero sirve para impedir la copia. En esta forma de realización, la despolarización es realizada durante o después del proceso de representación, con el fin de hacer que cualquier forma intermedia del documento sea esencialmente inutilizable.

En otra forma de realización de la invención, un procedimiento de proteger una obra digital utiliza una función de transformación oculta para transformar una obra digital encriptada en datos de presentación encriptados. El contenido digital del autor (*originator*) está protegido en su forma original por no ser desencriptado. Este procedimiento permite que la aplicación de representación o reproducción procese el documento encriptado en forma de datos de presentación encriptados sin desencriptarlos primero. Los datos de presentación encriptados son entonces desencriptados justo antes de mostrarlos al usuario. Este procedimiento mejora el rendimiento global del proceso (tanto el desencriptado como la representación), reduciendo al mínimo la sobrecarga del desencriptado (puesto que el desencriptado anterior a la representación es generalmente costoso en cuanto a tiempo y recursos) y posponiendo la desencriptación a una etapa tardía del proceso de representación.

La transformación oculta o procesamiento oculto se puede lograr de una de varias maneras. La mayoría de obras digitales incluyen información de formato, que cuando está encriptada no puede ser procesada por la aplicación de reproducción o representación (la función de transformación que transforma una obra digital en datos de presentación). Si la obra digital se encripta con un esquema de encriptado que preserva el formato, se puede usar cualquier función de transformación. Esto es particularmente útil en que cualquier aplicación comercial de reproducción o representación puede procesar la obra digital encriptada en forma de datos de presentación encriptados. De lo contrario, la función de transformación oculta es una función de la función de transformación original. Por ejemplo, la función de transformación oculta puede ser un polinomio (*polynomial*) de la función de transformación original. Alternativamente, tanto la función de transformación oculta como la función de transformación original puede ser cualquier función afín de coeficiente entero y multi-variable (*multivariate, integer coefficient affine function*).

No todos los esquemas de encriptado son esquemas de encriptado que preservan el formato. Pueden usarse esquemas de encriptado aditivo (*additive encryption schemes*) con todo tipo de documentos y todas las funciones de transformación asociadas. En algunas aplicaciones de reproducción o representación, para algunos tipos de documentos, pueden dejarse partes de la información de formato sin encriptar. En otros tipos de documentos, se puede encriptar la totalidad de la información de formato. En algunos tipos de documentos, se puede usar un esquema de encriptado aditivo para encriptar la información de formato y se puede usar cualquier esquema de encriptado para encriptar la parte de contenido o de datos del documento.

En particular, se pueden usar esquemas de encriptado aditivo para encriptar información de coordenadas de los documentos de modo que se pueden realizar algunas transformaciones de representación en los datos de coordenadas encriptados. En una clase especial de documentos, documentos basados en símbolos (*token-based*), por ejemplo, hay dos puntos durante el encriptado con preservación del formato que usan esquemas de encriptado: uno es para la información de ubicación o de coordenadas x e y de los símbolos (*tokens*) particulares dentro del documento, y el otro es para el diccionario de símbolos (*tokens*) individuales. Para llevar a cabo la transformación oculta en las coordenadas individuales de los símbolos particulares del documento, el primer esquema de encriptado debe ser un esquema de encriptado aditivo. Sin embargo, el diccionario de símbolos puede ser encriptado con cualquier sistema de encriptado.

Un diccionario de símbolos encriptado aún puede tener fugas de información tal como el tamaño de las imágenes simbólicas (*token images*). Si esto es una preocupación (por ejemplo, si el diccionario de símbolos es pequeño), los símbolos se pueden rellenar con algunos bits adicionales antes de la encriptación. El relleno puede resultar en imágenes simbólicas encriptadas de un mismo tamaño o de varios tamaños fijos. Para un documento basado en símbolos, la información de coordenadas de los símbolos del diccionario no puede ser codificada. Si se desea que la información de coordenadas sea codificada, por ejemplo, en forma de palabras de código (*codewords*) de Huffman, el mismo enfoque utilizado para encriptar los identificadores se puede utilizar para tratar esta situación. Básicamente, las palabras de código de las tablas de ubicación se dejan sin encriptar, y se hace un hash de las palabras de código del diccionario de palabras de código mediante una función hash unidireccional y se encripta su correspondiente información de coordenadas. Durante la representación, primero se hace un hash de las palabras de código de las tablas de ubicación y luego son utilizadas para buscar su información de coordenadas encriptada.

En otra forma de realización de la invención, una obra digital y un contexto de sistema (o información de recursos o recursos del sistema) son polarizados permitiendo una representación o reproducción de confianza de la obra digital sin despolarizar el contenido digital. En esta forma de realización, la obra digital es del tipo que incluye contenido digital e información de recursos. La información de recursos puede incluir información usada por una aplicación de reproducción para formatear o procesar la obra digital en forma de datos de presentación. La información de recursos puede incluir, por ejemplo, una colección de recursos del sistema disponibles para el software de reproducción en un sistema en particular, tal como la tabla de tipos de letra (*Font Table*), paleta de colores (*Color Palette*), coordenadas del sistema (*System Coordinates*) y el ajuste del volumen (*Volume Setting*).

Se pueden polarizar diferentes tipos de obras digitales. Además de la polarización de típicos documentos del tipo obras digitales, se pueden polarizar obras digitales de audio y video. La obra digital y el contexto del sistema digital son generalmente polarizados en una ubicación del propietario del contenido o del fabricante mediante un motor de polarización. Un motor de polarización es un componente utilizado para transformar la obra digital y el contexto del sistema en sus respectivas formas polarizadas. El motor de polarización utiliza un esquema de polarización que se basa en semillas de polarización (*polarization seed*), un elemento utilizado para inicializar y personalizar el motor de polarización.

Se pueden utilizar diversos esquemas de polarización para polarizar una obra digital. Por ejemplo, una polarización sin estado utiliza un número aleatorio como semilla (*seed*) para transformar una obra digital en una obra digital polarizada. Un esquema de polarización basado en estado utiliza una semilla basada en un estado del sistema o característica de un sistema para transformar una obra digital en una obra digital polarizada que está asociada con ese estado o característica del sistema. Un esquema de polarización basado en estado dinámico utiliza una semilla basada en un estado o característica dinámica del sistema para transformar una obra digital en una obra digital polarizada. En esta forma de realización, la obra digital polarizada normalmente estará provista con un motor de polarización para repolarizar la obra digital codificada y el contexto codificado del sistema de acuerdo con el esquema de polarización basada en estado dinámico cada vez que el sistema solicita la reproducción de la obra digital. Un esquema de polarización basada en autorización utiliza una semilla basada en información de autorización recibida de una fuente de confianza para transformar una obra digital en una obra digital polarizada. Para más seguridad, el contexto polarizado del sistema se puede almacenar por separado de la obra digital polarizada en un dispositivo de contexto extraíble, el cual debe ser acoplado al sistema antes del uso de la obra digital.

Preferiblemente, la semilla de polarización contiene información que puede ser usada para vincular la obra digital en particular al usuario final principal (*ultimate*) o a un sistema de usuario final principal (*ultimate*). Normalmente, el propietario o distribuidor seleccionará el tipo de esquema de polarización a usar en la polarización de la obra digital y el tipo de clave de polarización a utilizar en función del valor de la obra digital. Al igual que los esquemas de encriptado, los esquemas de polarización tienen diferentes niveles de complejidad y potencia. Cuando se solicita una obra digital, se hace una copia de una parte de la información de los recursos de la obra digital, llamada el contexto del sistema. Se selecciona la semilla de polarización y se polarizan tanto la obra digital como el contexto del sistema. Se puede utilizar un esquema de polarización para el contexto del sistema diferente del utilizado para la obra digital. Sin embargo, la semilla de polarización es la misma para ambos. La obra digital polarizada y el contexto del sistema polarizado son proporcionados a continuación al usuario para su reproducción o representación en un sistema de reproducción o de representación.

En la realización de encriptación que preserva el formato y representación de confianza de la invención, se proporciona una protección hasta que los datos encriptados de presentación deban ser desencriptados en forma de datos de presentación no encriptados (*clear presentation data*). En esta forma de realización de la invención, la aplicación de reproducción usa la información polarizada de recursos para transformar una obra digital polarizada en datos de presentación no encriptados (*clear presentation data*).

Si sólo se polariza el contenido digital de una obra digital, dejando la información de recursos sin polarizar o sin encriptar, la aplicación de reproducción será capaz de procesar la obra digital polarizada en forma de datos de presentación polarizados. Esto significa que un despolarizador debe despolarizar los datos de presentación en datos de presentación no encriptados adecuados para la visualización o el uso por parte del usuario. Si una parte de la información de recursos de una obra digital es también correspondientemente polarizada, cuando la aplicación de reproducción transforma la obra digital polarizada, la aplicación de reproducción usa la información polarizada de recursos del sistema para transformar la obra digital polarizada en datos de presentación no encriptados. Se puede polarizar toda o solo una parte de la información de recursos requerida. La reproducción es oculta en que la aplicación de reproducción no considera el contenido digital original, no polarizado.

En esta forma de realización, una obra digital polarizada es transformada por la aplicación de reproducción usando un contexto de sistema (información de recursos) polarizado para crear datos de presentación no encriptados; la aplicación de reproducción puede ser cualquier aplicación comercial o de terceros. La aplicación de reproducción no tiene que ser personalizada para despolarizar los datos de presentación y no se requiere ningún motor despolarizador. La aplicación de reproducción funciona como un sistema de reproducción oculta (que procesa contenido digital polarizado usando recursos de sistema polarizados) y se basa en un tipo de polarización que transforma o codifica la obra digital de tal manera que la capacidad de reproducirla utilizando un programa de software o dispositivo está vinculada a una información de recursos específica, protegiendo de este modo el contenido durante todo su uso.

A diferencia de los sistemas que utilizan el encriptado para proteger la obra digital y finalmente desencriptar la obra digital en su forma no encriptada (*clear form*) antes de que la obra digital sea proporcionada a la aplicación de

reproducción, el sistema de reproducción oculta mantiene la obra digital codificada en forma polarizada (no hay ninguna etapa de descodificación explícita en la respuesta oculta) hasta el último momento posible del proceso de reproducción. En el sistema de reproducción oculta, la propia obra digital polarizada nunca es despolariza en un formato no encriptado (*in the clear*). Dado que los datos de presentación suelen ser de menor calidad que la obra digital original, incluso si se capturan los datos de presentación en su forma no encriptada (*clear form*), no puede ser fácilmente (como mucho) transformada de nuevo en la obra digital original.

Muchos tipos diferentes de obras digitales y su información de recursos pueden ser polarizados y reproducidos en un sistema de reproducción oculta. Obras digitales como documentos, texto, archivos de audio, archivos gráficos y archivos de vídeo pueden ser reproducidos en el sistema de reproducción oculta de la invención por medio de la polarización de una información de recursos adecuada.

Breve descripción de los dibujos

La estructura y función de la invención se entienden mejor con referencia a los dibujos incluidos, que pueden ser descritos de la siguiente manera:

La Figura 1 es un diagrama de bloques de alto nivel que representa un modelo para la creación y distribución comercial de documentos electrónicos tanto en entornos seguros como inseguros;
La Figura 2 es un diagrama de flujo que ilustra la desencriptación de documentos electrónicos protegidos según la técnica;
La Figura 3 es un diagrama de flujo que ilustra la desencriptación de documentos electrónicos protegidos según una realización sencilla de la invención;
La Figura 4 es un diagrama de flujo que ilustra la desencriptación de documentos electrónicos protegidos según una realización preferida de la invención;
La figura 5 es un diagrama de bloques funcional que ilustra las estructuras de datos presentes en un documento con auto-protección según una realización de la invención;
La figura 6 es un diagrama de flujo que ilustra la creación y personalización de un documento con auto-protección según una realización de la invención;
La figura 7 es un diagrama de flujo, desde la perspectiva de un usuario, que ilustra las acciones realizadas en el manejo y el uso de un documento con auto-protección de acuerdo con la invención;
La Figura 8 es un gráfico que ilustra varios caminos posibles entre un documento no representado (*unrendered*) y encriptado, y los datos de presentación representados y desencriptados;
La Figura 9 es un diagrama de flujo que ilustra un proceso de polarización según la invención en el que la información de formato del documento permanece en su forma no encriptada (*in the clear*) para su representación;
La figura 10 es un diagrama de bloques de un procedimiento de encriptación que preserva el formato y representación de confianza de acuerdo con la invención;
La figura 11 es un ejemplo simple de un documento a ser dotado de símbolos (*to be tokenized*);
La figura 12 es el diccionario de símbolos para el documento de la figura 11;
La figura 13 es la tabla de ubicación para el documento de la figura 11;
La figura 14 es un diagrama de bloques que ilustra un proceso para generar una obra digital polarizada y recursos del sistema polarizados de acuerdo con la invención;
La figura 15 es un diagrama de bloques que ilustra la conversión de una obra digital en datos de imagen según la técnica;
La Figura 16 es un diagrama de bloques que ilustra un sistema para la reproducción oculta de una obra digital polarizada según la invención;
La figura 17 es un diagrama de bloques que ilustra otro sistema de reproducción oculta de una obra digital polarizada según la invención;
La figura 18 es un diagrama de bloques de un ejemplo de estructura de un documento digital;
La figura 19 es un documento digital de ejemplo;
La figura 20 es un ejemplo del documento digital de la figura 16 después de haber sido polarizado;
La figura 21 es un diagrama de bloques de un ejemplo de estructura de información de recursos o contexto del sistema para un documento digital;
La figura 22 es un diagrama de bloques de una tabla de ejemplo de tipos de letra; y
La figura 23 es un diagrama de bloques de la tabla de tipos de letra de la figura 22 después de haber sido polarizada.

Descripción detallada de las realizaciones preferidas

A continuación se describe la invención, con referencia a realizaciones ilustrativas detalladas. Será evidente que la invención puede ser realizada de una amplia variedad de maneras, algunas de las cuales pueden ser bastante

diferentes de las de las realizaciones divulgadas. En consecuencia, los detalles estructurales y funcionales específicos descritos en este documento son meramente representativos y no limitan el alcance de la invención.

La figura 1 representa un modelo funcional de alto nivel de un sistema para la distribución electrónica de documentos, que como se ha definido anteriormente, pueden incluir correspondencia, libros, revistas, diarios, periódicos, otros documentos, software, y clips de audio y video, y otras presentaciones multimedia.

Un autor (o editor) 110 crea el contenido original de un documento 112 y lo pasa a un distribuidor 114 para que lo distribuya. Aunque se contempla que el autor también pueda distribuir documentos directamente, sin implicar a otra parte como distribuidor, la división del trabajo expuesta en la figura 1 es más eficiente, ya que permite al autor/editor 110 concentrarse en la creación del contenido, y no en las funciones mecánicas y mundanas que asume el distribuidor 114. Por otra parte, este desglose permitiría que el distribuidor 114 consiga economías de escala asociándose con una serie de autores y editores (incluyendo el autor/editor ilustrado 110).

El distribuidor 114 entonces pasa el contenido modificado 116 a un usuario 118. En un modelo típico de distribución electrónica, el contenido modificado 116 representa una versión encriptada del contenido original 112; el distribuidor 114 encripta el contenido original 112 con la clave pública del usuario 118, y el contenido modificado 116 es personalizado solamente para el único usuario 118. El usuario 118 entonces es capaz de utilizar su clave privada para desencriptar el contenido modificado 116 y ver el contenido original 112.

Se pasa un pago 120 por el contenido 112 del usuario 118 al distribuidor 114 por medio de una cámara de compensación (*clearinghouse*) 122. La cámara de compensación 122 recoge las peticiones del usuario 118 y de otros usuarios que deseen ver un documento en particular. La cámara de compensación 122 recoge además información de pago, tales como transacciones de débito, transacciones de tarjetas de crédito, u otros esquemas de pago electrónico conocidos, y envía los pagos de los usuarios recogidos como un lote de pagos 124 al distribuidor 114. Por supuesto, se espera que la cámara de compensación 122 se quede con una parte del pago del usuario 120. A su vez, el distribuidor 114 se queda con una parte del lote de pagos 124 y envía un pago 126 (incluyendo royalties) al autor y editor 110. En una realización de este esquema, el distribuidor 114 espera un paquete de peticiones de usuario para un único documento antes de enviar nada. Cuando se hace esto, se puede generar un único documento con contenido modificado 116 para su desencriptación por parte de todos los usuarios solicitantes. Este método es bien conocido en la técnica.

Mientras tanto, cada vez que el usuario 118 pide (o usa) un documento, se envía un mensaje de contabilización 128 a un servidor de auditoría 130. El servidor de auditoría 130 garantiza que cada solicitud por parte del usuario 118 está vinculada con un documento enviado por el distribuidor 114; el servidor de auditoría 130 recibe información de contabilización 131 directamente del distribuidor 114. Las inconsistencias son transmitidas a través de un informe 132 a la cámara de compensación 122, la cual puede entonces ajustar los lotes de pago 124 hechos al distribuidor 114. Este esquema de contabilización está presente con el fin de reducir la posibilidad de fraude en este modelo de distribución de documentos electrónicos, así como para manejar cualesquiera permisos de uso dependientes del tiempo que pueden dar lugar a cargos que varían, dependiendo de la duración u otra extensión de uso.

El modelo anterior para comercio electrónico de documentos, que se muestra en la figura 1, es de uso común hoy en día. Como se mostrará en detalle más abajo, es igualmente aplicable al sistema y procedimiento expuesto en este documento para la distribución de documentos con auto-protección.

En referencia ahora a la figura 2, se muestran las etapas realizadas por el usuario 118 (figura 1) en un sistema de la técnica anterior para la distribución de documentos electrónicos. Como se comentó anteriormente, los mecanismos criptográficos se utilizan típicamente para encriptar documentos. Esos documentos encriptados son luego distribuidos y almacenados públicamente y desencriptados en privado por parte de usuarios autorizados. Esto proporciona una forma básica de protección durante la entrega de documentos por parte de un distribuidor de documentos a un usuario previsto a través de una red pública, así como durante el almacenamiento de documentos en un medio inseguro.

Al comienzo, un documento encriptado 210 es recibido por el usuario 118 y es pasado a una etapa de desencriptación 212. Como es bien conocido en la técnica, la etapa de desencriptación 212 recibe la clave privada del usuario 118, la cual se almacena localmente en el ordenador del usuario o es introducida por el usuario cuando es necesario. El documento 210 es desencriptado, dando como resultado un contenido no encriptado (*clear content*) 216 similar o idéntico al contenido original 112 (figura 1).

El contenido no encriptado 216 es pasado a una aplicación de representación 218, que construye unos datos de presentación 220, o una versión utilizable del contenido original del documento 112. En los sistemas típicos de este tipo, los datos de presentación 220 son datos inmediatamente adecuados para su visualización en una pantalla de vídeo, su impresión en papel, o para otros usos en función del tipo de documento.

Como se mencionó anteriormente, el documento es vulnerable en sistemas como este. El contenido no encriptado 216 puede ser copiado, almacenado o enviado a otros usuarios sin el conocimiento o consentimiento del distribuidor 114 o del autor/editor 110. Incluso un usuario legítimo puede tener la tentación de minimizar los honorarios de licencia mediante la captura del documento en un formato no encriptado (*in the clear*) con el fin de redistribuirlo y utilizarlo a su antojo, sin pagar por la propiedad intelectual de los propietarios del contenido. Como se comentó anteriormente, la presente invención está dirigida a un esquema para impedir que dicho usuario obtenga un formato usable del documento durante el proceso de representación en el sistema del usuario.

Por consiguiente, el sistema y procedimiento de la presente invención expone un esquema alternativo para manejar documentos encriptados en el sistema del usuario 118. Se ilustra una forma de realización sencilla de este esquema en la figura 3.

La figura 3 es similar a la figura 2, en que se pasa un documento encriptado 310 a una etapa de desencriptación 312 (que usa una clave privada 314) y una aplicación de representación 316, que dan lugar a datos de presentación 318. Sin embargo, se proporciona una capa adicional de protección por medio de una estructura (*shell*) de protección 320. La estructura de protección 320 permite que el documento 310 sea desencriptado y representado sin dejar nunca contenido no encriptado (como el contenido no encriptado 216 de la figura 2) disponible para ser interceptado. Esto se logra mediante la inclusión de elementos de desencriptación y representación dentro del documento 310, según se describirá más abajo con referencia a la figura 5. Los elementos de representación y desencriptación incluidos están adaptados para limitar la interacción del usuario con el SPD, prohibiendo determinadas operaciones (por ejemplo, operaciones de guardado del documento o de realización de operaciones de cortar y pegar) de acuerdo con los permisos del usuario.

