(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 956 359**

(51) Int. CI.:

G06F 21/60 (2013.01)

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(96) Fecha de presentación y número de la solicitud europea: **07.07.2020 E 20184594 (8)**

(97) Fecha y número de publicación de la concesión europea: **06.09.2023 EP 3764264**

(54) Título: **Métodos y dispositivos para el cifrado automático de archivos**

(30) Prioridad:

10.07.2019 US 201916507537

(45) Fecha de publicación y mención en BOPI de la traducción de la patente:
20.12.2023

(73) Titular/es:

BLACKBERRY LIMITED (100.0%)
2200 University Avenue East
Waterloo, Ontario N2K 0A7, CA

(72) Inventor/es:

ADAMS, NEIL PATRICK;
LOMBARDI, ROBERT JOSEPH y
MULAOSMANOVIC, JASMIN

(74) Agente/Representante:

ELZABURU, S.L.P

DESCRIPCIÓN

Métodos y dispositivos para el cifrado automático de archivos

Campo

La presente solicitud se refiere, en general, a la seguridad de datos y, más en particular, a la garantía de la privacidad de datos sensibles.

Antecedentes

Dado que el uso de los dispositivos informáticos cada vez se extiende más en todas las facetas de la vida, los usuarios están optando, cada vez más, por dispositivos informáticos móviles tanto para actividades personales como para actividades comerciales. Dichas actividades implican, con frecuencia, la creación y/o el guardado de varios tipos de archivos como, por ejemplo, un fanático de los deportes que toma una foto con su teléfono inteligente, o un empleado bancario que descarga un documento financiero en su tableta. En algunos casos, se crean y/o guardan archivos de naturaleza sensible o confidencial (tanto personales como comerciales). En algunos dispositivos, es posible cifrar archivos sensibles almacenados en el dispositivo.

El documento US2016078245A1 describe sistemas de almacenamiento de datos para generar, de forma automática, normas de cifrado según un conjunto de archivos de capacitación que se sabe que incluyen información sensible. El sistema puede usar una cantidad de algoritmos heurísticos para generar una o más normas de cifrado para determinar si un archivo incluye información sensible. Además, el sistema puede aplicar los algoritmos heurísticos al contenido de los archivos, según lo determinado por el uso de algoritmos de procesamiento de lenguaje natural, para generar las normas de cifrado. Además, se describen sistemas que pueden determinar, de forma automática, si cifrar un archivo según las normas de cifrado generadas. El contenido del archivo puede determinarse usando algoritmos de procesamiento de lenguaje natural y luego las normas de cifrado pueden aplicarse al contenido del archivo para determinar si cifrar el archivo.

Compendio

Por consiguiente, se provee un dispositivo, un método y un programa de ordenador según se detalla en las reivindicaciones anexas.

Breve descripción de los dibujos

Ahora se hará referencia, a modo de ejemplo, a los dibujos anexos que muestran realizaciones a modo de ejemplo de la presente solicitud, y en los cuales:

la Figura 1 ilustra, en forma de diagrama de bloques, un sistema a modo de ejemplo que incluye un archivo que se está moviendo a una memoria cifrada;

la Figura 2 muestra, en forma de diagrama de flujo, un método a modo de ejemplo de movimiento automático de un archivo a una memoria cifrada;

la Figura 3 muestra, en forma de diagrama de bloques, un dispositivo informático a modo de ejemplo configurado para mover de manera automática un archivo a una memoria cifrada;

la Figura 4 muestra una configuración a modo de ejemplo de un dispositivo informático para cifrar, de manera automática, archivos; y

la Figura 5 muestra, en forma de diagrama de bloques, una arquitectura parcial a modo de ejemplo de un dispositivo informático para cifrar, de manera automática, archivos.

Numerales de referencia similares pueden haberse usado en diferentes figuras para denotar componentes similares.

Descripción de realizaciones a modo de ejemplo

En un primer aspecto, la presente solicitud describe un dispositivo informático. El dispositivo informático incluye un procesador; una memoria; y una aplicación de cifrado automático de archivos almacenada en la memoria y que contiene instrucciones ejecutables por el procesador para cifrar, de manera automática, un archivo. Las instrucciones, cuando se ejecutan por el procesador, hacen que el procesador identifique una característica asociada al contenido probablemente sensible según un patrón de uso de cifrado de archivos que tiene la característica, detecte la creación del archivo, determine que el archivo contiene contenido sensible basado en que tiene la característica, y cifre el archivo según la determinación de que el archivo contiene contenido sensible.

En otro aspecto, la presente solicitud describe un método implementado por ordenador de cifrado automático de un archivo almacenado en un dispositivo informático. El método puede incluir identificar una característica asociada a contenido probablemente sensible según un patrón de uso de cifrado de archivos que tienen la característica; detectar la creación del archivo; determinar que el archivo contiene contenido sensible basado en que tiene la característica; y cifrar el archivo según la determinación de que el archivo contiene contenido sensible.

En un aspecto incluso adicional, la presente solicitud describe un medio de almacenamiento legible por ordenador que almacena instrucciones legibles por procesador que, cuando se ejecutan, configuran un procesador para que lleve a cabo cualquiera de los métodos descritos en la presente memoria. El medio de almacenamiento legible por ordenador puede ser no transitorio. También se describe en la presente solicitud un dispositivo informático que comprende: un procesador, una memoria y una aplicación que contiene instrucciones ejecutables por procesador que, cuando se ejecutan, hacen que el procesador lleve a cabo al menos uno de los métodos descritos en la presente memoria. En este aspecto, el término procesador pretende incluir todos los tipos de circuitos o chips de procesamiento que puedan ejecutar instrucciones de programas.

Otros aspectos y características de la presente solicitud se comprenderán por las personas con experiencia ordinaria en la técnica a partir de una revisión de la siguiente descripción de ejemplos en conjunto con las figuras anexas.

En la presente solicitud, los términos “alrededor de”, “aproximadamente” y “sustancialmente” pretenden cubrir variaciones que pueden existir en los límites superior e inferior de los rangos de valores como, por ejemplo, variaciones en propiedades, parámetros y dimensiones. En un ejemplo no restrictivo, los términos “alrededor de”, “aproximadamente” y “sustancialmente” pueden significar más o menos 10 por ciento o menos.

En la presente solicitud, el término “y/o” pretende cubrir todas las combinaciones y subcombinaciones posibles de los elementos enumerados, incluidos cualesquiera de los elementos enumerados solos, cualquier subcombinación, o todos los elementos, y sin excluir necesariamente elementos adicionales.

En la presente solicitud, la frase “al menos uno/a de...” pretende cubrir uno o más de los elementos enumerados, incluidos cualesquiera de los elementos enumerados solos, cualquier subcombinación, o todos los elementos, sin excluir necesariamente elementos adicionales, y sin requerir necesariamente todos los elementos.

En la presente solicitud, puede hacerse referencia a un “directorio de archivos con seguridad” o a una operación de “creación de directorio de archivos con seguridad”. El término “directorio de archivos con seguridad” se refiere, en general, a una porción de memoria cifrada en la cual pueden colocarse archivos para la protección frente al acceso no autorizado a o la exposición de los archivos. Solo puede accederse a los archivos dentro de la porción de memoria a través del descifrado de los archivos, lo cual requiere pasar una operación de autenticación. La autenticación puede incluir ingresar una frase de paso, datos biométricos, gestos, u otros datos de control de acceso o cualquier combinación. En algunos casos, la autenticación puede ser una autenticación multifactorial. El término “creación de directorio de archivos con seguridad” se refiere, en general, a mover un archivo al “directorio de archivos con seguridad”, a saber, mover un archivo de una porción de memoria no cifrada a la porción de memoria cifrada. De manera más general, la presente solicitud se refiere a “cifrar” un archivo. Se apreciará que “cifrar” un archivo puede incluir mover un archivo de la memoria temporal o una porción no cifrada de la memoria a una porción protegida o cifrada de la memoria, y eliminar cualquier copia del archivo de la memoria temporal o no cifrada.