La figura 4 es una versión más sofisticada. El esquema de la figura 4 incluye una etapa intermedia de "polarización" adaptada para asegurar el documento después de haber sido desencriptado pero antes de su representación. En primer lugar, se pasa el contenido del documento encriptado 410 a un polarizador 412. El polarizador 412 recibe la clave privada del usuario 414 y, a través de una etapa de desencriptación 416, desencripta el contenido del documento 410. Al mismo tiempo, el polarizador 412 recibe una clave de polarización 418 desde el sistema del usuario.

Esta clave de polarización 418 es utilizada por el polarizador 412 para transformar el documento en una versión que tiene contenidos polarizados 420. Todas estas operaciones pueden llevarse a cabo en abierto (*in the open*), sin ningún tipo de mecanismo de protección, siempre que el polarizador 412 no almacene una versión no encriptada (*clear version*) del documento entre su desencriptación y su polarización.

En una forma de realización de la invención, la clave de polarización 418 representa una combinación de elementos de datos obtenidos del estado interno del sistema del usuario, tales como la fecha y la hora del día, el tiempo transcurrido desde la última pulsación de tecla, la velocidad del procesador y el número de serie, y cualquier otra información del sistema del usuario que pueda ser derivada de forma repetible. Es de utilidad incluir alguna información derivada del tiempo en la clave de polarización 418 de manera que la interceptación e incautación (*seizure*) de contenidos polarizados 420 no serían de utilidad. Nuevas representaciones del documento polarizado no serían posibles, dado que la hora del sistema habría cambiado demasiado.

A continuación, de nuevo dentro de una estructura (*shell*) de protección 422, se pasan los contenidos polarizados 420 a una aplicación de representación 424. Como se mencionó anteriormente, las aplicaciones típicas de representación son aplicaciones de terceros tales como *Microsoft Word* o *Adobe Acrobat Reader*. Sin embargo, es probable que dichas aplicaciones de representación externas no sean capaces de procesar los contenidos polarizados 420, puesto que los contenidos, los códigos de formateo (*formatting codes*), y otras referencias (*cues*) usadas por el representador habrán sido codificadas (*scrambled*) en el proceso de polarización.

Por lo tanto, la aplicación de representación 424 debe ser conmutativa (o al menos tolerante a fallos), o debe recibir contenidos polarizados 420 que son en gran medida completos y procesables por la aplicación. Más abajo se comentará la última posibilidad, en relación con la figura 9.

El output de la aplicación de representación son datos de presentación polarizados 426, que han sido formateados por la aplicación de representación 424 pero que aún siguen polarizados, y por lo tanto no son legibles por el usuario. Los datos de presentación polarizados 426 son pasados a un despolarizador 428, que recibe la clave de polarización 418 y restaura la forma original del documento en forma de datos de presentación 430. En una forma de realización de la invención, se combina la función de despolarización con la función de representación o de visualización. En este caso, los datos de presentación polarizados 426 son recibidos directamente por un dispositivo de visualización, que puede ser independiente del sistema del usuario y recibir datos a través de un canal de comunicaciones.

La creación de la clave de polarización 418, la aplicación de representación 418, y la etapa de despolarización 428 son todos ellos elementos de la estructura de protección 422; éstos son elementos de programa resistentes a la manipulación (*tamper-resistant*). Se contempla que todas las etapas de cálculo (o transformación) que se producen dentro de la estructura de protección 422 sólo utilizarán datos locales, y no almacenarán datos temporales en cualquier medio de almacenamiento o zona de memoria accesible globalmente; solamente se exportarán de la estructura de protección 422 los resultados explícitos. Este enfoque evitará que los usuarios modifiquen fácilmente los puntos de entrada del sistema operativo o recojan información residual (*scavenging*) de los recursos del sistema con el fin de interceptar y utilizar datos intermedios.

Cabe señalar que los datos de presentación 430 de la figura 4, en realizaciones alternativas de la invención, pueden ser independientes del dispositivo o dependientes del dispositivo. En el caso de que sean independientes del dispositivo, será necesario un procesamiento adicional por parte de un controlador (*driver*) del dispositivo (tal como un controlador de pantalla o un controlador de impresora) para completar el proceso de representación. En el caso actualmente preferido de que sean dependientes del dispositivo, ya se han realizado las modificaciones específicas del dispositivo en los datos de presentación (ya sea en la aplicación de representación 424 o en la etapa de despolarización 428), y los datos de presentación 430 pueden ser enviados directamente al dispositivo de output deseado.

Los esquemas de desencriptación descritos anteriormente con referencia a las figuras 3 y 4 son habilitados por una única estructura de documento, que se muestra en detalle en la figura 5. Como se comentó anteriormente, determinadas operaciones realizadas por el sistema y procedimiento de la invención requieren componentes de confianza. Una forma de asegurar que se va a utilizar determinado código no modificado para realizar los aspectos de confianza de la invención es proporcionar el código junto con los documentos. Los diversos componentes de un documento con auto-protección de acuerdo con la invención se ilustran en la Figura 5.

El problema de la protección de documentos es abordado por la invención sin ninguna suposición sobre la presencia de unidades hardware o módulos software de confianza en el sistema del usuario. Esto se logra mediante la mejora de un documento para que sea un objeto meta-documento activo (*active meta-document object*). Los propietarios del contenido (es decir, los autores o editores) adjuntan derechos a un documento que especifican los tipos de usos, las autorizaciones necesarias y los honorarios asociados, y un módulo de software que hace cumplir los permisos concedidos al usuario. Esta combinación del documento, los derechos asociados, y los módulos de software adjuntos que hacen cumplir los derechos es el documento con auto-protección ("SPD") de la invención. Un documento con auto-protección impide el uso y la distribución del documento sin autorización y sin control, protegiendo así los derechos de los propietarios del contenido.

El documento con auto-protección 510 incluye tres segmentos funcionales principales: un segmento de código ejecutable 512 contiene determinadas porciones de código ejecutable necesarias para permitir al usuario utilizar el documento encriptado; un segmento de derechos y permisos 514 contiene estructuras de datos representativas de los diversos niveles de acceso que se van a permitir a los diversos usuarios; y un segmento de contenido 516 incluye el contenido encriptado 116 (figura 1) que se pretende que sea visto por el usuario.

En una realización preferida de la invención, el segmento de contenido 516 del SPD 510 incluye tres subsecciones: meta-información del documento 518 (que incluye pero no está limitada al título, formato y fecha de revisión del documento), información de etiqueta de derechos 520 (tal como un aviso de los derechos de autor adjunto al texto, así como información sobre derechos y permisos), y el contenido protegido 520 (el propio documento encriptado).

En una realización de la invención, el segmento de derechos y permisos 514 incluye información sobre los derechos específicos de cada usuario autorizado. Se puede adjuntar una lista de términos y condiciones a cada derecho de uso. Por ejemplo, al usuario *John Doe* se le puede dar el derecho de ver un documento en particular y de imprimirlo en dos ocasiones, con un coste de 10 dólares. En este caso, el segmento de derechos y permisos 514 identifica a *John Doe*, le asocia dos derechos (un derecho de visualización y un derecho de impresión), y especifica los términos y condiciones, incluyendo el precio (10 dólares) y una limitación en cuanto a la impresión (dos veces). El segmento de derechos y permisos 514 también puede incluir información de otros usuarios.

En una realización alternativa, el segmento de derechos y permisos 514 sólo incluye un enlace a información externa que especifica información sobre derechos. En tal caso, los derechos y permisos reales se almacenan en otro lugar, por ejemplo en un servidor de permisos en red, que debe ser consultado cada vez que se va a utilizar el documento. Este enfoque ofrece la ventaja de que los derechos y permisos puedan ser actualizados dinámicamente por los propietarios del contenido. Por ejemplo, se puede incrementar el precio de una visualización, o se pueden finalizar los derechos de un usuario si se ha detectado un uso no autorizado.

En cualquiera de los casos, el segmento de derechos y permisos 514 es firmado criptográficamente (por procedimientos conocidos en la técnica) para evitar la alteración de los derechos y permisos específicos; también se puede encriptar para evitar que el usuario pueda ver directamente los derechos y permisos de sí mismo y de otros.

El segmento de código ejecutable 512, también llamado el "Control del SPD," también contiene varias subsecciones, cada una de las cuales comprende un módulo de software al menos parcialmente dentro del segmento de código ejecutable. En una forma de realización de la invención, se utiliza el lenguaje de programación Java para el Control del SPD; sin embargo, se contempla que pueda usarse cualquier lenguaje independiente de la plataforma o específico de plataforma, ya sea interpretado o compilado, en una implementación de la presente invención.

Un ejecutor de derechos (*rights enforcer*) 524 está presente para verificar la identidad del usuario, para comparar una acción solicitada por el usuario con aquellas acciones enumeradas en el segmento de derechos y permisos 514, y para permitir o denegar la acción solicitada en función de los derechos especificados. El funcionamiento del ejecutor de derechos 524 se comentará en mayor detalle más adelante, en relación con la figura 7.

Un motor de polarización protegido 526 también está presente dentro del segmento de código ejecutable 512; éste sirve para leer y polarizar los datos según el estado del sistema (u otra clave de polarización) como se comentó anteriormente. En una forma de realización preferida de la invención, el motor de polarización 526 actúa sobre el documento antes de que sea almacenado o desencriptado, con lo que el documento nunca es almacenado en un formato no encriptado (*in the clear*) en el sistema del usuario. El motor de polarización 526 está protegido, es decir, está firmado criptográficamente y encriptado, para evitar la manipulación, ingeniería inversa, y descomposición (*disassembling*).

También se incluye un motor de despolarización equivalente (*counterpart depolarization engine*) 528 para permitir la generación de datos de presentación no encriptados a partir del contenido polarizado (véase la figura 4). El motor de despolarización incluye un conjunto de objetos de ventana segura, que proporciona una interfaz relativamente a prueba de manipulación a la API (interfaz de programa de aplicación) de representación del sistema del usuario. Los objetos de ventana segura son resistentes a la interceptación, reduciendo de este modo la posibilidad de que el documento, en su forma no encriptada, pueda ser reconstruido mediante su interceptación y recepción de datos destinados al sistema operativo.

También se incluye un motor de despolarización equivalente 528 para permitir la generación de datos de presentación no encriptados a partir del contenido polarizado (véase la figura 4). El motor de despolarización 528 proporciona una interfaz relativamente a prueba de manipulación al dispositivo lógico o físico de salida (por ejemplo, el dispositivo de visualización del usuario). El input al motor de despolarización 528 son datos de presentación polarizados. Por lo tanto, si esos datos son interceptados, no revelarán ninguno de los contenidos no encriptados sin una despolarización adicional que depende de, por ejemplo, el estado del sistema del usuario.

Se incluye opcionalmente un visor seguro 530 en el segmento de código ejecutable 512. El visor seguro 530 se utiliza para permitir sólo aquellos niveles de acceso que están permitidos de acuerdo con el segmento de derechos y permisos 514. Por ejemplo, si el usuario sólo compró los derechos suficientes para ver el documento (y no guardarlo o imprimirlo), el visor no permitirá al usuario guardar, imprimir, o realizar las operaciones estándar de cortar y pegar que son posibles en los sistemas operativos más modernos.

Finalmente, se incluye o se hace referencia a un motor de representación (*rendering engine*) 532 dentro del segmento de código ejecutable 512. El motor de representación 532 no necesita ser seguro. Por consiguiente, el código para el motor de representación 532 se puede incluir dentro de la mini-aplicación (*applet*) del SPD, o alternativamente recuperarlo (mediante un enlace seguro) de alguna otra ubicación. En cualquiera de los casos, el motor de representación 532 está adaptado para recibir contenidos polarizados del documento y datos de presentación polarizados producidos a partir de los mismos (véase la figura 4).

Los aspectos y elementos anteriores del documento con auto-protección 510 serán comentados en más detalle más abajo, junto con el funcionamiento del sistema.

La figura 6 muestra las etapas realizadas cuando se crea y distribuye un documento con auto-protección 510. Un SPD genérico 610 no incluye ninguna información sobre derechos específicos del usuario y no está encriptado para cualquier usuario particular. El SPD genérico 610 se crea a partir de tres elementos: el contenido del documento original 612, en un formato sin encriptar; una especificación de derechos de alto nivel 614; y una marca (*watermark*) opcional 616.

El contenido 612 es pre-procesado (etapa 618) para diseñar el documento según desee el autor o el editor. Por ejemplo, se puede seleccionar un tamaño de página preferido, el tipo de letra, y el diseño de página. El contenido 612 es esencialmente "pre-representado" en la etapa de pre-procesamiento del contenido de modo que estará en un formato que es compatible con los sistemas de los usuarios y el SPD. Por ejemplo, el contenido 612 se puede convertir de Microsoft Word (".DOC") o formato de Adobe Acrobat (".PDF") a un formato diferente adaptado especialmente para ser leído por el motor de representación 532 (figura 5). En una forma de realización de la invención, se generan múltiples versiones del contenido 612 por parte de la etapa de pre-procesamiento del

contenido y se almacenan en el SPD genérico 610; esas versiones diferentes pueden entonces ser compradas por separado por el usuario según sus necesidades.

La especificación de derechos de alto nivel 614 establece qué combinaciones de derechos de acceso son permisibles. Esta especificación de los derechos está adapta a un determinado documento, y es capaz de describir diferentes grupos de derechos para diferentes clases de usuarios de descarga (*downstream users*). Por ejemplo, un editor puede tener el derecho de distribuir hasta 100.000 copias de un documento con un royalty de un 1 dólar por copia, y con un royalty de 2 dólares para copias adicionales. De modo similar, los usuarios pueden tener la opción de comprar una versión del documento que "caduca" después de un mes, un año, o nunca. Se describen varias limitaciones posibles con referencia a un ejemplo detallado, que se expone a continuación.

El Lenguaje de Derechos de la Propiedad Digital (DPRL - *Digital Property Rights Language*) es un lenguaje que se puede utilizar para especificar los derechos de las obras digitales. Proporciona un mecanismo en el que se pueden especificar los diferentes términos y condiciones y hacer cumplir los derechos. Las especificaciones de los derechos son representados como sentencias en el DPRL. Para más detalles, véase, por ejemplo, la patente de EE.UU. Nº 5.715.403 de *Stefik*, titulada "*System for Controlling the Distribution and Use of Digital Works Having Attached Usage Rights Where the Usage Rights are Defined by a Usage Rights Grammar.*" El cumplimiento de los derechos y la verificación de las condiciones asociadas a los derechos se realizan utilizando la tecnología SPD.

Los diferentes derechos se pueden especificar para las diferentes partes de una obra digital utilizando una especificación de "obra". Dentro de una especificación de obra, se especifican diferentes conjuntos de derechos aplicables a esta obra. Los derechos pueden ser agrupados en unos grupos denominados "grupos de derechos". Cada derecho dentro de un grupo de derechos está asociado con un conjunto de condiciones. Las condiciones pueden ser de diferentes tipos: honorarios a pagar, tiempo de uso, tipo de acceso, tipo de marca (*watermark*), tipo de dispositivo en el que se puede realizar la operación, etcétera. El DPRL permite diferentes categorías de derechos: derechos de representación, transferencia, derechos de obra derivados (*derivative work rights*), derechos de gestión de archivos y derechos de configuración. Los derechos de transporte gobiernan el movimiento de una obra de un repositorio a otro. Los derechos de representación gobiernan la impresión y la visualización de una obra, o más en general, la transmisión de una obra mediante un transductor (*transducer*) a un medio externo (esto incluye el derecho de "exportación", que se puede utilizar para hacer copias en formato no encriptado (*in the clear*)). Los derechos de obra derivados gobiernan la reutilización de una obra en la creación de nuevas obras. Los derechos de gestión de archivos gobiernan la realización y restauración de copias de seguridad. Finalmente, los derechos de configuración se refieren a la instalación de software en los repositorios.

A continuación se expone una especificación de obra ejemplar en DPRL:

```
(Work:
(Rights-Language-Version: 1.02)
(Work-ID: "ISDN-1-55860-166-X; AAP-2348957tut")
(Description: "Title: 'Zuke-Zack, the Moby Dog Story'
    Author: 'John Beagle'
    Copyright 1994 Jones Publishing")
(Owner: (Certificate:
    (Authority: "Library of Congress")
    (ID: "Murphy Publishers")))
(Parts: "Photo-Celebshots-Dogs-23487gfj" "Dog-Breeds-Chart-AKC")
(Comment: "Rights edited by Pete Jones, June 1996.")
(Contents: (From: 1) (To: 16636))
(Rights-Group: "Regular"
(Comment: "This set of rights is used for standard retail editions.")
(Bundle:
(Time: (Until: 1998/01/01 0:01))
    (Fee: (To: "Jones-PBLSH-18546789")(House: "Visa")))
(Play:
    (Fee: (Metered: (Rate: 1.00 USD) (Per: 1:0:0) (By: 0:0:1))))
(Print:
    (Fee: (Per-Use: 10.00 USD))
    (Printer:
        (Certificate:
            (Authority: "DPT"
            (Type: "TrustedPrinter-6")))
    (Watermark:
        (Watermark-Str: "Title: 'Zeke Zack - the Moby Dog' Copyright
        1994 by Zeke Jones. All Rights Reserved.")
```

```
        (Watermark-Tokens: user-id institution-location render-name
        render-time))))
    (Transfer: )
    (Copy: (Fee: (Per-Use: 10.00 USD)))
    (Copy: (Access:
        (User: (Certificate:
            (Authority: "Murphy Publishers")
            (Type: "Distributor")))))
    (Delete:)
    (Backup:)
    (Restore: (Fee: (Per-Use: 5.00 USD)))))
```

Esta especificación de obra tiene un grupo de derechos llamado "Regular", que especifica los derechos para ediciones comerciales estándar de un libro titulado "Zuke-Zack, the Moby Dog Story." La especificación de obra expresa las condiciones para varios derechos: reproducción, impresión, transferencia, copia, borrado, copia de seguridad y restauración. La obra incluye en el ejemplo otras dos partes, una fotografía y un gráfico de razas incorporados desde otras fuentes. Una especificación de "paquete" empaqueta un conjunto de condiciones comunes que se aplican a todos los derechos del grupo. Esta especificación establece que todos los derechos sobre el grupo son válidos hasta el 1 de enero de 1998 y que los honorarios deben pagarse a la cuenta "Jones-PBLSH-18546789". La cámara de compensación de esta transacción debe ser Visa. El siguiente contrato aplica que: la obra se puede reproducir mediante el pago de 1 dólar cada hora, en que los honorarios se acumulan por segundo; la obra se puede imprimir en *TrustedPrinter-6* que está certificada por el "DPT" por un precio de 10,00 dólares por impresión; la copia impresa debe tener una cadena de marcaje (*watermark string*) (según se muestra) y una lista de símbolos (*tokens*) que indican una información de "huella digital" ("*fingerprint*") conocida en el momento de su impresión; esta obra puede ser copiada o bien mediante el pago de 10,00 dólares o mediante la adquisición de un certificado de distribuidor de la editorial *Murphy*; y se permite la transferencia, borrado o realización de copias de seguridad de esta obra sin restricciones (gastos de restauración 5,00 dólares).

La especificación de derechos de alto nivel 614 también está sujeta a una etapa de pre-procesamiento (etapa 620), en la que la especificación de alto nivel (es decir, legible por un humano) es recopilada en una representación de estructura de datos más eficiente para su uso por la invención.

El SPD genérico 610 entonces es creado (etapa 622) combinando el contenido pre-procesado 612, la especificación de los derechos pre-procesados 614, y la marca (*watermark*) 616. Una marca (*watermark*) se puede añadir por medio de cualquier medio conocido en la técnica; ésta puede ser visible u oculta dentro del SPD. El SPD genérico 610 puede también ser encriptado opcionalmente por el autor/editor 110 para su transmisión al distribuidor 114 (figura 1).