Según se observa más arriba, muchos usuarios producen o almacenan archivos y documentos en sus dispositivos informáticos, incluidos archivos y documentos de naturaleza privada. Dichos archivos y documentos pueden almacenarse por defecto en un sistema de archivos no seguro por el sistema operativo del dispositivo informático.

Ello ha resultado en una preocupación particular por la seguridad para los usuarios de dichos dispositivos informáticos. Una vulnerabilidad particular surge cuando un nuevo archivo que contiene contenido sensible es creado o añadido por el usuario. Como el nuevo archivo se guarda en el sistema de archivos no cifrado por defecto, es susceptible de un acceso no autorizado. Por consiguiente, algunos dispositivos informáticos proveen la capacidad de cifrar archivos. En algunos casos, ello incluye mover el archivo de la porción no cifrada de la memoria, p. ej., sistema de archivos, a una porción de memoria cifrada, p. ej., un directorio de archivos con seguridad. En este sentido, el movimiento puede incluir copiar el archivo de la memoria no cifrada a la memoria cifrada y eliminar o borrar la copia en la memoria no cifrada. Un usuario que desea proteger archivos frente al acceso no autorizado puede protegerlos moviéndolos al directorio de archivos con seguridad.

Incluso si el dispositivo informático provee al usuario la funcionalidad de mover manualmente el archivo a un directorio de archivos con seguridad cifrado, una vulnerabilidad adicional surge en que el usuario puede descuidar la protección de archivos sensibles. El cifrado automático de todos los archivos puede provocar una carga y un retraso computacionales innecesarios cuando la mayoría de los archivos no requieren niveles elevados de control de acceso. Partes maliciosas pueden, de manera activa, buscar archivos confidenciales tanto personales como comerciales.

Por consiguiente, según un aspecto de la presente solicitud, se describe una aplicación de cifrado automático de archivos. La aplicación de cifrado automático de archivos es una aplicación implementada por software que cifra un archivo que se ha determinado que contiene contenido sensible, por ejemplo, copiándolo a un directorio de archivos con seguridad cifrado y eliminando la copia no cifrada. Lleva a cabo esto, en una implementación a modo de ejemplo,

determinando que el archivo contiene contenido sensible según una característica del archivo. La característica puede identificarse según un patrón de uso en el cual otros archivos que tienen la misma característica se han cifrado previamente. En un ejemplo, el patrón de uso se basa en el historial del usuario de movimiento de archivos al directorio de archivos con seguridad en el dispositivo informático. En otro ejemplo, el patrón de uso se basa en el historial de otros usuarios de movimiento de archivos a sus respectivos directorios de archivos con seguridad en sus respectivos dispositivos informáticos.

En algunas implementaciones, la característica puede ser metadatos asociados al archivo. Es decir, puede ser una característica del archivo identificable a través de metadatos como, por ejemplo, una hora o fecha de creación, una ubicación de creación, etc. En incluso otras implementaciones, la característica puede incluir contenido del archivo como, por ejemplo, características identificables dentro de una imagen o mensaje o documento.

Más de una característica puede incluirse en la determinación de que un archivo contiene contenido sensible. Por ejemplo, la determinación de que un archivo contiene contenido probablemente sensible puede basarse en una combinación de ubicación y hora asociadas a la creación del archivo. A modo de ilustración, puede determinarse que una imagen que tiene las características de que se captura en la ubicación de un club nocturno o bar entre las 23:00 y las 3:00 contiene contenido probablemente sensible.

Primero se hace referencia a la Figura 1, que ilustra un sistema 10 a modo de ejemplo que incluye un sistema 12 operativo que tiene un sistema 14 de archivos por defecto y un directorio 16 de archivos con seguridad. El sistema 12 operativo puede ser cualquier sistema operativo adecuado como, por ejemplo, el sistema operativo Android™, por ejemplo. La presente solicitud no se encuentra limitada a un sistema operativo particular siempre que el sistema operativo provea acceso a un sistema de archivos cifrado además de a un sistema de archivos no cifrado por defecto. El sistema 14 de archivos por defecto puede incluir un sistema de archivos no cifrado donde se guardan y/o almacenan los archivos 18 que se crean o añaden inicialmente. Por ejemplo, un usuario que crea un archivo de foto tomando una foto con su teléfono inteligente almacena el archivo, por defecto, en el almacenamiento interno o tarjeta de memoria del teléfono inteligente. A modo de un ejemplo adicional, un usuario que añade un documento financiero a su ordenador portátil (creándolo o descargándolo) almacena el documento, por defecto, en el disco duro interno o externo del ordenador portátil.

El directorio 16 de archivos con seguridad puede incluir un sistema de archivos cifrado que garantiza el acceso a los archivos 20 allí cifrados. Como se muestra en la Figura 1, el directorio 16 de archivos con seguridad puede ser un directorio de archivos con seguridad local basado en el disco. Dicho directorio de archivos con seguridad local puede ser, por ejemplo, un volumen separado o unidad lógica en el mismo disco bajo control del sistema 12 operativo. En el caso de un directorio de archivos con seguridad local, el acceso a los archivos 20 cifrados allí almacenados puede asegurarse por medio de mecanismos de seguridad comunes como, por ejemplo, una contraseña, una huella dactilar, u otro dato biométrico. El directorio 16 de archivos con seguridad puede también ser un directorio de archivos con seguridad basado en la nube como, por ejemplo, un servicio de almacenamiento seguro/cifrado alojado de manera remota. En el caso de un directorio de archivos con seguridad basado en la nube, el dispositivo informático del usuario puede comunicarse con el directorio de archivos con seguridad basado en la nube usando su módulo de comunicaciones (según se describe en mayor detalle con relación a la Figura 3), y puede requerir autenticación con el fin de acceder a los archivos almacenados.

Según se ilustra, los archivos 18 son archivos que se han creado o añadido en el sistema 12 operativo y, por defecto, se almacenan en el sistema 14 de archivos por defecto. Los archivos 18 pueden ser de cualquier tipo compatible con el sistema 12 operativo como, por ejemplo, archivos multimedia, archivos de mensajes o archivos de documentos. Los archivos multimedia pueden incluir uno o más de una imagen, una foto, un vídeo, un fragmento de audio y similares. Los archivos de mensajes pueden incluir uno o más de un correo electrónico, un mensaje de texto (SMS, por sus siglas en inglés), una conversación con mensajes instantáneos (IM, por sus siglas en inglés), y similares. Los archivos de documentos pueden incluir uno o más de un documento de texto, una hoja de cálculo, una presentación, un PDF (formato de documentos portátiles, PDF, por sus siglas en inglés) y cualquier otro tipo de documento. La presente solicitud no se encuentra limitada a un tipo de archivo particular y cualquier archivo que provea sus metadatos u otros atributos a su sistema operativo anfitrión es adecuado.

En la implementación a modo de ejemplo de la Figura 1, los archivos 18 almacenados en el sistema 14 de archivos por defecto se han colocado allí por defecto tras su creación o adición al sistema. Algunos de los archivos 18 pueden contener contenido sensible que un usuario desea mantener en privado. El archivo 22 confidencial es tal archivo, en el presente ejemplo. Sin embargo, el sistema 10 se configura de modo tal que identifica, de manera automática, el archivo 22 como uno que contiene contenido sensible sin acción o entrada del usuario y mueve 24, de manera automática, el archivo 22 confidencial del sistema 14 de archivos por defecto al directorio 16 de archivos con seguridad según la determinación de que el archivo 22 confidencial probablemente contenga contenido sensible. Detalles a modo de ejemplo de dicha determinación se describen más abajo.

Ahora se hace referencia a la Figura 2, que muestra un método 200 a modo de ejemplo del cifrado automático de un archivo. El método 200 puede, por ejemplo, llevarse a cabo por una aplicación de cifrado automático de archivos que funciona en un dispositivo informático. El dispositivo informático puede incluir un dispositivo móvil en algunas implementaciones. En algunas implementaciones, el dispositivo informático puede incluir una tableta, reloj inteligente,

teléfono inteligente, lector de libros electrónicos, ordenador personal, ordenador portátil, o cualquier otro dispositivo informático.