El SPD genérico 610 entonces es recibido por el distribuidor 114, y es almacenado para su posterior personalización. Cuando una petición de usuario 624 es recibida por el distribuidor 114 (ya sea directamente o a través de la cámara de compensación 122 u otro intermediario), el distribuidor 114 crea un conjunto de permisos de usuario (etapa 626) que es consistente tanto con la petición de usuario 624 como con la especificación de derechos 614. Si no hay tal grupo consistente de permisos, entonces no se realiza ninguna otra acción en nombre de dicho usuario (excepto un mensaje opcional de notificación al usuario).

Los permisos del usuario y la clave pública del usuario 628 se utilizan entonces para generar (etapa 630) un SPD personalizado 632 adaptado para ser utilizado por el usuario. Los permisos del usuario procedentes de la etapa 626 se almacenan en el segmento de derechos y permisos 514 del SPD 632, y la clave pública del usuario 628 se utiliza para encriptar el contenido en el segmento de contenido 516 del SPD 632. Se puede utilizar un mecanismo de encriptación de clave pública para transformar el SPD de la forma genérica al SPD personalizado 632. Este mecanismo es útil si el SPD tiene que ser transferido de forma confidencial entre diferentes partes, por ejemplo, del autor al editor al minorista al consumidor, con protección de los derechos en cada etapa. Además, debe tenerse en cuenta que se pueden componer y alojar múltiples peticiones de usuario dentro de un único SPD 632; hay técnicas conocidas en la técnica que son capaces de usar múltiples claves públicas para encriptar un documento de tal manera que cualquiera de las claves privadas de los usuarios se pueden utilizar para desencriptarlo.

El SPD personalizado resultante 632 se transmite después al usuario 118 a través de cualquier medio disponible, tal como a través de una red informática o es almacenado en un medio físico (tal como un disco magnético u óptico).

Las operaciones realizadas cuando un usuario recibe un SPD están ilustradas en el diagrama de flujo de la figura 7. El SPD primero es recibido y almacenado en el sistema del usuario (etapa 710); en muchos casos, no es necesario utilizar el SPD de inmediato. Cuando se desea su uso, primero el usuario es autenticado (etapa 712), típicamente con un nombre de usuario y una contraseña o clave. Entonces el sistema determina qué acción es la deseada por el usuario (etapa 714). Cuando se elige una acción, la etapa de aplicación de los derechos de la invención (etapa 716)

verifica las condiciones asociadas con la acción deseada (tales como honorarios, tiempo, nivel de acceso, marca, u otras condiciones); esto puede realizarse a nivel local a través del *applet* del SPD 512 (figura 5) o accediendo a un servidor de aplicación de derechos.

Si la etapa de aplicación de derechos (etapa 716) falla, se lleva a cabo un procedimiento de actualización (etapa 718). El usuario puede elegir actualizar sus permisos, por ejemplo autorizando honorarios adicionales. Después de la verificación satisfactoria de las condiciones, se realiza un procedimiento de pre-auditoría (etapa 718), en el que el sistema SPD registra el estado de la verificación en un servicio de seguimiento (*tracking service*) (por ejemplo, el servidor de auditoría 130 de la figura 1). El contenido es entonces representado con seguridad en la pantalla (etapa 722) según se comentó anteriormente. Cuando el usuario ha terminado, se realiza un procedimiento de post-auditoría (etapa 724) en el que se actualiza la cantidad de uso mediante el servicio de seguimiento. El sistema SPD espera entonces nuevas acciones.

La protección proporcionada por el SPD se deriva de la incapacidad por parte del usuario de capturar un formato útil del documento en cualquier etapa intermedia durante el proceso de representación. Esto se logra mediante el desencriptado del contenido del documento a un formato no encriptado (*a clear form*) en la última etapa que sea posible, idealmente en la última etapa.

El modelo de desencriptación SPD se ilustra en la figura 8. E indica la función de encriptación realizada por el editor; D indica el desencriptado realizado en el sistema del usuario, y R indica la transformación de representación. Muchos sistemas de la técnica anterior usan una primera secuencia de transformaciones 810, $D(E(x))$ seguida de $R\left(D(E(x))\right)$. Como se comentó anteriormente, las primeras desencriptaciones dejan el documento en un estado vulnerable. Idealmente, las transformaciones se realizan en el orden inverso 812, $R'\left(E(x)\right)$ seguida de $D\left(R'\left(E(x)\right)\right)$. Esto pospone el desencriptado al último momento posible.

La existencia de R', una operación de representación que se puede realizar antes del desencriptado, es determinada por la siguiente igualdad:

$$D\left(R'\left(E(x)\right)\right) = R\left(D(E(x))\right)$$

En caso de que las funciones de encriptado y desencriptado sean conmutativas, es decir, $E(D(x)) = D(E(x))$ para cualquier x, se asegura la existencia de R':

$$R'(y) = E\left(R\left(D(y)\right)\right) \text{ para } y = E(x)$$

En la práctica, las funciones de encriptado y desencriptado en los sistemas criptográficos de clave pública populares tales como el sistema RSA y el sistema de logaritmo discreto *ElGamal* satisfacen el requisito de conmutación. Esto significa que la transformación R' existe si estos sistemas criptográficos se utilizan para encriptación y desencriptación.

La ruta $x' = D\left(R'\left(E(x)\right)\right)$ representa una solución SPD ideal para la protección de documentos contra el uso y la distribución no autorizados del documento. Un escenario de distribución y uso de un documento se puede describir de la siguiente manera. Cuando un usuario compra el documento, el documento es encriptado usando la información pública de un usuario y es transmitido por un canal de red inseguro tal como Internet. El documento encriptado tiene adjunta la información sobre los derechos y un *applet* de protección 512 que hace cumplir los derechos y permisos concedidos al usuario por el propietario del contenido. Ante una petición de usuario sobre el uso del documento, el *applet* verifica los derechos y permisos y genera a partir del documento encriptado el formato de presentación del documento original. Puesto que cualquier forma intermedia del documento anterior a los datos finales de presentación está encriptada junto con la información privada del usuario, el modelo SPD de protección de documentos garantiza que cualquier forma intermedia del documento no es útil para otros sistemas donde sea que fuese interceptado.

Claramente, este modelo ideal se basa en si la transformación R' que corresponde a la transformación de representación R se puede calcular o no de manera eficiente, y en particular en si es necesaria o no una invocación de la función de desencriptación D durante una implementación de R'. Un caso trivial en el que R' puede ser implementada de manera eficiente es aquella en la que R es conmutativa con la función de encriptación E. Cuando esto sucede,

$$R'(y) = E\left(R\left(D(y)\right)\right) = R\left(E\left(D(y)\right)\right) = R(y)$$

para $y = E(x)$. En este caso, $R' = R$.

La consideración de la figura 8 revela que pueden existir muchas soluciones intermedias (por ejemplo, las soluciones intermedias 814, 816, y 818) al problema de la protección de documentos, en el sistema del usuario entre los dos extremos $x' = R\left(D\left(E(x)\right)\right)$, que no tiene protección en $x = D\left(E(x)\right)$, y $x' = D\left(R'\left(E(x)\right)\right)$, que tiene protección ideal (bajo los supuestos expuestos anteriormente). Como se muestra en la figura 8, se pueden considerar diferentes rutas desde el documento encriptado $E(x)$ hasta los datos de presentación x' que corresponden a diferentes combinaciones de transformaciones parciales de representación y transformaciones parciales de desencriptación. Una vez más, se debe reconocer que el retraso de la desencriptación D en cualquier ruta aumenta el nivel de protección del documento.

Como se mencionó anteriormente, un procedimiento alternativo de retrasar el desencriptado hasta el último momento posible utiliza una técnica de polarización que encripta sólo los contenidos del documento, no el formato o todo el documento en conjunto. Esta posibilidad se muestra en la figura 9. Comenzando con el contenido no encriptado del documento 910 (que, cabe señalar, no existe en ninguna sola ubicación identificable durante el procesamiento del usuario, sino que es más bien un estado transitorio que ocurre dentro de la etapa 412 de la figura 4), el documento es dividido (etapa 912) en una porción de datos 914 y una porción de formato 916. La porción de datos 914 es polarizada (etapa 918), utilizando la clave de polarización 920 y fusionada (etapa 922) con la porción de formato no encriptada 916. Esto produce el contenido polarizado 924 que puede ser representado en forma de datos de presentación polarizados sin desencriptar primero el contenido. Se debe observar que esta forma de polarización es probablemente menos segura que el encriptado total con la clave de polarización, puesto que potencialmente puede derivarse una gran cantidad de información a partir del diseño (*layout*) de un documento, longitudes de palabra, longitudes de línea, etc.; sin embargo, este esquema presentará un elemento disuasorio de utilidad en cuanto a la infracción casual de derechos de autor.

Se muestra con referencia a la figura 10 un procedimiento de proteger una obra digital durante su reproducción que utiliza una función de transformación oculta. En la figura 10, se proporciona una obra digital encriptada 1010 a la aplicación de reproducción 1012. La obra digital 1010 ha sido encriptada con un esquema de encriptación que preserva el formato que permite que la aplicación de reproducción 1012 genere datos de presentación encriptados 1016. Entonces, los datos de presentación encriptados 1016 se envían al motor de desencriptación 1018 en el que son desencriptados en forma de datos de presentación no encriptados 1020. Los datos de presentación están ahora en un formato no encriptado (*in the clear*), pero menos propenso a ser regenerado en el formato digital original. Si los datos de presentación 1020 pueden ser vistos o utilizados directamente por el usuario, entonces no se necesita otro procesamiento. Sin embargo, a veces se requiere una representación adicional por parte de un sistema de visualización tal como una impresora. En tal caso, se proporcionan los datos de presentación 1020 a la aplicación de representación del sistema de visualización (en el caso de una impresora ésta podría ser un descomponedor (*decomposer*)) 1022 que genera datos de imagen 1024. Entonces los datos de imagen 1024 son proporcionados a un dispositivo de visualización 1026.

En un contexto general, el problema de la transformación oculta puede enunciarse de la siguiente manera. Supongamos que un cliente *Cathy* quiere que un servidor *Steve* calcule para ésta un valor de la función $F(a, x)$ con sus datos (públicos o privados) a y sus datos privados x, y *Cathy* desea, por cuestiones de privacidad, que la transformación se realice sin que *Steve* conozca sus datos privados x y el valor de la función $F(a, x)$. Desde el punto de vista de *Steve*, esto significa que éste calcula $F(a, x)$ para *Cathy* pero con sus ojos vendados. Lo que esto significa es que a *Cathy* le gustaría que el servidor *Steve* realizara la transformación sólo con datos $E_k(x)$ encriptados usando la clave k de *Cathy*, y le retornara el valor de la función $E_k\left(F(a, x)\right)$ también encriptado usando su clave k. Si *Steve* puede realizar la transformación usando datos encriptados, entonces *Cathy* ha evitado revelar los datos x en un formato no encriptado (*in the clear*) y el resultado $F(a, x)$ en un formato no encriptado (*in the clear*). A continuación se muestra el modelo ideal de la transformación oculta con datos encriptados parcialmente:

$$\begin{array}{ccc} (a, x) & \xrightarrow{E_k} & \left(a, E(x)\right) \\ F \downarrow & & \downarrow F' \\ F(a, x) & \xleftarrow[D_k = k^{-1}]{} & F'\left(a, E(x)\right) \end{array}$$

La función F' que hace que el diagrama conmute es lo que *Steve* calcula realmente, y el resultado de la transformación $F'\left(a, E_k(x)\right) = E_k\left(F(a, x)\right)$ está preparado para su desencriptado con el fin de revelar el valor deseado de la función $F(a, x)$. Puesto que *Steve* no "ve" los datos x en formato no encriptado (*clear data x*) así como el valor de la función $F(a, x)$, éste realiza una transformación "oculta" para *Cathy*.

Un protocolo de transformación oculta se puede describir de la siguiente manera para la evaluación oculta de la función $F(a, x)$:

(i) *Cathy* encripta x usando su clave de encriptado k, de lo cual resulta $E_k(x)$.

(ii) *Cathy* envía $E_k(x)$ a *Steve*.

(iii) *Steve* evalúa la versión modificada F' de la función F sobre los datos no encriptados a y los datos encriptados $E_k(x)$.

(iv) *Steve* devuelve el resultado $F'(a, E_k(x))$ a *Cathy*.

(v) *Cathy* desencripta $F'(a, E_k(x))$ usando su clave de desencriptación k^{-1} y obtiene $F(a, x)$.

El modelo ideal de transformación oculta introducido aquí se puede considerar como una generalización de firmas ocultas (*blind signatures*) y ocultación de instancias (*instance hiding*). La transformación oculta permite ahora datos parcialmente encriptados como input y, más importante aún, permite que la función F' calculada por el servidor posiblemente sea diferente de la función prevista F. Calculando F' en vez de F, el servidor, aunque tenga aún los ojos vendados, es consciente de que el input está parcialmente encriptado y por lo tanto es cooperativo con el cliente. La transformación oculta y el cálculo móvil seguro comparten un objetivo común de mantener el valor de la función que el servidor calcula en privado para el cliente, pero difieren en que el cliente proporciona los datos de input y el servidor proporciona (un programa que evalúa) la función de transformación oculta, si bien es en el sentido inverso en el cálculo móvil seguro. Téngase en cuenta que la transformación oculta permite que una parte de los datos (por ejemplo, a) estén sin encriptar. Esto permite el uso de algunos datos dinámicos y aún sin encriptar en el proceso de representación, tales como el tamaño de la ventana de visualización, las posiciones de referencia para el cambio de contenido (*shifting content*), el factor de escala y coeficientes en una operación de rotación.

La transformación oculta sólo funciona si existen las funciones F y F' para procesar los datos encriptados. Se puede demostrar que funciones afines de coeficiente entero y multi-variables (*multivariate, integer coefficient affine functions*) que usan esquemas de encriptado aditivo (*additive encryption schemes*) permiten, en la transformación oculta, evaluar muchas funciones de representación de documentos de tipo afín en las coordenadas x e y. Para un esquema de encriptado S dado, una función $F: X \to X$ se dice que es calculable de forma S-oculta (*S-blindly computable*) si existe alguna función $F': X \to X$ tal que la complejidad de cálculo para evaluar F' es un polinomio de la complejidad para evaluar F, y

$$F(a, x) = D^{k-1}(F'(a, E_k(x)))$$

para cualquier $k \in K$ y $x \in X$. Una función $F: X \to X$ se dice que es calculable de forma oculta si existe un esquema de encriptación S de manera que X es un subconjunto de su espacio de mensajes tal que F es calculable de forma S-oculta.

Cualquier función afín de coeficiente entero y multi-variable (*multivariate, integer coefficient affine function*) es calculable de forma S-oculta para cualquier esquema de encriptado aditivo. En concreto, supóngase que

$F_{x_0,a_1,\ldots,a_k}(x_1,\ldots,x_k) = x_0 + \sum_{i=1}^{k} a_i x_i$ es una función afín multivariable con una constante $x_0 \in X$, unos coeficientes enteros a_i y unas variables $x_1,\ldots,x_k$ en X. Entonces, para cualquier clave $k \in K$, existe una función computacionalmente eficiente

$F'_{y_0,b_1,\ldots,b_k}(y_1,\ldots,y_k) = y_0 \oplus \bigoplus_{i=1}^{k} b_i y_i$ de tal manera que

$$E_k(F_{x_0,a_1,\ldots,a_k}(x_1,\ldots,x_k)) = E_k\left(x_0 + \sum_{i=1}^{k} a_i x_i\right) = F'_{y_0,b_1,\ldots,b_k}(E_k(x_k))$$

En efecto, puede considerarse que la constante y_0 y los coeficientes enteros b_i en $F'_{y_0,b_1,\ldots,b_k}$ son $y_0 = E_k(x_0)$, $b_i = a_i \quad i = 1,\ldots,k$. La transformación oculta de funciones afines de coeficiente entero y multi-variables usando esquemas de encriptado aditivo permite que muchas funciones de representación de documentos de tipo afín en las coordenadas x e y sean evaluadas de forma oculta, lo cual proporciona una base teórica para la encriptación que preserva el formato y la representación confiable de documentos que se describen en este documento.

Un documento es por lo general un mensaje que se ajusta a un determinado formato. Para encriptar el documento, aparte de simplemente encriptar todo el documento, hay muchas maneras diferentes de encriptar sólo algunas partes del documento. El objetivo aquí es que no pueda utilizarse la fuga de información sobre la parte sin encriptar, o si hay fuga, que sea computacionalmente difícil de reconstruir el documento original no encriptado.

Si un esquema de encriptado que preserva la información de formato de la obra digital, entonces se puede usar cualquier función de transformación (aplicación de reproducción o aplicación de representación). Se describe a modo de referencia un ejemplo de procedimiento de encriptación que preserva el formato con referencia a documentos basados en símbolos (*tokens*). El procedimiento de encriptación que preserva el formato puede extenderse fácilmente o aplicarse a documentos en otros formatos (por ejemplo HTML/XML, Microsoft Word, Acrobat PDF, etc.). En un formato basado en símbolos (*tokens*) como el *Xerox DigiPaper*, cada imagen de página de un documento se representa como un "diccionario" de imágenes simbólicas (*token images*) (tales como caracteres y elementos gráficos) e información de ubicación (que indica donde aparecen esas imágenes simbólicas en la página). Por lo tanto, se pueden representar varias ocurrencias del mismo símbolo en el documento mediante una sola imagen de ese símbolo en el diccionario.

El proceso de representación de un documento en dicho formato se lleva a cabo entonces leyendo consecutivamente ubicaciones de símbolos (*tokens*), recuperando del diccionario las imágenes de los símbolos y dibujando las imágenes en las ubicaciones especificadas. Los beneficios de los documentos basados en símbolos son un tamaño compacto de los archivos y una velocidad rápida de representación para su uso en la distribución, visualización e impresión de los documentos electrónicos. En el formato *DigiPaper*, los símbolos se almacenan como imágenes binarias utilizando el formato de compresión Grupo 4 de CCITT, o como imágenes en color utilizando la compresión JPEG, y la información de ubicación de los símbolos se comprime aún más mediante la codificación Huffman.

Para mayor provecho, un documento D basado en símbolos de P páginas es modelado formalmente como una tabla (diccionario) de símbolos T de tamaño $|T|$, junto con una secuencia de P tablas de ubicaciones L_k de tamaño $|L_k|$ $(1 \leq i \leq P)$, que representan las imágenes de las P páginas. Cada entrada $T[j], 1 \leq j \leq |T|$, es un par $(id[j], t[j])$ de un identificador $id[j]$ y una imagen $t[j]$ del j-ésimo símbolo. Cada entrada $L_i[k], 1 \leq k \leq |L_i|$, de la tabla L_i de ubicación de la i-ésima imagen es una terna $(id[k], x[k], y[k])$ que representa la k-ésima ocurrencia del símbolo en la i-ésima imagen de página, en que $id[k]$ es el identificador de símbolo y $x[k], y[k]$ son sus diferencias en cuanto a las coordenadas x e y con respecto a la anterior $(k-1)$-ésima ocurrencia de símbolo. Por ejemplo, considérese el documento simple que se muestra en la Figura 11. El diccionario de símbolos y la tabla de ubicaciones (usando las coordenadas x, y) para este documento se muestran en las Figuras 12 y 13, respectivamente.

El pseudo-código esquemático $Representar(D)$ de más abajo muestra cómo se representan las imágenes de página de un documento D. En el código, x_0, y_0 son las referencias de base para las coordenadas x e y de cada página, $Buscar(T, id[k])$ es un subprograma que, con el input del diccionario T y un identificador de símbolo $id[k]$, devuelve una imagen simbólica t de T que corresponde al identificador dado, y $Dibujar(x, y, t)$ es un subprograma que dibuja la imagen simbólica t en la ubicación (x, y).

```
Representar(D)

{

        Cargar T en memoria

        para i=1 hasta P hacer
```

{

Cargar L_i en memoria

$x = x_0$

$y = y_0$

para k=1 hasta $|L_i|$ hacer

{

$x = x + x[k]$

$y = y + y[k]$

$t = Buscar(T, id[k])$

$Dibujar(x, y, t)$

}

}

}

Además de la transformación de desplazamiento (*shifting transformation*) $x' = x + a$, $y' = y + b$ según se usa en el proceso esquemático de representación descrito anteriormente, hay otras varias transformaciones de coordenadas que pueden producirse durante la representación del documento.