En la operación 202, se identifica una característica que se asocia a contenido probablemente sensible según operaciones de cifrado de archivos previas. Es decir, se identifica un patrón de uso por medio del cual otros archivos que tienen la misma característica se han cifrado. El cifrado de los otros archivos puede haber ocurrido a través de la instrucción del usuario en algunas implementaciones. Por consiguiente, según un historial de cifrado de archivos que tienen la característica, la característica se identifica como asociada a contenido probablemente sensible.

Según se describe más arriba, la característica puede incluir una característica encontrada en metadatos asociados al archivo. La característica puede también, o de manera alternativa, incluir contenido del archivo, incluidas características detectadas, palabras clave, etc. La característica puede incluir dos o más características en combinación. Características a modo de ejemplo se describen más arriba y más abajo.

En una realización a modo de ejemplo, el patrón de uso se obtiene de operaciones previas de cifrado llevadas a cabo en el dispositivo móvil. En un ejemplo, el patrón de uso se basa en un historial de archivos que el dispositivo móvil ha movido previamente a su memoria cifrada en respuesta a configuraciones o instrucciones del usuario. Mediante el análisis de dichos archivos previamente cifrados, el dispositivo móvil identifica una característica común de los archivos indicativa de contenido probablemente sensible.

La identificación puede además basarse en la determinación de que los archivos previamente cifrados tienen la característica y de que los archivos previamente no cifrados no tienen la característica. Es decir, una característica que es común a los archivos cifrados puede no ser indicativa de contenido probablemente sensible a menos que dicha característica también esté ausente en archivos que se han creado y almacenado en la memoria no cifrada pero que no se han movido al directorio de archivos con seguridad.

La identificación puede incluir determinar si una de múltiples características candidatas está presente en los archivos previamente cifrados. Ciertas características pueden identificarse con antelación como características candidatas, de modo que la identificación de una característica incluye buscar una de las características candidatas en el patrón de uso. A modo de ejemplo, características de imagen de cosas sensibles conocidas como, por ejemplo, imágenes de una pizarra blanca, alcohol, desnudez, información o documentos de identificación personal, etc., pueden ser características candidatas que están disponibles para su identificación como una característica común a archivos previamente cifrados. Por el contrario, ciertas características pueden excluirse como características candidatas. Por ejemplo, en el caso de la ubicación asociada a un archivo, un lugar de trabajo asociado a un usuario puede excluirse sobre la base de que es una ubicación muy común para la creación del archivo que no puede indicar sensibilidad. Por otro lado, para un usuario en una posición sensible que tiene un lugar de trabajo con restricciones de confidencialidad, la ubicación del lugar de trabajo puede ser indicativa de contenido probablemente sensible. A modo de otro ejemplo, la hora de creación puede excluirse como una característica a menos que la hora de creación sea una hora inusual o inesperada como, por ejemplo, entre las 22:00 y las 6:00.

En la invención, el patrón de uso se basa en operaciones previas de cifrado llevadas a cabo en otros dispositivos informáticos. Es decir, el patrón de uso puede “reclutarse”, en el sentido de que un patrón de otros usuarios que eligen cifrar archivos que tienen una característica lleva a la identificación de la característica como una asociada a contenido probablemente sensible. Por ejemplo, el patrón de uso puede indicar que un gran porcentaje de usuarios que capturan una imagen en cierta ubicación eligen cifrar dicha imagen. En dicho caso, el patrón de uso puede indicar que la ubicación es una característica asociada a contenido sensible.

En el caso de patrones de uso reclutados, en una implementación, la identificación de la característica puede llevarse a cabo por el dispositivo móvil según información recibida de otros dispositivos informáticos con respecto a su actividad de cifrado de archivos, ya sea de forma directa o mediante un servidor. En la invención, la identificación de la característica puede llevarse a cabo por un servidor que analiza el patrón de uso según información que el servidor recibe de los otros dispositivos informáticos con respecto a su actividad de cifrado. El servidor entonces provee al dispositivo móvil datos relativos a la característica para permitir que el dispositivo móvil lleve a cabo el resto del método 200. Se apreciará que, en el caso de la identificación de característica reclutada, el archivo real previamente cifrado puede no proveerse, por motivos de privacidad, al servidor o al dispositivo móvil. En su lugar, los otros dispositivos móviles pueden enviar metadatos y/o información de contenido relativa a los archivos previamente cifrados al servidor, y el servidor puede entonces determinar la característica a partir de las similitudes entre metadatos o información de contenido provistos por los otros dispositivos móviles.

Después de haber identificado una característica, dicha característica puede entonces usarse por el dispositivo móvil para identificar si deben cifrarse otros archivos, p. ej., almacenarse en memoria cifrada. Se apreciará que la(s) característica(s) puede(n) ser información sensible y que el almacenamiento de las características en el dispositivo móvil puede ser un riesgo de seguridad en sí mismo. Con respecto a ello, las características pueden almacenarse en forma cifrada y pueden descifrarse cuando se evalúa si un nuevo archivo debe colocarse en el directorio con seguridad o no. En algunas implementaciones, las características pueden trocearse para protegerse frente a su divulgación. Se apreciará que, en dicha implementación, las características de un nuevo archivo pueden entonces necesitar trocearse para ver si concuerdan con características troceadas almacenadas, aunque el troceado puede no ser efectivo cuando

se evalúa si una característica como hora o ubicación cae dentro de un rango definido que se correlaciona con datos sensibles que deben cifrarse.

Con referencia aún a la Figura 1, luego de haber identificado la característica asociada al contenido probablemente sensible, el dispositivo móvil entonces detecta la creación de un archivo en la operación 204. La creación puede incluir detectar un archivo recientemente creado generado en el dispositivo móvil como, por ejemplo, captura de una nueva imagen, vídeo de grabación de audio, y puede incluir detectar un archivo recientemente añadido. Archivos recientemente creados pueden incluir, por ejemplo, una nota de voz grabada en un reloj inteligente, un mensaje enviado desde un dispositivo médico personal, etc. Archivos recientemente añadidos pueden incluir, por ejemplo, recibir un videoclip compartido con un teléfono inteligente mediante un enlace inalámbrico, recibir un historial de uso en un televisor inteligente enviado por un proveedor de servicios, etc. La detección de un archivo recientemente creado o añadido puede implicar que el dispositivo informático escanee de manera periódica su sistema de archivos por defecto. De manera adicional, o alternativa, el dispositivo informático puede proveer notificación en tiempo real de un archivo recientemente creado o añadido. En una implementación a modo de ejemplo, la detección incluye escanear archivos recientemente creados o añadidos de uno o más tipos de archivo especificados (a saber, solo ciertos tipos de archivo relevantes pueden especificarse) que pueden tener el beneficio de reducir la carga de procesamiento en el dispositivo informático.

En la operación 206, el dispositivo informático determina que el archivo contiene contenido sensible basado en que este tiene la característica identificada en la operación 202. En base a ello, en la operación 208, el dispositivo informático entonces cifra el archivo de manera automática, sin intervención o instrucción alguna del usuario. Por ejemplo, puede mover el archivo al espacio de memoria cifrada, a saber, el directorio de archivos con seguridad, copiando el archivo en la memoria cifrada y eliminando la copia de la memoria no cifrada.

Según se describe más arriba, la característica indicativa de contenido sensible se identifica según un patrón de uso de archivos previamente cifrados que tienen la característica. La característica puede incluir metadatos para el archivo como, por ejemplo, datos de geoubicación, y fecha y/o datos de marca de tiempo. Por ejemplo, la característica puede incluir la ubicación en la cual se crea una foto, vídeo o grabación de audio. La ubicación puede determinarse, por ejemplo, según metadatos asociados al archivo. Los metadatos pueden almacenarse con el archivo, por ejemplo, en un encabezado u otra estructura de datos. En un ejemplo, los metadatos pueden asociarse al archivo por una aplicación de cámara que recibe datos de ubicación de un chip GPS en algunos ejemplos. Puede considerarse que fotos que se han tomado en ubicaciones dentro de una distancia umbral entre sí tienen la misma característica, en algunos ejemplos.