De escala. La transformación de escala es de la forma $x' = ax$, $y' = by$, en la que a y b son factores de escala para la coordenada x y la coordenada y , respectivamente. El escalado puede ser causado por el cambio de tamaño de la ventana de visualización o del papel de impresión.

Rotación. La transformación de rotación es $\begin{pmatrix} x' \\ y' \end{pmatrix} = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \begin{pmatrix} x \\ y \end{pmatrix}$ para algunas constantes a , b , c , d , que forman una matriz de rotación de 2 por 2. Esta transformación es necesaria cuando se rota la imagen de la página.

Transformación afín. Una transformación afín es una de la forma $x = ax + by + e$; $y = cx + dy + f$ para algunas constantes a , b , c , d , e , f . En forma de vector, ésta es:
$\begin{pmatrix} x \\ y \end{pmatrix} = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \begin{pmatrix} x \\ y \end{pmatrix} + \begin{pmatrix} e \\ f \end{pmatrix}$. Claramente, las transformaciones de desplazamiento, escala y rotación son casos especiales de transformaciones afines. Son esas transformaciones de tipo afín que hacen que sea posible lograr una representación confiable de alto nivel bajo la encriptación de la información de coordenadas usando unos esquemas de encriptado aditivo que se describen a continuación.

Se usa una clase especial de sistemas de encriptación, es decir, esquemas de encriptado aditivo, para llevar a cabo una transformación oculta de las funciones de tipo afín, lo que proporciona una base para la representación confiable de documentos. La transformación oculta por medio de una transformación de representación R y R' de un documento encriptado satisface la relación: $D\left(R'\left(E(x)\right)\right) = R\left(D\left(E(x)\right)\right)$, en la que E es una función de encriptación y D es una función de desencriptación para E . Si $E(x)$ es un esquema de encriptado aditivo, entonces $R' = R$.

Un esquema de encriptación S consta generalmente de básicamente cinco componentes: (i) un espacio de mensajes X que es una colección de mensajes posibles, (ii) un espacio de texto encriptado Y que es una colección de mensajes encriptados posibles, (iii) un espacio de claves K que es un conjunto de claves posibles, (iv) una función de encriptación computacionalmente eficiente $E: K \times X \rightarrow Y$, y (v) una función de desencriptación computacionalmente eficiente $D: K \times Y \rightarrow X$. Para cada clave $k \in K$, hay una clave única $k^{-1} \in K$, de tal manera que la función de encriptado $E_k = E(k,): X \rightarrow Y$ y la función de desencriptación $D_{k^{-1}} = D(k^{-1},): Y \rightarrow X$ satisface que, por cada mensaje $x \in X$, $D_{k^{-1}}(E_k(x)) = x$. La clave k se denomina una clave de encriptación y k^{-1} su correspondiente clave de desencriptación.

Tales esquemas de encriptación definidos pueden variar de diversas maneras para cubrir una amplia gama de esquemas de encriptación concretos utilizados en la práctica. Una variación es considerar si las claves utilizadas para la encriptación y la desencriptación son diferentes o no. En el caso en que todas las claves de encriptación k son iguales a sus correspondientes claves de desencriptación k^{-1}, el esquema es simétrico (o de clave privada); de lo contrario, el esquema es asimétrico. En el caso en que, para todas las k posibles, k^{-1} es diferente de k y es computacionalmente difícil derivarla a partir de k , el esquema es un esquema de encriptación de clave pública.

Otra variante es diferenciar los esquemas de encriptación deterministas y probabilísticos. En un esquema determinista, todas las funciones de encriptación y desencriptación E_k y $D_{k^{-1}}$ son funciones deterministas, mientras que en un esquema probabilístico la función de encriptación E_k puede ser no determinista, es decir, la aplicación dos veces de la función a un mensaje puede dar lugar a dos mensajes encriptados diferentes.

Un esquema de encriptado aditivo es un esquema de encriptación cuyo espacio de mensajes X y espacio de texto encriptado Y poseen algunas estructuras aditivas y la función de encriptación $E_k = E(k,): X \rightarrow Y$ es homomórfica con respecto a las estructuras aditivas. En concreto, considérese que $X = (X, +, 0)$ e $Y = (Y, \oplus, 0)$ son dos semigrupos conmutativos con (posiblemente diferentes) elementos cero 0 que satisfacen, por ejemplo, para todo x , $x + 0 = x$ y $0 + x = x$, y operaciones eficientes $+$ y $\oplus$. Un esquema de encriptado se dice que es aditivo si, para cualquier elemento $k \in K$ y cualquier x , $x' \in X$, $E_k(x + x') = E_k(x) \oplus E_k(x')$, y la operación $\oplus$ no revela los

mensajes no encriptados x y x'. La última condición sobre $\oplus$ hace que los esquemas de encriptado aditivo sean no triviales. Sin esta condición, la operación $\oplus$ sobre Y se puede definir de forma trivial $y \oplus y' = E_k(D_{k-1}(y) + D_{k-1}(y'))$; es decir, se realiza desencriptando primero los argumentos, a continuación sumándolos y finalmente re-encriptando el resultado.

En estrecha relación con los esquemas de encriptado aditivo están los que son multiplicativos. Un esquema de encriptado se dice que es multiplicativo si su espacios X e Y tienen estructuras de anillo (es decir, además de sus estructuras aditivas, tienen unas respectivas multiplicaciones $\times$ y $\otimes$ que son distributivas sobre sus adiciones $+$ y $\oplus$, e identidades multiplicativas), la función de encriptación E_k es homomórfica con respecto a las multiplicaciones, $E_k(x \times x') = E_k(x) \otimes E_k(x')$; y la operación $\otimes$ no revela los mensajes no encriptados x y x'.

En general, los esquemas de encriptado aditivo (así como los multiplicativos) no son no maleables, ya que un esquema no maleable requiere que, dado un mensaje encriptado sea (al menos computacionalmente) imposible generar un mensaje encriptado diferente de manera que los respectivos mensajes no encriptados estén relacionados. En consecuencia, tienen una debilidad ante ataques activos en los que el adversario intenta eliminar, añadir o alterar de alguna otra manera los mensajes encriptados. Sin embargo, cuando se utilizan estos esquemas para encriptar documentos, se pueden tomar medidas adicionales de integridad de datos y de autenticación de mensajes para reducir los riesgos causados por estos ataques activos en la integridad de los documentos, así como en la confidencialidad. Por otra parte, los usuarios finales están menos motivados en cuanto a iniciar ataques activos, ya que los ataques afectarán al contenido del documento que los usuarios van a utilizar y consumir.

No todos los esquemas de encriptado se pueden definir al igual que los aditivos de una manera fácil y natural. De hecho, algunos esquemas de encriptado están diseñados con un requisito de no ser aditivo o al menos de ser capaz de convertirse en no aditivo. Sin embargo, hay muchos ejemplos de esquemas de encriptado aditivos que se pueden utilizar en el procedimiento de encriptación que preserva el formato y representación confiable de documentos. **Mult**, **Exp** y **EG** (tres esquemas deterministas), **OU** (probabilístico) y **RSA** son ejemplos de esquemas de encriptado aditivo (con diversos grados de vulnerabilidad a los ataques) que se pueden usar en el procedimiento que preserva el formato.

El Cifrado Multiplicativo (**Mult**) es un esquema de encriptado simétrico, en el que $X = Y = Z_n = \{0,1,\ldots n-1\}$ para algún entero $n > 0$. La encriptación de un mensaje x mediante una clave a es

$$y = E_a(x) = ax \pmod n$$

y la desencriptación de un mensaje y con una clave a es

$$x = D_a(y) = a^{-1}\, y \pmod n,$$

en que a^{-1} es el inverso multiplicativo de un módulo n.

El encriptado exponencial (**Exp**) es una encriptación simétrica, en la que $X = Z_{p-1}$ y el espacio de texto cifrado $Y = Z_p$ para algún primo p, y K es el conjunto de todos los generadores del grupo multiplicativo Z_p^*. Para cualquier generador $g \in K$, la función de encriptación se define como la función exponencial

$$E_g(x) = g^x \pmod p,$$

mientras que la función de desencriptación se define como la función logarítmica

$$D_g(y) = log_g y \pmod{p-1}.$$

El cifrado semi-probabilístico *ElGamal* (**EG**) extiende el cifrado exponencial al cifrado *ElGamal*, que hace que el cifrado *ElGamal* funcione en un modo semi-probabilístico. Para cada mensaje $x \in Z_p$, en que $Z_p = \{1,\ldots p-1\}$ para algún número primo p, g es un generador en el grupo multiplicativo Z_p^*, la clave de desencriptación privada de un usuario es un número aleatorio $a \in Z_{p-1}^*$, la clave de encriptación pública $a = g^a \pmod p \in Z_p$, la encriptación $E_a(x,r)$ depende de un número aleatorio elegido uniformemente $r \in Z_{p-1}^*$:

$$E_a(x,r) = (g^r \pmod p, xa^r \pmod p) = (s,t).$$

Para un mensaje encriptado (s,t), la función de desencriptación se define como

$$D_a(s,t) = t(s^a)^{-1} \pmod p$$

El cifrado *ElGamal* en su forma original según se ha descrito anteriormente es apenas aditivo. Sin embargo, el operador $\oplus$ puede ser definido en parte en el texto cifrado de aquellas x que comparten un mismo número aleatorio r, de la siguiente manera:

$$E_\alpha(x,r) \oplus E_\alpha(x',r) = (s,t) \oplus (s,t') = (s, t+t') = E_\alpha(x+x' (mod\ p), r).$$

Esta operación parcialmente definida es aplicable cuando un lote (*batch*) de mensajes se encriptan utilizando un mismo número aleatorio r.

Cifrado *Okamoto-Uchiyama* (**OU**). Okamoto y Uchiyama propusieron un esquema de encriptación de clave pública, aditivo en *T. Okamoto* y *S. Uchiyama*. "*A New Public-Key Cryptosystem as Secure as Factoring*", *Eurocrypt'98, Lecture Notes in Computer Science* 1403, 308-318, 1998, que es probabilística y demostrablemente tan seguro como la dificultad de factorizar $n = p^2 q$ contra adversarios pasivos. Elíjanse dos números primos grandes p, q de k bits para algunas $k > 0$, y sea $n = p^2 q$. Elíjase $g \in Z_n^*$ aleatoriamente de modo que el orden de $g_p = g^{p-1} (mod\ p^2)$ es p. Sea $h = g^n (mod\ n)$. El espacio de mensajes X del esquema **OU** es el conjunto Z_p^* (no el conjunto $\{1, \ldots, 2^{k-1}\}$ según reivindican *Okamoto* y *Uchiyama*) y el espacio de textos encriptados Y es Z_n. Para un usuario, una clave pública es una tupla (n, g, h, k) y su correspondiente clave privada es el par (p, q) de los números primos. Para encriptar un mensaje $x \in X$, se elige de manera uniforme un número aleatorio $r \in Z_n$. Entonces el mensaje encriptado es

$$y = E_{(n,g,h,k)}(x,r) = g^x h^r (mod\ n).$$

Para desencriptar el mensaje encriptado y, se utiliza una función "logarítmica" $L: \Gamma \rightarrow \Gamma$,

$$L(x) = (x-1) p^{-1} (mod\ p^2),$$

en la que Γ es el p-subgrupo de *Sylow* de $Z_{p^2}^*$, es decir, $\Gamma = \{x \in Z_{p^2}^* \mid x \equiv 1 (mod\ p)\}$.

Con la función L, la función de desencriptación es

$$x = D_{p,g}(y) = L(y^{p-1} (mod\ p^2)) L(g_p)^{-1} (mod\ p^2).$$

Se pueden construir nuevos esquemas de encriptado aditivo a partir de los ya existentes a través de la construcción de composición de esquemas de encriptado. La construcción de composición también se puede utilizar para construir esquemas de encriptado aditivo a partir de no-aditivos. Por ejemplo, la composición del encriptado exponencial **Exp** y cualquier esquema de encriptado multiplicativo S (por ejemplo RSA) resulta en uno aditivo.

Los esquemas de encriptado aditivos permiten la transformación oculta con datos encriptados parcialmente, lo cual sirve de base para la representación confiable de documentos, según se mencionó anteriormente. En particular, se pueden usar esquemas de encriptación aditivos para llevar a cabo la transformación oculta de funciones afines con coeficientes sin encriptar y variables encriptadas.

Volviendo al ejemplo de un documento basado en símbolos (*tokens*), puesto que un documento basado en símbolos D consiste en un diccionario T de imágenes simbólicas y una secuencia de tablas de ubicación L_i (una para cada imagen de página), la idea es encriptar el contenido del diccionario T y las tablas de ubicación L_i, lo que resulta en un diccionario T' de imágenes simbólicas encriptadas y unas tablas L'_i de ubicaciones encriptadas. Recuérdese que el diccionario T consiste en una colección de pares $\{id[j], t[j] \mid j = 1, \ldots, |T|\}$. Una subrutina de Buscar (*Lookup*) está asociada con T en el proceso de representación, la cual dado un identificador válido id de símbolo, devuelve su correspondiente imagen simbólica t en T. En la encriptación del diccionario T, hay tres opciones básicas: encriptación de identificadores de símbolos, imágenes simbólicas, o ambos. Encriptar identificadores o imágenes simbólicas ayuda a desvincular la conexión entre los identificadores y sus imágenes simbólicas. Además, la encriptación de imágenes simbólicas protege las imágenes simbólicas propietarias. En cualquier caso, es deseable permitir el acceso válido al diccionario sólo dentro del proceso de representación P, al mismo tiempo que se hace que sea computacionalmente difícil obtener una copia de la totalidad de los contenidos no encriptados del diccionario. Esto es posible porque en muchos casos los identificadores válidos (por ejemplo, palabras de código de *Huffman*) son sólo un subconjunto muy pequeño de todas las cadenas binarias de hasta una cierta longitud, y en consecuencia cualquier búsqueda exhaustiva de identificador no será eficiente.

Más formalmente, dado el diccionario T y la rutina de Buscar (*Lookup*) que accede al mismo, el requisito en la encriptación del diccionario es que el diccionario encriptado T' y el correspondiente subprograma *Buscar'* satisfagan las siguientes restricciones:

(1) Para cualquier identificador encriptado $E_k(id)$, $Buscar'(T', E_k(id)) = E_k(Buscar(T, id))$ y

(2) Dadas T' y $Buscar'$, es computacionalmente imposible reconstruir T.

Para un esquema de encriptado S, T' y $Buscar'$ se pueden construir de la siguiente manera. Sea ID el conjunto de todos los identificadores sintácticamente posibles; en particular, $ID^* \subseteq ID$, en que $ID^* = \{id | (id,t) \in T\}$. Sea h una función hash unidireccional cuyo dominio es ID. Entonces, el diccionario de símbolos encriptado T' se deriva de T de la siguiente manera: para cada par (id,t) de T, se inserta un par $(h(id), E_K(t))$ en T'. La subrutina modificada *Buscar'* utiliza el algoritmo:

```
Buscar'(T', id)
{
    id* = h(id)
    t' = Buscar(T', id*)
    retornar(t')
}
```

Téngase en cuenta que el valor de retorno de $Buscar'$ es una imagen simbólica encriptada. La desencriptación de esta imagen será aplazada hasta la subrutina final $Dibujar'$ en el proceso de representación, que es parte de la representación de confianza que se describe a continuación.

Esta encriptación del diccionario es computacionalmente factible, tanto en términos de sobrecarga en cuanto a espacio de almacenamiento como en términos de sobrecarga en cuanto a tiempo de ejecución, para la realización de cálculos con versiones encriptadas de diccionarios de símbolos. Si los algoritmos de hash y codificación utilizados en la subrutina *Buscar'* son lo suficientemente seguros, entonces es computacionalmente muy difícil recuperar T dados T' y *Buscar'*.

Puesto que cada entrada de una tabla de ubicaciones L_i consiste de un identificador, y de la diferencia de ubicación en coordenadas x e y, puede encriptarse cualquier combinación de los tres elementos. Para encriptar la información de ubicación, se recomienda un esquema de encriptado aditivo para permitir la aplicación de cualquier transformación de representación de tipo afín a las coordenadas de ubicación. Para los identificadores, se debe conseguir un equilibrio entre la compresión del documento y la protección del documento. En un documento basado en símbolos, un identificador de símbolo es generalmente una palabra de código (*codeword*) de algún esquema de codificación para compresión. Por ejemplo, cuando se utiliza el código *Huffman* para comprimir el documento, los identificadores son las palabras de código *Huffman* binarias de los símbolos en función de su frecuencia de aparición en el documento. En este caso, el simple uso de un esquema de encriptado determinista para encriptar estos identificadores no ofrece ninguna protección eficaz sobre los mismos. Esto se debe a que el esquema no cambia la frecuencia de aparición de cada símbolo, y por lo tanto cualquier persona puede volver a contar el número de apariciones de los identificadores encriptados para reconstruir las palabras de código *Huffman* que son los identificadores. Por lo tanto, con el fin de ocultar las frecuencias de aparición de los símbolos en el documento, se prefiere utilizar un esquema de encriptado probabilístico para encriptar los identificadores. Sin embargo, esto interferirá con la codificación óptima realizada en los identificadores (palabras de código) y reducirá la ratio de compresión del documento. Esto puede no ser deseable para documentos basados en símbolos, puesto que conseguir una buena compresión del documento es uno de los objetivos de diseño para documentos basados en símbolos.

Se sugiere un compromiso razonable para la encriptación de L_i. Elegir un esquema de encriptado aditivo S, preferiblemente uno probabilístico y asimétrico como el cifrado **OU** de *Okamoto-Uchiyama* si la eficiencia de la encriptación y desencriptación no es un gran problema. Para cada entrada (id,x,y) de L_i, insertar $(id, E_K(x), E_K(y))$ en L'_i. Si también es necesario encriptar los identificadores, pueden insertarse entradas como $(E_K(id), E_K(x), E_K(y))$ en la tabla de ubicación L'_i. Pero en este caso, se requiere cambiar las entradas del diccionario encriptado T' por $(E_K(id), E_K(t))$'s, y la subrutina *Buscar'* de antes también necesita ser modificada para reflejar el cambio.

Con el encriptado que preserva el formato de un documento basado en símbolos mencionado anteriormente, también se puede proteger el contenido del documento durante el proceso de representación. La idea es retrasar la desencriptación en $Dibujar'(x,y,t)$. El proceso de representación se muestra a continuación.

Representar(D)

{

Cargar T en memoria

para i=1 hasta P hacer

{

Cargar L_i *en memoria*

$x = E_K(x_0)$

$y = E_K(y_0)$

para k=1 hasta $|L|$ hacer

{

$x = x \oplus x[k]$

$y = y \oplus y[k]$

$t =$ *Buscar*$(T, x[k])$

Dibujar(x, y, t)

}

}

}

Dibujar(x, y, t)

{

$x = D_{k-1}(x)$

$y = D_{k-1}(y)$

$t = D_{k-1}(t)$

Dibujar(x, y, t)

}

Durante el proceso, toda la información de coordenadas e imágenes simbólicas permanece encriptada antes de llamar a la subrutina *Dibujar*(x, y, t). Esto es posible para la información de coordenadas debido a que el esquema de encriptado es aditivo. Por consiguiente, el nivel de protección del contenido y el rendimiento del proceso de representación del proceso de representación se basan en la potencia de la seguridad y la complejidad de cálculo del esquema utilizado.

En otra forma de realización de la invención, una obra digital es polarizada permitiendo la representación o reproducción de confianza de la obra digital sin despolarizar el contenido digital o los datos de presentación. En esta forma de realización, la obra digital es del tipo que incluye contenido digital e información de recursos (también llamado un contexto de sistema). La información de recursos incluye información de formato u otra información

utilizada por una aplicación de reproducción o de representación para convertir la obra digital en datos de presentación.

La polarización es un tipo de transformación que hace que el contenido original sea ilegible o inutilizable. Para una obra digital w, un esquema de polarización T, el cual utiliza una semilla s, genera una obra digital polarizada w' de acuerdo con: $w' = T(w,s)$. Se puede utilizar también la misma transformación T para generar la información polarizada de recursos s' de acuerdo con $s' = T(s,s)$. En este ejemplo, se usa una semilla s para hacer que la ingeniería inversa del esquema de polarización sea más difícil.

Por ejemplo, una obra digital de tipo documento puede ser polarizada utilizando un esquema de polarización sencillo. En un documento, el contenido digital comprende una serie de caracteres en un orden o ubicación particular. Si el documento se va a mostrar en un dispositivo de visualización, cada carácter debe poder ser mostrado en una ubicación determinada para su visualización por parte del usuario en el dispositivo de visualización, como en un monitor. Se requiere un sistema de coordenadas para mostrar cada carácter en el monitor, con lo que cada carácter del documento puede ser mostrado en el monitor. El contenido digital contiene información de coordenadas que es referenciada por el sistema de coordenadas del monitor. Por ejemplo, en este párrafo, la letra "F" aparece en la línea superior, con una sangría de cinco espacios.

Un esquema de polarización simple para mezclar (*jumbling*) el texto del párrafo anterior es traducir la ubicación de las letras con respecto al sistema de coordenadas. Cada letra del párrafo tiene una ubicación (x,y). Supóngase que la ubicación (x,y) de cada letra del párrafo anterior es polarizada usando una semilla (a,b) procedente del sistema de usuario. Se pueden usar las siguientes funciones de polarización para polarizar el párrafo anterior:

$Y = b^y$, para el eje vertical; y

$X = \frac{x}{a}$, para el eje horizontal.

En este ejemplo, el sistema de coordenadas del dispositivo de usuario debe ser polarizado para que la aplicación de reproducción transforme el contenido digital en datos de presentación, es decir, mostrar en el monitor el párrafo desencriptado. El sistema de coordenadas del dispositivo de usuario debe ser polarizado utilizando la misma semilla (a,b) para generar un sistema de coordenadas polarizado. Se utilizan las siguientes funciones de transformación para calcular ambas ubicaciones x e y de un punto dado:

$Y = \log_b(Y)$, para el eje vertical; y $X = aX$, para el eje horizontal, en que $\log_b$ es el logaritmo en base b.

Cuando la aplicación de reproducción obtiene la ubicación de un carácter de la obra digital polarizada, la ubicación viene dada por $(X,Y) = \left(\frac{x}{a}, b^y\right)$. Este valor es entonces aplicado al sistema de coordenadas del dispositivo $(X,Y) = (\log_b(Y), aX) = (x,y)$. Así, se muestra la ubicación correcta de "F" en la pantalla del usuario. En ambos casos de polarización, las formas polarizadas de la información de recursos y de la obra digital mantienen una asociación inherente. Estas formas polarizadas complementarias de la información de recursos y de la obra digital resultan en la base para un mecanismo eficaz para proteger la obra digital. Mientras que la aplicación de reproducción es capaz de mostrar la obra digital polarizada, es sólo con el contexto de sistema polarizado que la aplicación de reproducción es capaz de proporcionar datos de presentación sin encriptar (*clear*).

Mientras que la polarización, en general, no es tan rigurosa en cuanto a protección como la encriptación, pueden usarse diferentes niveles de polarización en función de la sensibilidad de la obra digital a proteger. Una obra sensible puede requerir un alto nivel de polarización; una obra de menor valor puede requerir un menor nivel de polarización. Si el entorno del usuario es de confianza, se puede utilizar un nivel más bajo de polarización. Una ventaja de utilizar un nivel más bajo de polarización es que requiere menos recursos del sistema para crear la obra digital polarizada y para representar o reproducir la obra digital polarizada. El tipo y la calidad de la semilla de polarización también se pueden usar en combinación con el esquema de polarización para determinar el nivel y la potencia de la polarización. Por ejemplo, una semilla de polarización más compleja (tal como una que contenga información de autorización procedente de una fuente de confianza o una semilla dinámica) proporcionará un mayor nivel de polarización y potencia.

La polarización se produce normalmente en la ubicación de distribución o de elaboración. Las obras digitales son por lo general polarizadas antes de su distribución al usuario o cliente mediante un esquema de polarización elegido por el elaborador o el distribuidor. La información de recursos a polarizar también puede ser preseleccionada antes de la entrega. Preferiblemente se utiliza una semilla para cada esquema de polarización. También preferiblemente, se genera la semilla utilizando la información proporcionada por el contexto de sistema del usuario.

Cuando un usuario compra una obra digital, el usuario proporciona preferentemente información del sistema de usuario en el cual el usuario pretende reproducir la obra digital. Esta información puede ser utilizada para generar la semilla de polarización tanto para la obra digital polarizada como la información de recursos polarizada (denominada a veces contexto de sistema polarizado). A continuación, la obra digital polarizada y el contexto de sistema polarizado o la información polarizada de recursos son proporcionados al usuario. También, por lo general, pero no es necesario para el funcionamiento de esta forma de realización de la invención, la obra digital polarizada y el contexto de sistema polarizado pueden ser encriptados antes de la distribución al usuario. El desencriptado de tanto la obra digital polarizada como el contexto de sistema polarizado en datos de presentación pueden ser necesarios antes de la reproducción de la obra digital polarizada, dependiendo del esquema de encriptado que se utilice.

El proceso para crear una obra digital polarizada se divide en tres etapas. Estas etapas son la generación de la semilla de polarización, la polarización de la obra digital y, la polarización de la información de recursos. Una vez que se genera la semilla de polarización, el motor de polarización es sembrado (*seeded*) con ésta. El motor de polarización toma como input la obra digital o la información de recursos, y genera la forma polarizada de la obra digital o de la información de recursos en base a la función de transformación sembrada (*feeded*) con la semilla de polarización. Durante la reproducción de la obra digital polarizada, se usa la información polarizada de recursos para generar los datos de presentación y/o datos de imagen. Se pueden usar las mismas o diferentes funciones de transformación de polarización para la obra digital y la información de recursos.

Se muestra un proceso para crear una obra digital polarizada con referencia a la Figura 14. Una obra digital 1410 incluye contenido digital y un conjunto de información de recursos utilizado para formatear y representar el contenido digital en una forma utilizable o visible para un usuario. La obra digital 1410 pasa por un proceso de polarización de contenido 1420 en el que se polariza el contenido digital y se preserva la información de recursos, creando la obra digital polarizada 1422. La polarización del contenido 1420 se puede producir según se muestra con referencia a la figura 9. Una obra digital suele incluir contenido, instrucciones y formato. Aunque la polarización puede producirse en toda la obra digital, preferiblemente sólo se polariza el contenido; las instrucciones y el formato no se polarizan. Sin embargo, en algunos casos, para algunas aplicaciones de reproducción, puede polarizarse también parte de la información de recursos contenida dentro de la obra digital. Esto es similar para el procedimiento de encriptado que preserva el formato descrito anteriormente.

La extracción de recursos 1412 extrae al menos una información de recurso del conjunto de información de recursos asociada con la obra digital 1410. La extracción consiste en copiar la información de recursos en un archivo de recursos del sistema 1414. Los recursos del sistema 1414 son entonces polarizados en la polarización de recursos 1416 para convertirse en recursos del sistema polarizados 1424. El esquema de polarización para la polarización del contenido y la polarización de recursos no tiene que ser el mismo. Preferiblemente, cada esquema de polarización utiliza una semilla de polarización 1418 que es generada por el generador de semillas 1426. A continuación se describen varios ejemplos de procedimientos para la generación de semilla. En particular, en una realización preferida, la semilla de polarización se basa en una información única procedente del sistema de usuario.

Se pueden utilizar varias técnicas para la generación de la semilla de polarización. Por ejemplo, se puede usar un generador de semilla que genera un número a partir de un generador de números aleatorios. Este procedimiento, conocido como polarización sin estado, no depende de ninguna información de clave secreta ni de información del sistema de usuario. El proceso para la polarización sin estado produce un valor específico para el sistema para la polarización. La vulnerabilidad inherente de los sistemas de seguridad digitales se puede encontrar en un mal manejo de información secreta, la complejidad matemática, y la complejidad algorítmica. La eliminación de la información secreta protege un objetivo del ataque. Con la polarización sin estado, un generador de números aleatorios produce la semilla de polarización. En este caso, una vez que se ha completado el proceso de polarización, la semilla es descartada sin dejar rastro. Por lo tanto, la seguridad del sistema está libre de ataques enfocados a poner en peligro la información secreta, y el usuario no necesita divulgar información sensible que pueda ser considerada una violación de la privacidad.

Otro generador de semilla que puede ser utilizado es un generador basado en estado. El generador de semillas basado en estado construye una semilla adquiriendo primero información del estado del sistema procedente del sistema de reproducción o dispositivo de presentación del usuario. La información del estado del sistema incluye identificadores de hardware, configuración del sistema y otra información relacionada con el estado del sistema. Si bien la polarización sin estado es de gran valor, otros requisitos de seguridad pueden requerir el uso de un enlace inseparable con un determinado sistema o dispositivo de usuario. Mediante la generación de la semilla de polarización a partir de información específica de dispositivo/sistema, el motor de polarización producirá una obra digital que es polarizada de una forma que corresponde a un sistema/dispositivo específico.

El generador de la semilla de polarización también puede estar vinculado a un proceso de autorización. En la polarización basada en autorización, la generación de la semilla puede estar vinculada con el resultado del proceso de autorización. Un repositorio de autorización separado (que es una fuente de confianza) proporciona información

de autorización como parte de alguna otra característica de seguridad asociada con el acceso de entrega de una obra digital a un usuario. La fuente de confianza de la información de autorización puede ser un repositorio de autorización en línea según se describe en la Patente de EE.UU. Nº 5.629.980. Esta información de autorización es entonces utilizada para generar una semilla de polarización.

Si se utiliza una semilla de polarización sin estado, la obra digital y su información de recursos pueden ser polarizadas y almacenadas en conjunto para su entrega a un usuario cuando un usuario compra los derechos de uso asociados para la obra digital en particular. Si se utiliza uno de los otros procedimientos de generación de semillas de polarización, la polarización normalmente debe esperar hasta que el usuario proporciona el estado del sistema o la información de autorización antes de que la obra digital y la información de recursos puedan ser polarizadas.

Una realización que proporciona un mayor nivel de protección en términos de asegurar que la obra digital puede ser reproducida sólo en un sistema o dispositivo físico específico, utiliza una semilla de polarización basada en un estado dinámico. En esta forma de realización, se deben proporcionar un motor de polarización y un generador de semillas de polarización a la aplicación de reproducción o dispositivo de representación junto con la obra digital y la información de recurso. En esta forma de realización, la obra digital y la información de recursos son polarizadas antes de la reproducción y representación utilizando una semilla que se genera basándose en el estado dinámico del sistema o dispositivo en particular. El estado dinámico puede derivarse, por ejemplo, del reloj del sistema, la utilización de la CPU, la asignación (*allocation*) del disco duro, las coordenadas del cursor, etc. Polarizando la obra mediante la captura de un estado dinámico, la obra es bloqueada bajo una configuración particular del sistema (es decir, estado) en el tiempo. La polarización de la obra digital, y en última instancia su reproducción oculta (descrita más abajo), se basa en un estado de evolución dinámico. La evolución del estado dinámico no produce una información secreta única que permita la repetición del proceso de polarización, y por lo tanto la polarización basada en el estado dinámico hace que sea más difícil que la obra digital polarizada y el contexto del sistema se vean comprometidos. El hecho de que el proceso de polarización se realiza dentro de un sistema de confianza, implica que el proceso no puede ser deconstruido.

El proceso real de polarización puede ser, según se describe en el ejemplo anterior, una transformación basada en algorítmica parametrizada por la semilla de polarización. Durante la polarización, los identificadores de datos y recursos de la obra digital son transformados según se ha descrito anteriormente. Sin embargo, la estructura de la obra digital no se ve alterada de manera que se mantiene el formato original, tal como PDF, DOC, WAV, u otro formato, al igual que en el encriptado que preserva el formato. De forma similar, la polarización de la información de recursos produce una forma polarizada de la información de recursos de tal manera que se transforman los identificadores de recursos, identificadores de elemento y características de los recursos, aunque la estructura del contexto del sistema permanece inalterada. Polarizando la obra digital y la información de recursos de acuerdo con la misma semilla basada en información del sistema o dispositivo específico de usuario, se establece una relación inseparable de tal manera que la obra no puede ser reproducida en su forma no encriptada con cualquier otro aparato o sistema de usuario. Si es distribuida de forma no autorizada, la protección sigue teniendo efecto.

Durante la reproducción oculta, las características únicas de la información polarizada de recursos permiten que la aplicación de reproducción reproduzca de forma adecuada la obra digital polarizada y genere los datos de presentación no polarizados o no encriptados (*clear*). Debido a que la obra digital y la información de recursos fueron transformadas de manera complementaria, los elementos polarizados de la obra digital, tales como identificadores y datos de recursos, hacen referencia sin querer a los elementos complementarios dentro de los recursos del contexto del sistema. Debido a la transformación de coincidencias (*matching transformation*) la aplicación de reproducción identifica los elementos adecuados dentro del contexto de tal manera que los datos de presentación resultantes aparecen no encriptados. Por lo tanto, la obra está protegida hasta el último momento posible después de la reproducción.

Como se comentó anteriormente, la distribución convencional de obras digitales a través de la web es relativamente sencilla. La obra se crea usando un editor, es publicada en un sitio web, es visitada por el público usuario y reproducida en un visor o en un sistema de visualización. Si un propietario de contenidos no desea proteger su obra digital (o si el propietario del contenido confía en todos los usuarios que recibirán la obra), la obra digital es proporcionada "sin encriptar" ("*in the clear*"), es decir, sin ningún tipo de codificación, encriptación u otra protección para su uso directo por parte de cualquier usuario.

Si la obra digital es descargada en el sistema del usuario, se almacena normalmente en la memoria. Si la obra digital es proporcionada a través de un medio de almacenamiento, tal como un disquete o CD-ROM o DVD-ROM, la obra digital suele ser accedida directamente desde el medio de almacenamiento.

Con el fin de reproducir la obra digital, en referencia a la figura 15, la obra digital 1510 es proporcionada a una aplicación de reproducción 1512. En el caso de un documento u otro tipo de obra digital que requiera información de formato o información de recursos, la obra digital incluirá contenidos digitales, además de información de recursos

que establece el contexto del sistema en particular o los recursos del sistema que necesita la aplicación de reproducción para procesar el contenido digital. Por ejemplo, la obra digital 1510 puede ser un documento de texto en el que el texto es mostrado con el tipo de letra Arial. Cuando la aplicación de reproducción 1512 accede a la información de recursos de la obra digital 1510 que indica que se utiliza el tipo de letra Arial, accede a los recursos del sistema apropiados 1516 (que en este caso es la tabla del tipo de letra Arial) y utiliza la información de recursos del sistema para convertir el contenido digital en datos de presentación 1514.

En algunas aplicaciones de reproducción, la conversión del contenido digital en datos de presentación es suficiente para su uso por parte del usuario. En otros, los datos de presentación es sólo una forma intermedia que debe ser convertida aún más. Por ejemplo, en el caso de un sistema de visualización 1524 que es una impresora, los datos de presentación 1514 deben ser representados aún más por la aplicación de representación 1518. La aplicación de representación 1518 puede ser un descomponedor dentro de la impresora. La aplicación de representación 1518 usa otros recursos del sistema 1516 para transformar los datos de presentación 1514 en datos de imagen 1520. Los datos de imagen 1520 están en una forma que puede ser mostrada directamente en el dispositivo de visualización 1522 (en el caso de una impresora, mostrado como un documento impreso).

Además de los sistemas y procedimientos descritos anteriormente para proteger una obra digital durante su reproducción, una obra digital puede ser protegida durante la reproducción polarizando la obra digital de acuerdo con un primer esquema de polarización que produce un contenido polarizado y conserva la información de recursos de la obra digital. Una parte de la información de recursos de la obra digital es copiada y polarizada de acuerdo con un segundo esquema de polarización. En referencia a la Figura 16, la aplicación de reproducción 1612 utiliza la información polarizada de recursos 1614 (y cualquier otra información de recursos del sistema 1616 que pueda ser necesaria) para transformar la obra digital polarizada 1610 en datos de presentación no encriptados 1618. Los datos de presentación están necesariamente en un formato no encriptado (*in the clear*), lo que significa que pueden ser capturados por otros programas (tal como un programa de utilidad de captura de pantallas). Sin embargo, el output de tales otros programas no está en el mismo formato y con frecuencia no es de la misma fidelidad que la obra digital original.

La información polarizada de recursos puede ser considerada como que actúa como un filtro de polarización para llevar el contenido digital polarizado hacia una imagen no encriptada (datos de presentación). Este sistema es un sistema de reproducción oculta en el que la aplicación de reproducción, que puede ser cualquier aplicación comercial, no conoce o necesita conocer el contenido digital no encriptado. La reproducción oculta funciona para cualquier función de transformación R , tal que $R(w',s') = R(w,s)$, en que w' es el contenido digital polarizado, w es el contenido digital no encriptado, s' es la información polarizada de recursos y s es la información no polarizada de recursos. La reproducción oculta de obras digitales polarizadas que utiliza información polarizada de recursos es diferente de la transformación oculta descrita anteriormente en que la reproducción oculta produce datos de presentación no encriptados sin tener que despolarizarlos. En la transformación oculta, la aplicación de reproducción convierte la obra digital encriptada en datos de presentación encriptados, que luego deben ser desencriptados. En ambos casos, el usuario no ve la obra digital original en forma no encriptada.

La reproducción oculta (también denominada representación oculta) que usa una obra digital polarizada e información polarizada de recursos puede ser utilizada en solitario para proteger la obra digital durante su reproducción, así como además del encriptado habitual. Por ejemplo, la obra digital polarizada y la información polarizada de recursos pueden ser encriptadas para protegerlas durante su distribución, luego desencriptada en el sistema del usuario para obtener la obra digital polarizada y la información polarizada de recursos. El usuario debe obtener primero el permiso del propietario del contenido o del distribuidor actuando en nombre del propietario del contenido (con el fin de desencriptar la obra digital encriptada). Una vez que el usuario está cualificado, la obra digital polarizada encriptada y la información de recursos polarizada encriptada son desencriptadas y la obra digital polarizada es reproducida en la aplicación de reproducción utilizando la información polarizada de recursos.

La complejidad de representar una obra digital en una forma utilizable para su visualización por un usuario puede ser utilizada para proteger aún más la obra digital durante su reproducción. En referencia a la figura 17, la obra digital polarizada 1710 es proporcionada a una aplicación de reproducción 1712, la cual utiliza los recursos del sistema polarizados 1716 y otros recursos del sistema 1718 para transformar la obra digital polarizada 1710 en datos de presentación parcialmente polarizados 1714. En esta forma de realización, se necesita que el sistema de visualización 1728 transforme los datos de presentación en una forma utilizable por el usuario. Los datos de presentación parcialmente polarizados 1714 son proporcionados a la aplicación de representación 1720 la cual utiliza los recursos del sistema polarizados 1716, los recursos locales del sistema 1722 y los recursos del sistema 1718 para transformar los datos de presentación parcialmente polarizados 1714 en datos de imagen no encriptados 1724. Los datos de imagen no encriptados 1724 a continuación son mostrados en el dispositivo de visualización 1726 para su uso por parte del usuario. En esta forma de realización, los datos de presentación todavía están polarizados, trasladando la ubicación de los datos no encriptados a un punto posterior del proceso de visualización y proporcionando una mayor protección.

Para mejorar la usabilidad del sistema para polarizar obras digitales, la información polarizada de recursos puede estar separada de la obra digital y vinculada a un dispositivo transportable tal como una tarjeta inteligente (*Smart card*). En esta forma de realización, la aplicación de reproducción 1712 reproduce de nuevo la obra utilizando los recursos del sistema polarizados 1716. En lugar de tener los recursos de sistema polarizados 1716 almacenados en una memoria local, junto con la obra digital polarizada, 1710, los recursos del sistema polarizados 1716 están almacenados en un dispositivo transportable tal como una tarjeta inteligente (*Smart card*). Además, la tarjeta inteligente, posiblemente con funciones hardware mejoradas, puede poseer unos atributos que proporcionen una resistencia a la manipulación. En el contexto transportable, los datos polarizados son procesados por la aplicación de reproducción 1712 para producir los datos de presentación parcialmente polarizados y luego son proporcionados a la aplicación de representación 1720.

Se pueden proteger muchos tipos diferentes de obras digitales durante toda su utilización mediante el procedimiento de polarización. Por ejemplo, si la obra digital es un documento o archivo de texto, la aplicación de reproducción puede ser un procesador de textos, los recursos del sistema o la información de recursos puede incluir tablas de tipos de letra, diseño de página, y tablas de colores. Si la obra digital son datos de audio o vídeo (por ejemplo, secuencias (*streams*)), la aplicación de reproducción puede ser un reproductor de vídeo o de audio. Los datos de presentación serán las secuencias (*streams*) de datos finales de audio/vídeo. El sistema de visualización puede ser un dispositivo de audio/vídeo. La aplicación de representación puede ser el controlador (*driver*) del dispositivo de audio/vídeo. Los datos de imagen pueden ser las secuencias (*streams*) de datos del dispositivo de audio/vídeo y el dispositivo de visualización puede ser el dispositivo de representación de audio/vídeo (altavoz o monitor, por ejemplo).

Para una obra digital que es una secuencia (*stream*) de datos de audio/vídeo, los recursos del sistema o información de recursos pueden incluir características del dispositivo de audio/vídeo: frecuencia de muestreo (*sample rate*) (muestras por segundo - por ejemplo, 8 kHz, 44,1 kHz), calidad de la muestra (bits por muestra - por ejemplo, 8, 16), el tipo de muestra (número de canales - por ejemplo, 1 para mono, 2 para estéreo), y el formato de la muestra (instrucciones y bloques de datos). A continuación se muestra una tabla de algunas secuencias de datos de audio/vídeo y su correspondiente información de recursos o parámetros variables que se pueden seleccionar para la polarización:

Extensión	Origen	Parámetros variables (#Fijos)	Compresión	Reproductor
.mp3	MPEG estándar	frecuencia de muestreo, calidad, #tipo	MPEG	*MP3 player*
.ra	*Real Networks*	frecuencia de muestreo, calidad, #tipo	complementos (*plug-ins*)	*Real player*
.wav	*Microsoft*	frecuencia de muestreo, calidad, #tipo	ADPCM	*Windows Media*
.snd	*Apple*	frecuencia de muestreo, #calidad, #tipo	MACE	*Quicktime*

Tabla 1: Obra Digital: (secuencias de) datos de Audio/Vídeo

La estructura de una obra digital se puede utilizar de forma ventajosa para la polarización. Si bien es posible polarizar toda la obra digital, es más conveniente polarizar sólo una parte de la obra digital. La mayoría de obras digitales incluyen tres elementos principales: instrucciones, datos y recursos. Preferiblemente, sólo los datos y los recursos de la obra digital son polarizados, al igual que en el procedimiento de encriptado que preserva el formato descrito anteriormente. Transformando selectivamente solamente los datos y los recursos, una obra digital puede ser transformada de tal manera que el contenido permanece en el formato original, aunque los datos y los recursos son incomprensibles.

El diseño general de una obra digital del tipo documento se muestra en la Figura 18. En la figura 18, la obra digital 150 incluye un Descriptor de Página 152, Códigos de Control 154, 158 y 162, Identificador de Recursos 156, y Datos 160 y 164. Los Descriptores de Página 152 definen el diseño general de una obra. Por ejemplo, el tamaño de página, el número de página y los márgenes caen en la categoría de los Descriptores de Página con respecto a los documentos digitales. Los Códigos de Control 154, 158 y 162 son similares en que éstos describen la presentación del contenido. Unos ejemplos incluyen comandos para configurar la posición del texto, el texto de output, la configuración del tipo de letra, y la configuración de las coordenadas actuales de la pantalla. Los Identificadores de Recursos 156 simplemente hacen referencia a los recursos deseados. En el ámbito de documentos digitales, los recursos podrían variar desde el tipo de letra hasta el color de fondo. Por último, los Datos 160, 164 representan la

información básica comunicada por la obra digital. Ésta podría ser las coordenadas de dibujo (*drawing coordinates*) utilizadas en un clip multimedia o los códigos de caracteres para su representación como un documento digital.

Se muestran en las figuras 19 y 20 un ejemplo de una obra digital (en este caso un documento digital simple) y una de sus formas polarizadas, un documento *HTML* en forma no encriptada (*clear*) y polarizada. Las etiquetas *<html>* y *<body>* son Descriptores de Página. La etiqueta *<font>...<\font>* es un ejemplo de Código de Control para configurar las características del recurso de tipo de letra, mientras que *"Arial"* y *"14"* son Identificadores de Recursos para un tipo de letra *Arial*, de 14 puntos. El texto *"Hello World"* son los Datos o la información central de la obra. El *<p>* es otro Código de Control para señalar el comienzo de párrafo. Por último, el documento acaba con unos Descriptores de Página *<\ body>* y *<\ html>* para identificar el final del documento.

La figura 20 muestra el aspecto de la obra digital de la figura 19 en una forma polarizada. Se puede observar que el Descriptor de Página y las etiquetas de Códigos de Control permanecen inalterados; las etiquetas *<html>*, *<body>* y *<font>* están sin cambios. Mientras que, los Identificadores de Recursos, "Arial" y "14", se han transformado en valores indescifrables. De modo similar, los datos, "Hello World", también se han transformado en un valor indescifrable. Mediante la transformación de los Identificadores de Recursos y los Datos el contenido se representa con sentido pero en forma polarizada. Sin embargo, el hecho de que los Descriptores de Página y los Códigos de Control se mantengan intactos permite que el documento conserve su formato original, que en general podría ser *HTML*, *Adobe PDF*, *RealNetworks RAM*, *Apple QuickTime*, etc.

El contexto del sistema (o recursos del sistema o información de recursos) puede ser entendido como la colección de recursos del sistema disponibles para una aplicación de reproducción en un sistema particular. Por ejemplo, puede incluir la Tabla de Tipos de letra, Paleta de Colores, Coordenadas del Sistema y configuración del volumen. Cuando una obra digital es proporcionada como input a una aplicación de reproducción, la aplicación de reproducción usa la información de recursos en particular contenida dentro de la obra digital para transformar el contenido digital en datos de presentación. Cada contexto de sistema o información de recursos contenida dentro de una obra digital es o puede ser alterada para ser única para un sistema que la puede reproducir. El contexto del sistema es un elemento requerido para el uso de la obra digital, vinculando el uso de la obra digital a un sistema específico o dispositivo físico o aplicación de reproducción para su reproducción. Los Identificadores de Recursos y Datos dentro de la obra digital pueden referenciar ya sea directa o indirectamente a elementos contenidos dentro del contexto del sistema. Polarizando la obra digital y el contexto del sistema permite la representación oculta en forma de datos de presentación sin encriptar (*clear*). Polarizando el contexto del sistema con una semilla de polarización que está vinculada a un sistema único, el contexto del sistema polarizado resultante puede ser un entorno único en el que una obra digital polarizada complementaria, que ha sido polarizada con la misma semilla de polarización, puede ser accedida y reproducida.

La Figura 21 ilustra una configuración típica de contexto de sistema. Los elementos incluyen el identificador de recurso (ResID), el identificador de elemento (ElemID), y las características del recurso (Características). El ResID incluye la información pertinente para que otros componentes del sistema referencien a los recursos. El ElemID es el identificador de un elemento individual dentro del recurso. Por último, las Características son las características reales del recurso utilizadas para expresar el elemento de recurso individual.

La Figura 22 es una ilustración del recurso para la tabla de tipos de letra perteneciente al tipo de letra Arial. El identificador de recurso clave en este caso es el nombre del tipo de letra "Arial". Siguiendo la convención ASCII, el número 48 identifica el identificador de elemento de recurso individual. Las características del elemento de recurso para el ElemID representan la información para expresar la letra 'a'.

La Figura 23 es una ilustración del contexto del sistema polarizado para el recurso tipo de letra que se muestra en la Figura 22. El mismo identificador de recurso es transformado en "k13k2". El propio identificador de elemento no tiene por qué ser transformado, ya que es suficiente transformar solo las características del recurso. En este caso, "48" se representa como transformado para expresar las características de 'Y' en lugar de 'a'.

La polarización y la representación oculta se pueden utilizar para muchos tipos diferentes de obras digitales. Además de para documentos, la polarización y la representación oculta pueden utilizarse para datos de audio/vídeo. Como se señaló anteriormente, los datos de audio/vídeo generalmente se proporcionan en forma de secuencias (*streams*). Una aplicación de reproducción es el reproductor de audio/vídeo que transforma la secuencia de audio/vídeo digital en una secuencia de datos final, que puede ser procesada por un transductor (altavoz) en forma de un output de audio o por un visualizador en forma de una imagen de vídeo.

En referencia a la Figura 17, la aplicación de reproducción 1712 corresponde a un reproductor de audio/vídeo que generalmente funciona tomando muestras de las secuencias de input de audio/vídeo 1710 a alguna frecuencia de muestreo, calidad y tipo aceptado por un dispositivo de audio/vídeo de destino. Utiliza los recursos del sistema de audio/vídeo para muestrear, mezclar y producir secuencias de audio/vídeo y luego mezcla las secuencias de audio/vídeo re-muestreadas para producir una secuencia de audio/vídeo final en un formato esperado por el

dispositivo de destino. En el caso de un reproductor de audio/vídeo, los datos de presentación 1714 son la secuencia de audio/vídeo mezclada final a alguna frecuencia de muestreo, calidad, tipo y formato esperado por un dispositivo de audio/vídeo de destino.

El Dispositivo de audio/vídeo de destino (por ejemplo, la aplicación de representación 1720) es algún sistema hardware que es capaz de convertir secuencias de audio/vídeo (datos de presentación 1714) a una frecuencia de muestreo específica, calidad, tipo (canal) y formato (por ejemplo, PAL o NTSC) en los datos de audio/vídeo del dispositivo 1724. Ejemplos de dispositivos de audio incluyen tarjetas de sonido, altavoces, monitores y el convertidor de digital a analógico situado dentro del dispositivo de audio/video. Muchos dispositivos son capaces de reproducir secuencias de audio/vídeo a un rango de diferentes frecuencias de muestreo. Los datos de imagen 1724 (por ejemplo, una señal de audio o una secuencia de imágenes de vídeo) son generados por el controlador del dispositivo de audio/vídeo 1720 y "consumidos" por el dispositivo de visualización 1726.

Por ejemplo, para polarizar una secuencia de datos de audio/video, puede dividirse en dos o más secuencias separadas. Una secuencia es polarizada y una secuencia no es polarizada. Cada secuencia puede tener diferentes características de dispositivo (información de recursos): frecuencias de muestreo, canales, cualidades y/o formatos asociados a éste. Las características del dispositivo (una o más de las frecuencias de muestreo de la secuencia, canales, cualidades y/o formatos) también pueden ser polarizadas para generar la información polarizada de recursos.

La reproducción oculta de la secuencia de audio/video polarizada se lleva a cabo de una manera similar que para un documento digital polarizado. La aplicación de reproducción (reproductor de audio/vídeo) mezcla conjuntamente la secuencia no polarizada y la secuencia polarizada, y el uso de la información polarizada de recursos, produce una secuencia de datos finales polarizados para el dispositivo de audio/vídeo de destino con un conjunto correcto de información de recursos. El dispositivo de destino (1720) utiliza la información polarizada de recursos para reproducir la secuencia de datos polarizados que genera efectos de sonido/visuales no encriptados (1724).

Si bien anteriormente se han descrito en detalle ciertas formas de realización ejemplares de la invención, se debería reconocer que otras formas, alternativas, modificaciones, versiones y variaciones de la invención son igualmente operativas y serán evidentes para los expertos en la técnica. La divulgación no está enfocada a limitar la invención a alguna forma de realización en particular, y está enfocada a abarcar todas estas formas, alternativas, modificaciones, versiones y variaciones. Por ejemplo, las porciones de la invención que se han descrito anteriormente como componentes de software podrían ser implementadas como hardware. Además, mientras que ciertos bloques funcionales se describen en este documento como separados e independientes entre sí, estos bloques funcionales pueden ser consolidados y realizados en un único ordenador de propósito general, o aún más subdivididos en sub-funciones según se reconoce en la técnica. En consecuencia, el verdadero alcance de la invención está orientado a cubrir todas las alternativas, modificaciones, y equivalentes y debe determinarse con referencia a las reivindicaciones que se exponen a continuación.

REIVINDICACIONES

1. Un procedimiento de proteger una obra digital (1410; 1510) durante su transformación por una función de transformación en sus datos de presentación (1020; 1514), en el que la obra digital incluye contenido digital (1024; 1520; 1724) e información de formato, que comprende:

encriptar la obra digital de acuerdo con un esquema de encriptado aditivo que preserva el formato para generar una obra digital encriptada, en el que dicho esquema de encriptación que preserva el formato cuando genera la obra digital encriptada sólo encripta el contenido digital y preserva el formato de la obra digital;

transformar la obra digital encriptada en sus datos de presentación encriptados (1016); y

desencriptar los datos de presentación encriptados (1016) de acuerdo con una función de desencriptación para obtener los datos de presentación (1020; 1514), en el que los datos de presentación después de aplicar la función de desencriptación son los mismos que si se hubieran generado aplicando directamente la función de transformación a la obra digital.

2. El procedimiento de la reivindicación 1, en el que el esquema de encriptado aditivo que preserva el formato comprende el uso de un algoritmo de encriptación seleccionado del grupo que consiste de Mult, Exp, EG, OU, RSA y composiciones de los mismos.

3. El procedimiento de la reivindicación 1, en el que la función de transformación comprende cualquier función afín de coeficiente entero y multi-variable.

4. El procedimiento de la reivindicación 1, en el que la función de transformación comprende una transformación de coordenadas de tipo afín en coordenadas x e y de la forma $x' = ax + by + e$ e $y' = cy + dy + f$, en la que a, b, c, d, e, y f son coeficientes, (x,y) es la ubicación original de un elemento en la obra digital z y (x',y') es la ubicación transformada.

5. Un sistema de protección de una obra digital (1410; 1510) durante su transformación por una función de transformación en sus datos de presentación (1020; 1514), en el que la obra digital incluye contenido digital (1024; 1520; 1724) e información de formato, que comprende:

un motor de encriptación para encriptar la obra digital de acuerdo con un esquema de encriptación aditivo que preserva el formato para generar una obra digital encriptada, en el que dicho esquema de encriptación que preserva el formato cuando genera la obra digital encriptada sólo encripta el contenido digital y preserva el formato de la obra digital;

una función de transformación para transformar la obra digital encriptada en sus datos de presentación encriptados (1016); y

un motor de desencriptación (1018) para desencriptar los datos de presentación encriptados (1016) de acuerdo con una función de desencriptación para obtener los datos de presentación (1020; 1514), en el que los datos de presentación después de aplicar la función de desencriptación son los mismos que si se hubieran generado aplicando directamente la función de transformación a la obra digital.

6. El sistema de la reivindicación 5, en el que el esquema de encriptado aditivo que preserva el formato comprende el uso de un algoritmo de encriptación seleccionado del grupo que consiste de Mult, Exp, EG, OU, RSA y composiciones de los mismos.

7. El sistema de la reivindicación 5, en el que la función de transformación comprende cualquier función afín de coeficiente entero y multi-variable y E es un esquema de encriptado aditivo.

8. El sistema de la reivindicación 5, en el que la función de transformación comprende una transformación de coordenadas de tipo afín en coordenadas x e y de la forma $x' = ax + by + e$ e $y' = cy + dy + f$, en la que a, b, c, d, e, y f son coeficientes, (x,y) es la ubicación original de un elemento en la obra digital z y (x',y') es la ubicación transformada.

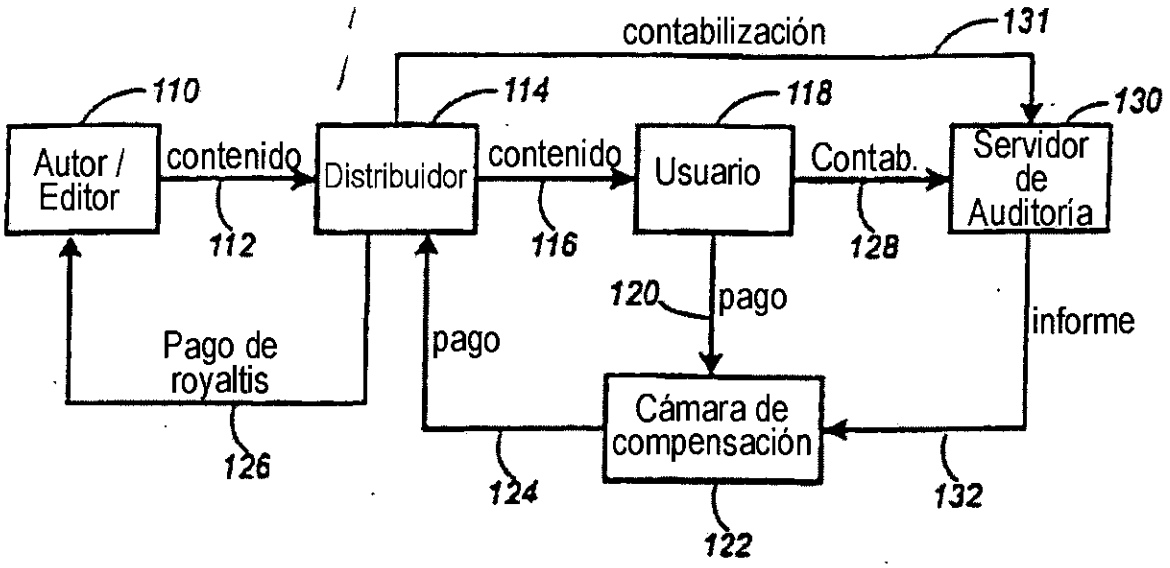


FIG. 1

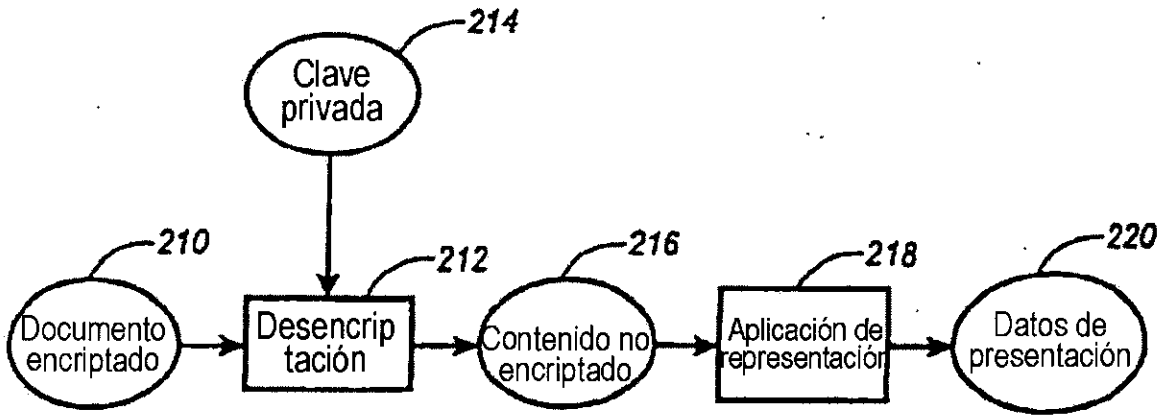


FIG. 2
(Técnica anterior)

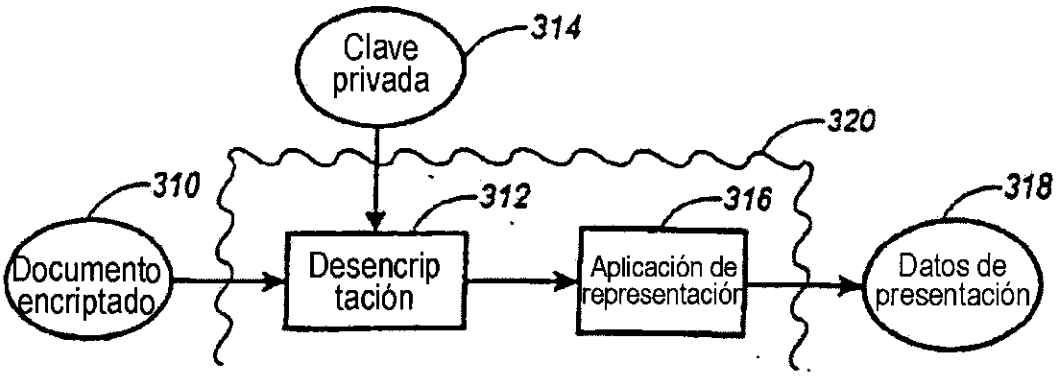

Clave privada
314
320
310
312
316
318
Documento encriptado
Desencrip tación
Aplicación de representación
Datos de presentación

FIG. 3

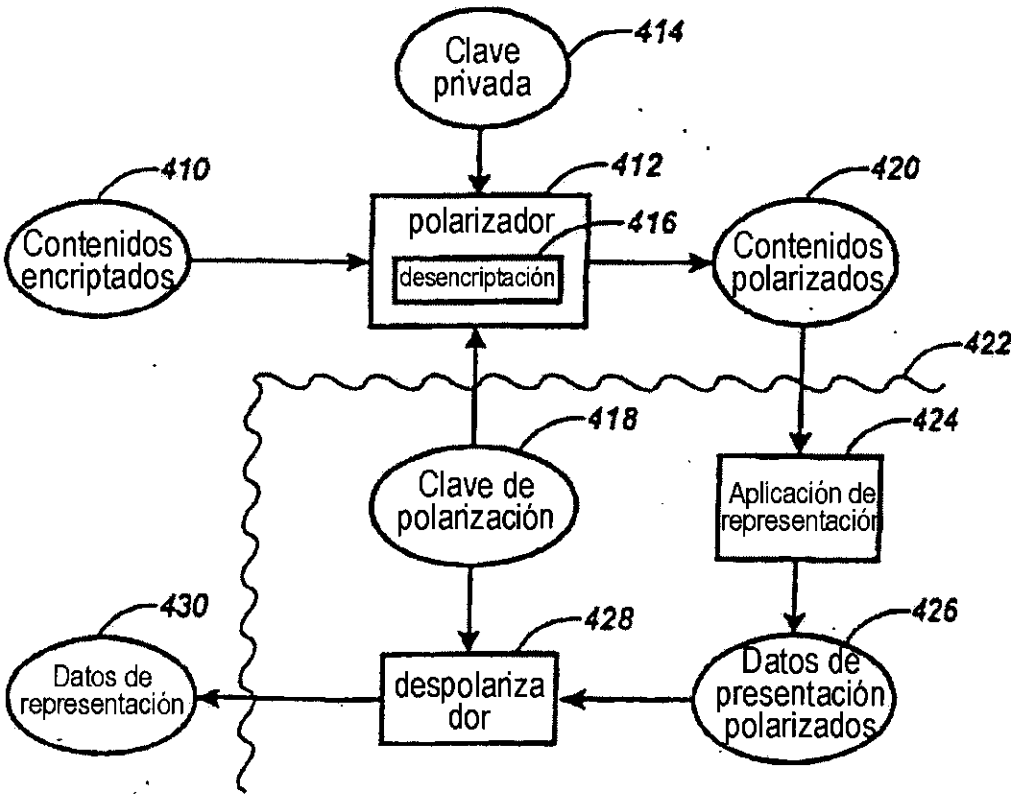

Clave privada
414
410
412
420
Contenidos encriptados
polarizador
416
desencriptación
Contenidos polarizados
422
418
424
Clave de polarización
Aplicación de representación
430
428
426
Datos de representación
despolariza dor
Datos de presentación polarizados

FIG. 4

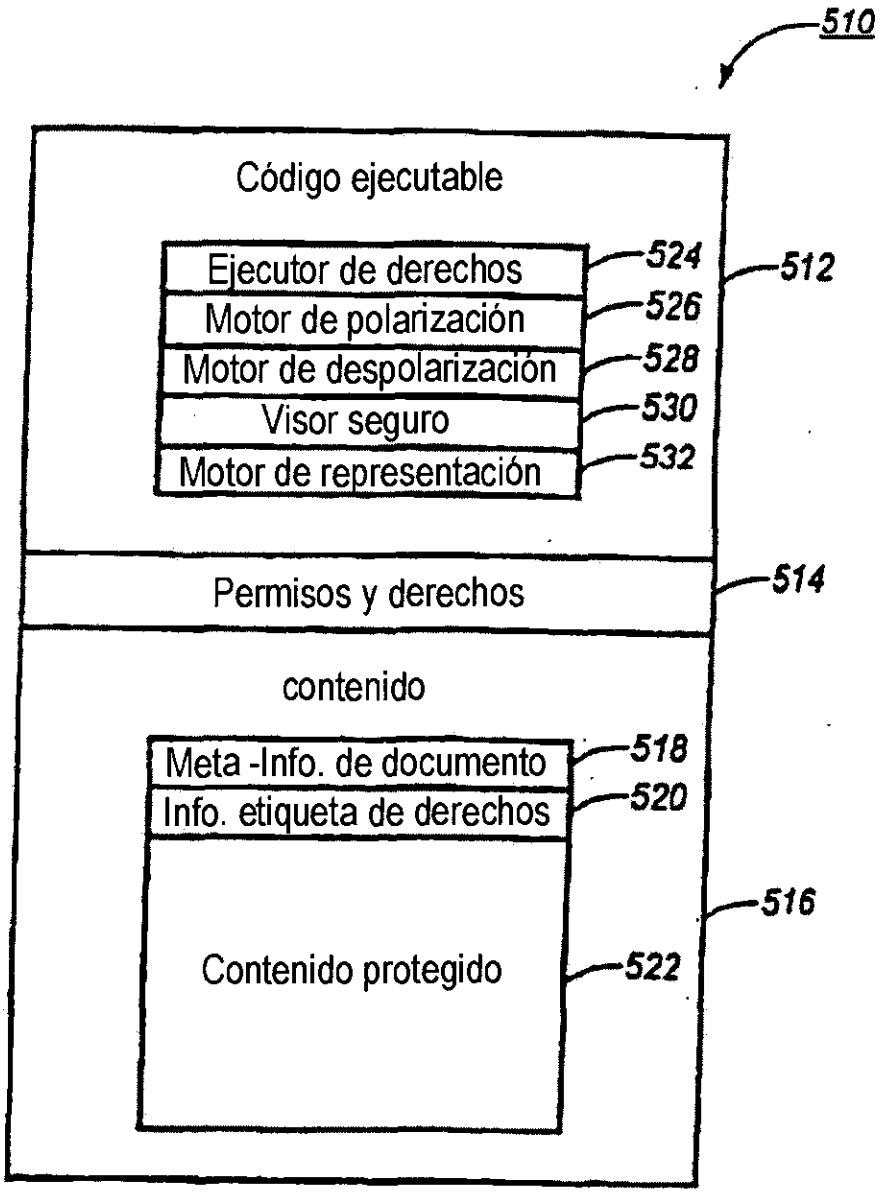

510
Código ejecutable
Ejecutor de derechos
Motor de polarización
Motor de despolarización
Visor seguro
Motor de representación
524
526
528
530
532
512
Permisos y derechos
514
contenido
Meta -Info. de documento
Info. etiqueta de derechos
Contenido protegido
518
520
522
516

FIG. 5

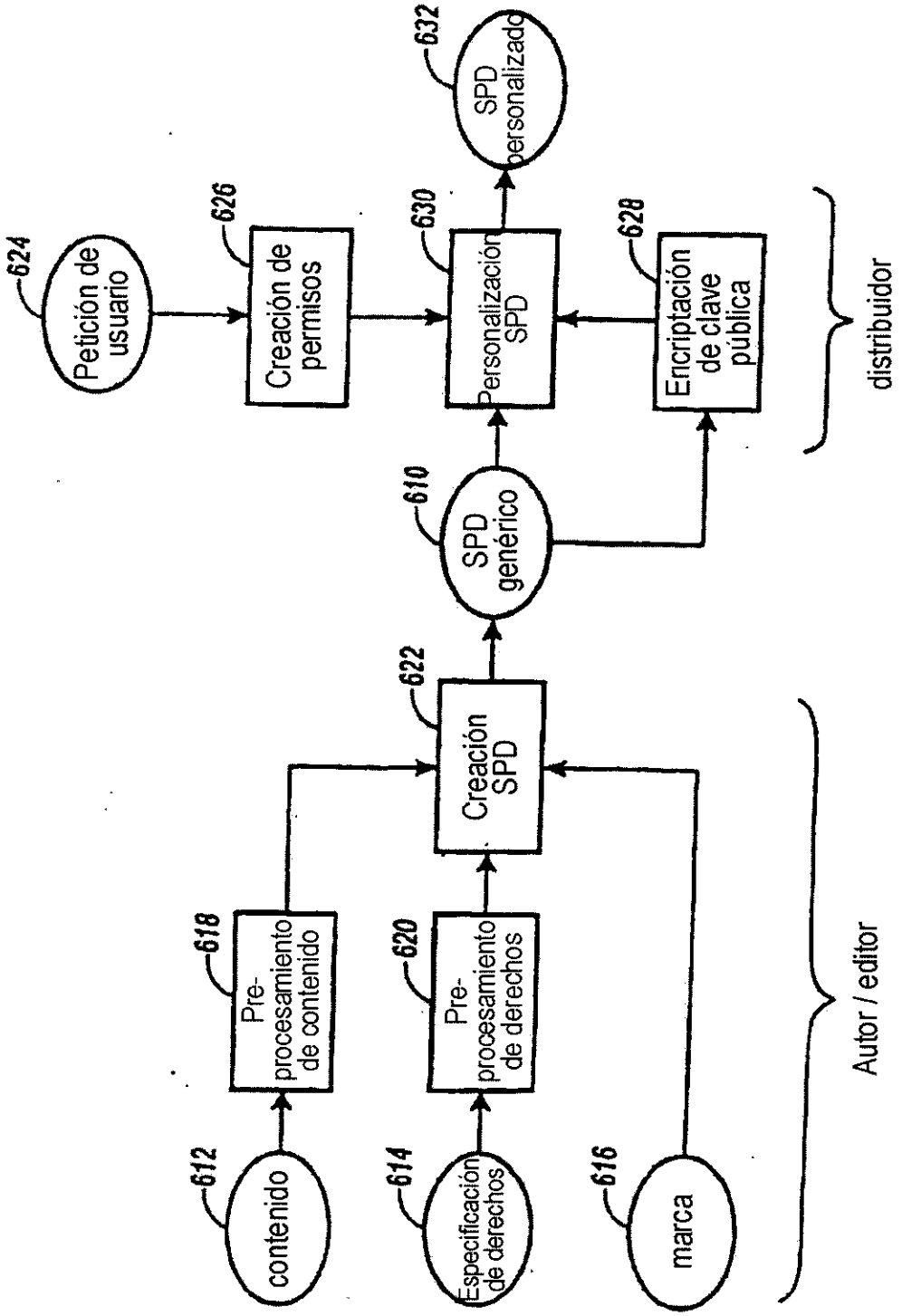

612
contenido
614
Especificación de derechos
616
marca
618
Pre-procesamiento de contenido
620
Pre-procesamiento de derechos
622
Creación SPD
610
SPD genérico
624
Petición de usuario
626
Creación de permisos
630
Personalización SPD
628
Encriptación de clave pública
632
SPD personalizado
Autor / editor
distribuidor

FIG. 6

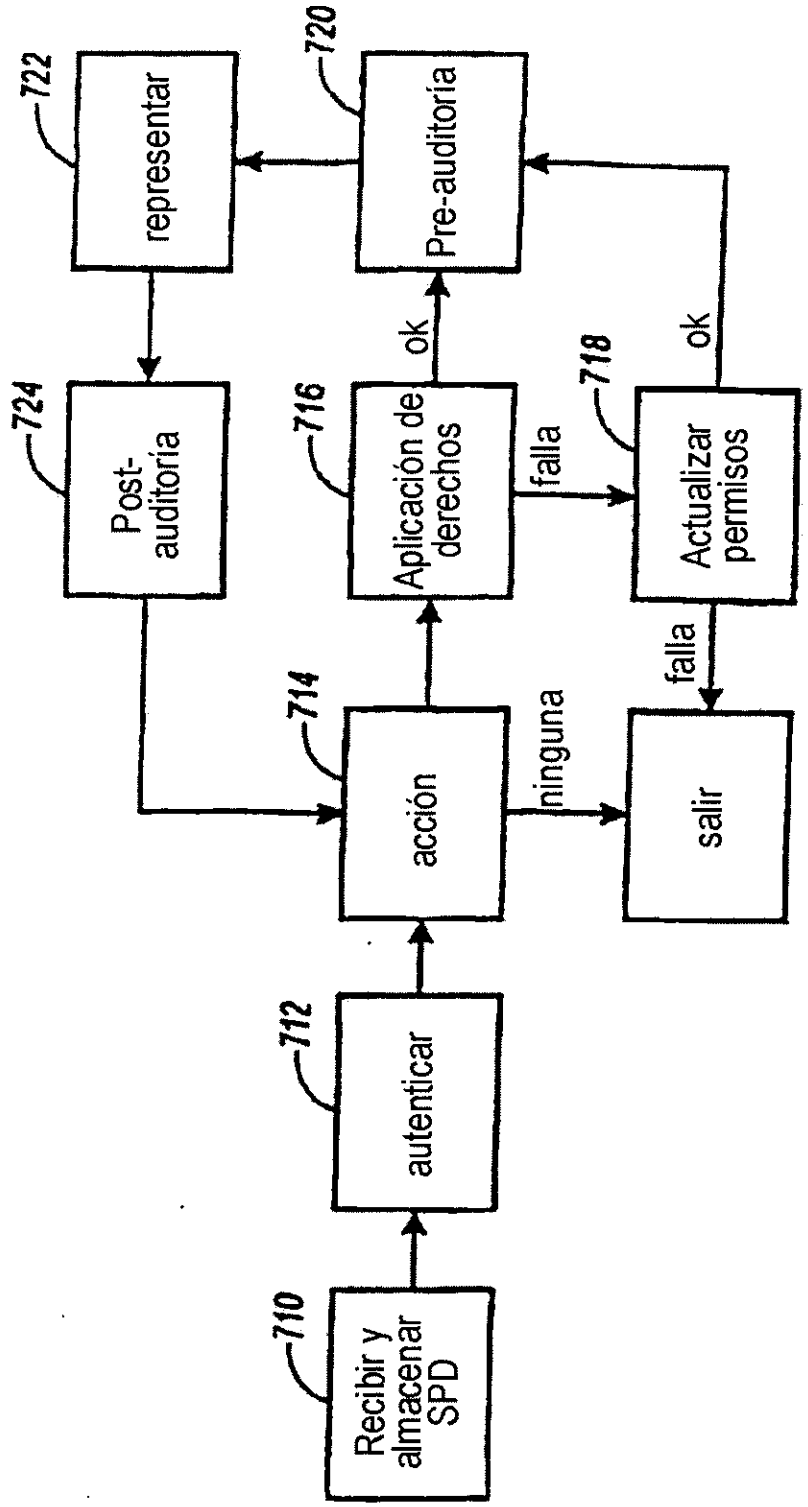

710
Recibir y almacenar SPD
712
autenticar
714
acción
ninguna
salir
falla
716
Aplicación de derechos
ok
falla
718
Actualizar permisos
ok
720
Pre-auditoría
722
representar
724
Post-auditoría

FIG. 7

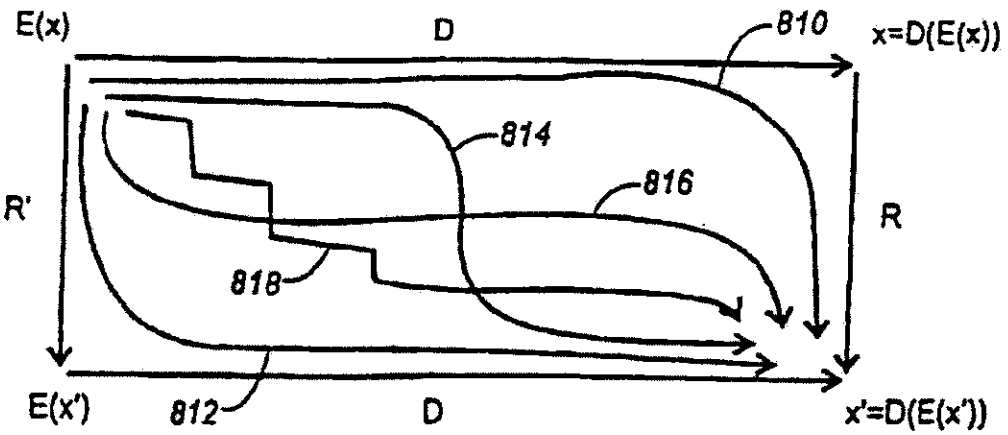

E(x)
D
810
x=D(E(x))
814
816
R'
R
818
E(x')
812
D
x'=D(E(x'))

FIG. 8

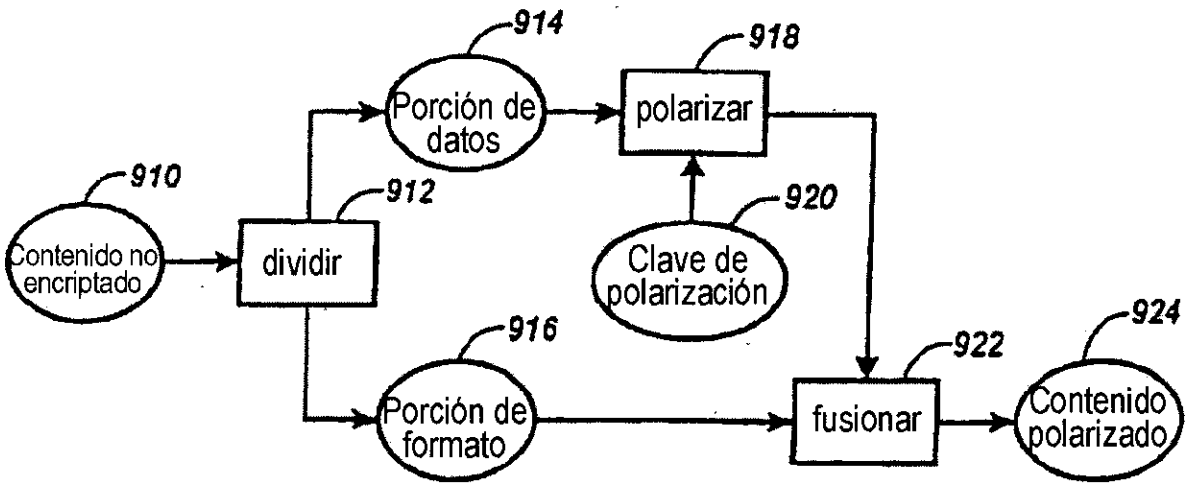

914
Porción de datos
918
polarizar
910
Contenido no encriptado
912
dividir
920
Clave de polarización
916
Porción de formato
922
fusionar
924
Contenido polarizado

FIG. 9

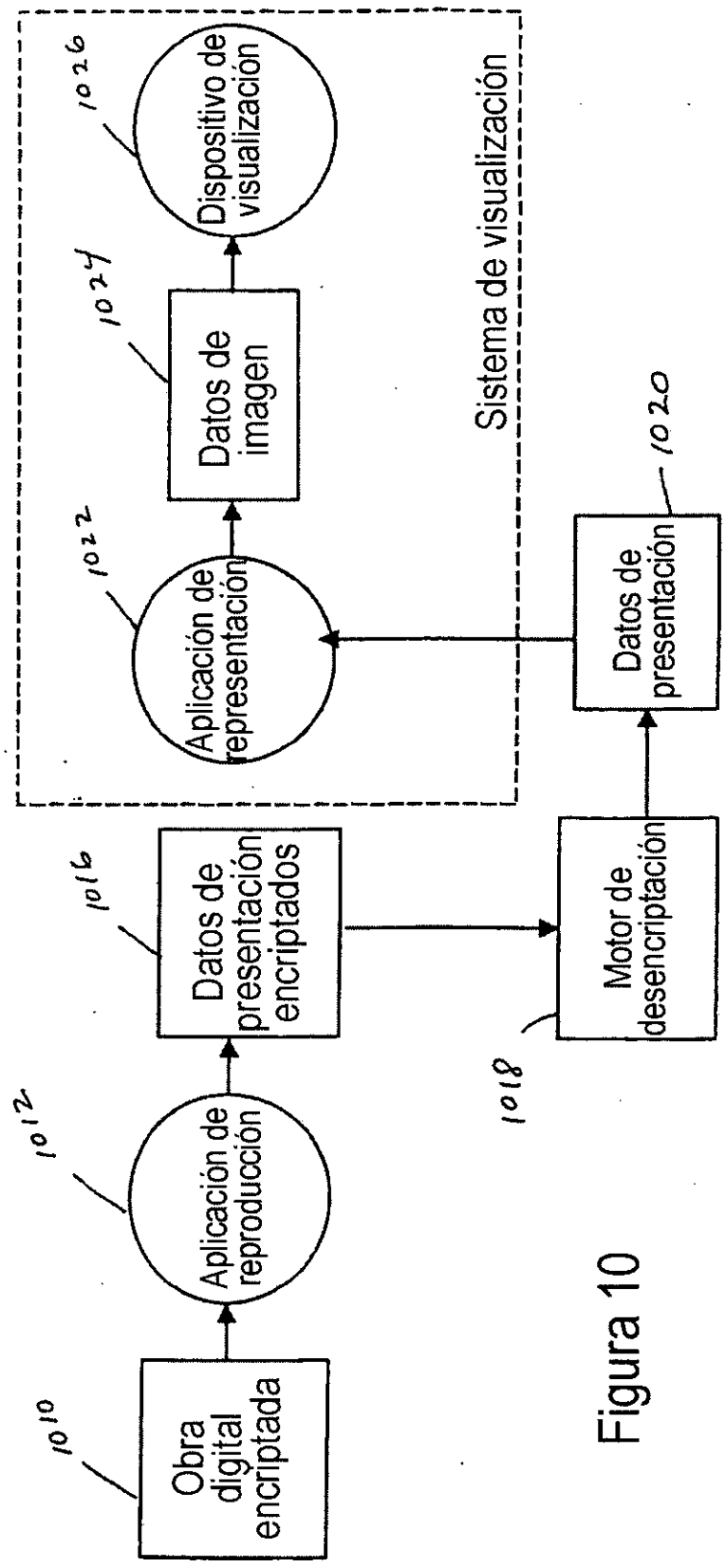

Obra digital encriptada
1010
Aplicación de reproducción
1012
Datos de presentación encriptados
1016
Motor de desencriptación
1018
Datos de presentación
1020
Sistema de visualización
Aplicación de representación
1022
Datos de imagen
1024
Dispositivo de visualización
1026

Figura 10

Figura 11

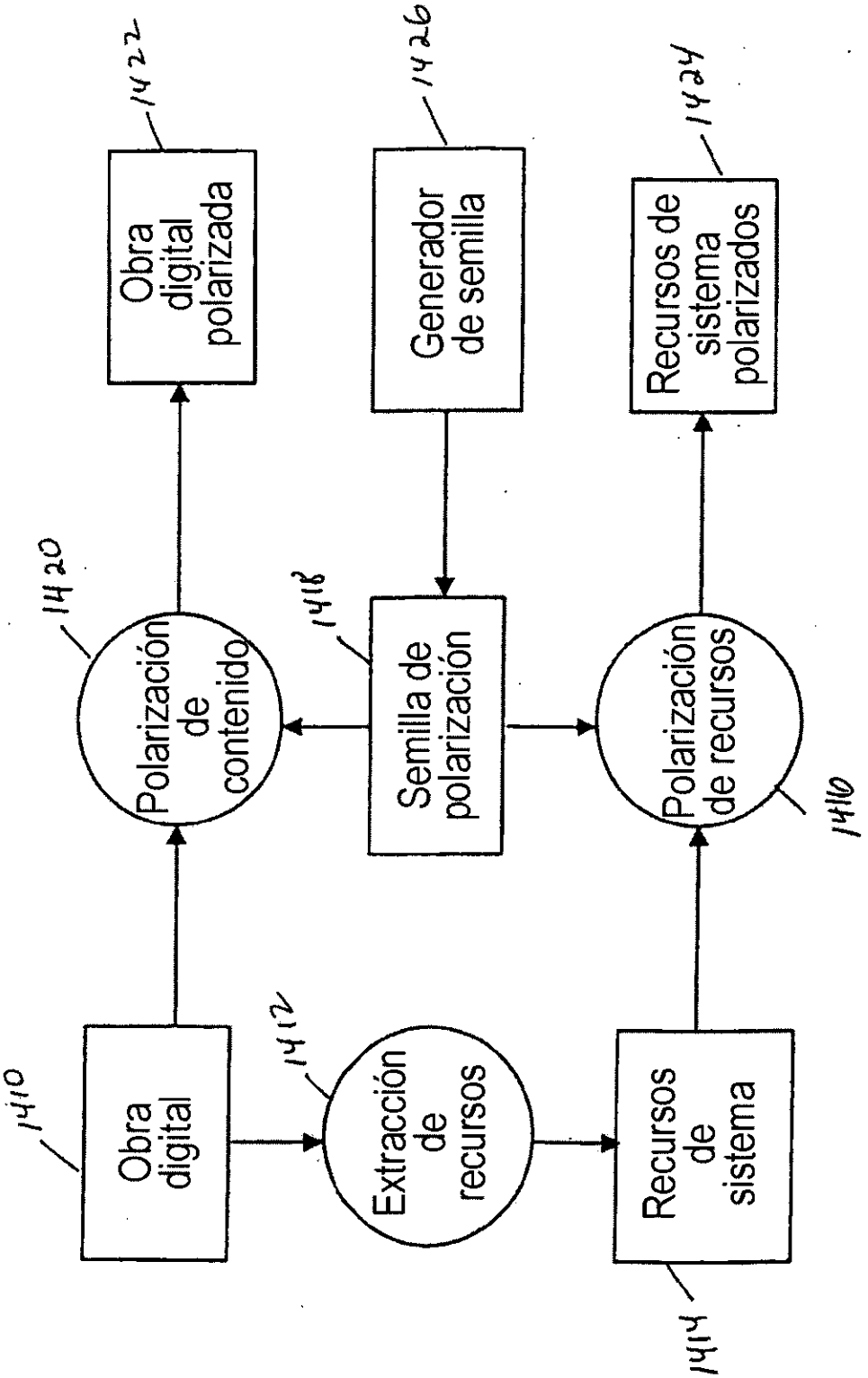
identificador	1000	1001	101	0100	000	001	0101	011	1101	11000	11001	11100	1111	11101
simbolo	l	h	e	d	o	c	u	m	n	p	a	y	x	r

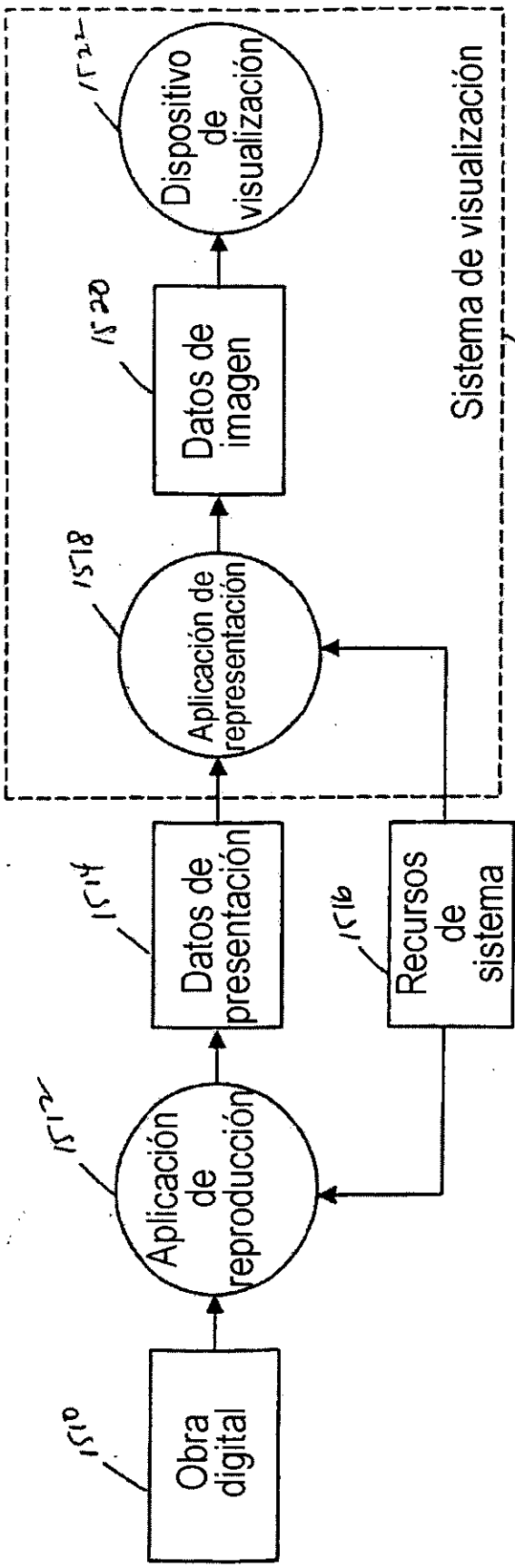
Figura 12

identificador	1000	1001	101	0100	000	001	0101	011	101	1101	1000	001	000	011
x	10	10	10	20	10	10	10	10	10	10	10	20	10	10
y	10	0	0	0	0	0	0	0	0	0	0	0	0	0
identificador	11000	11001	1101	11100	1111	101	11101	000	1111					
x	10	10	10	10	20	10	10	10	10					
y	0	0	0	0	0	0	0	0	0					

Figura 13

Figura 14


1410
Obra digital
1412
Extracción de recursos
1414
Recursos de sistema
1420
Polarización de contenido
1418
Semilla de polarización
1416
Polarización de recursos
1422
Obra digital polarizada
1426
Generador de semilla
1424
Recursos de sistema polarizados



Técnica anterior

Figura 15

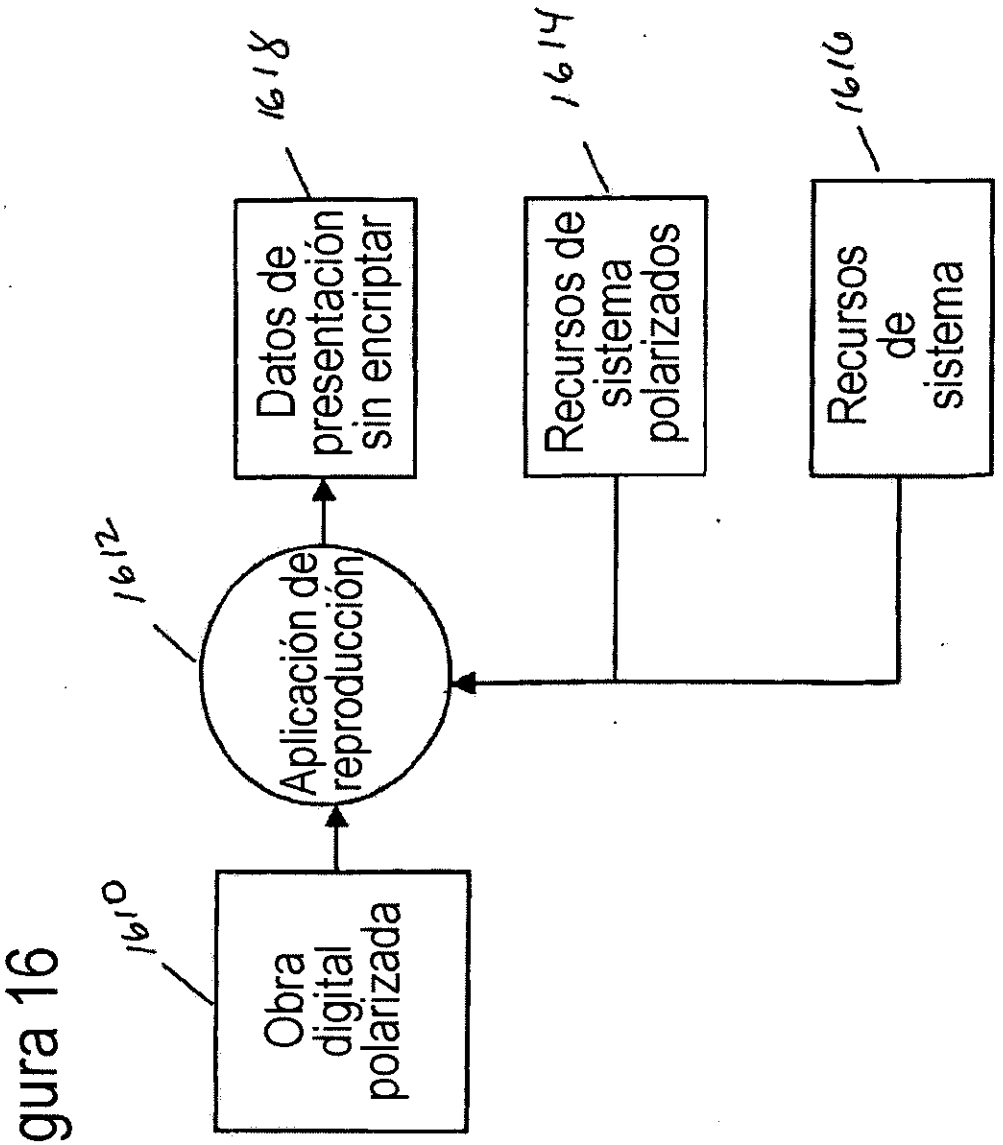
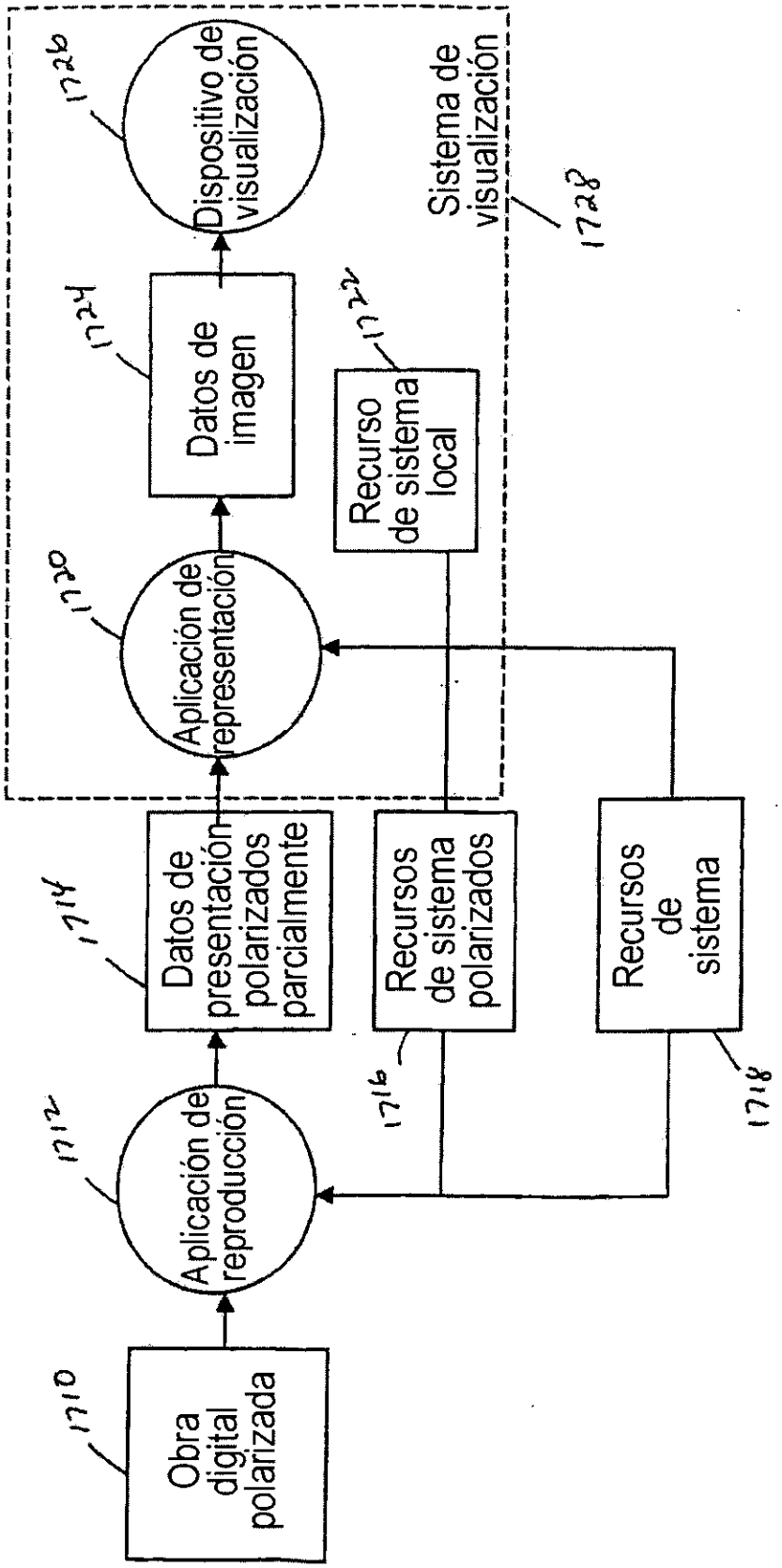

1618
1614
1616
Datos de presentación sin encriptar
Recursos de sistema polarizados
Recursos de sistema
1612
Aplicación de reproducción
1610
Obra digital polarizada

Figura 16

Figura 17


1710
Obra digital polarizada
1712
Aplicación de reproducción
1714
Datos de presentación polarizados parcialmente
1716
Recursos de sistema polarizados
1718
Recursos de sistema
1720
Aplicación de representación
1722
Recurso de sistema local
1724
Datos de imagen
1726
Dispositivo de visualización
1728
Sistema de visualización

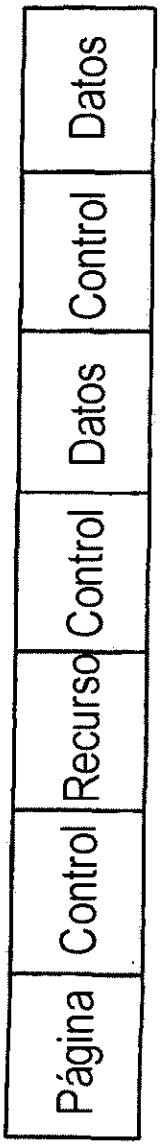


Figura 18

```
<html>
<body>
<font name="Arial" size="14">
Hello World
</font>
<p>
</body>
</html>
```

Figura 19

```
<html>
<body>
<font name="kl3k2" size="21">
v0aa 8 aa0
</font>
<p>
</body>
</html>
```

Figura 20

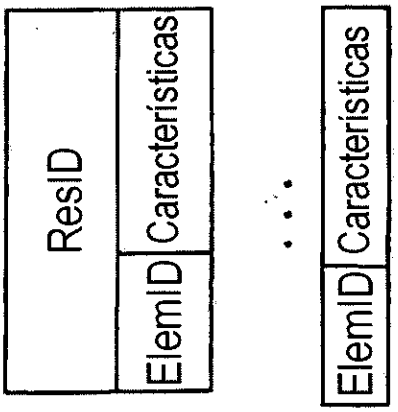
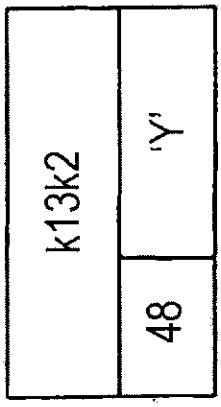


Figura 21



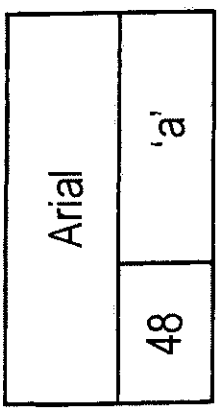


Figura 22

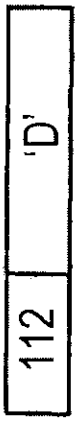


Figura 23