También se apreciará que la identificación de una característica puede basarse en cierto porcentaje de archivos previamente cifrados del mismo tipo que tienen la característica o combinación de características. A modo de ejemplo, si el usuario cifra imágenes creadas en una ubicación particular dentro de una ventana de tiempo de tres horas particular el 80% de las veces, entonces dicha combinación de ubicación y tiempo puede considerarse una característica de contenido probablemente sensible. De manera similar, si cierto porcentaje, p. ej., 50%, de otros usuarios que toman imágenes en una ubicación particular (o dentro de una distancia umbral de dicha ubicación) cifran dichas imágenes, entonces la ubicación puede ser característica de contenido probablemente sensible.

En algunas implementaciones, la característica incluye contenido del archivo. Contenido del archivo puede incluir, en el caso de una foto o vídeo, una característica detectada en la foto o vídeo. Características a modo de ejemplo detectadas en una imagen o vídeo pueden incluir caras humanas, una persona específica identificada a través del reconocimiento facial, desnudez o potencial contenido sexual, alcohol, o información o documentos de identificación personal, o cualquier otra característica que pueda detectarse en una imagen o vídeo y que pueda clasificarse como potencialmente sensible. Por ejemplo, contenido laboral sensible puede indicarse por la detección de una pizarra blanca, que puede contener escritura confidencial. Contenido de un archivo de texto puede incluir palabras clave como, por ejemplo “secreta/o(s)” o “confidencial(es)”. Cuando se trata de la detección de características, las características identificadas pueden clasificarse según algoritmos de detección de características y ciertas clases pueden categorizarse como potencialmente sensibles. Ello evitará encontrar una “característica” en archivos previamente cifrados que pueden ser comunes a los archivos, pero no se correlaciona, en realidad, con el deseo de cifrar los archivos como, por ejemplo, características ordinarias y comunes, como una calzada, muebles, árboles, automóviles, o similares.

Según se describe más arriba, el archivo puede ser de varios tipos de archivo, y las características del archivo que son características candidatas para establecer un patrón de uso pueden depender del tipo de archivo. Por ejemplo, en el caso de un archivo multimedia, como una imagen, vídeo o grabación de audio, las características candidatas pueden incluir uno o más de: una identidad de una persona (p. ej., amante); la presencia de un objeto (p. ej., bebida alcohólica); y un atributo de una persona u objeto (p. ej., porcentaje de piel que se ve). A modo de otro ejemplo, si el archivo es uno de varios archivos de mensajes, entonces las características candidatas pueden incluir uno o más de: una identidad de un emisor o receptor (p. ej., emisor de correo electrónico jefe de agencia de espionaje); un rango de fechas y/o marca de tiempo (p. ej., viernes o sábado por la noche después de las 10 p. m.), la presencia de texto especificado (p. ej., “ultrasecreto”); la presencia de un adjunto (p. ej., foto o vídeo); una identidad de una persona en un adjunto; la presencia de un objeto en un adjunto; y un atributo de una persona u objeto en un adjunto. En incluso un ejemplo adicional, el archivo puede ser uno de varios tipos de archivos de documentos, en cuyo caso la

característica candidata puede incluir uno o más de: un título o etiqueta especificada (p. ej., Proyecto X); y la presencia de texto especificado (p. ej., “Solo para sus ojos”).

Ahora se hace referencia a la Figura 3, que ilustra un dispositivo 300 informático a modo de ejemplo que implementa una aplicación 330 de cifrado automático de archivos. El dispositivo 300 informático incluye un procesador 302, que puede incluir una o más unidades de procesamiento, y una memoria 304. El dispositivo 300 informático además incluye un sistema 314 de archivos por defecto y un directorio 316 de archivos con seguridad. La memoria 304 almacena un sistema 312 operativo y aplicaciones 306. El sistema 312 operativo y las aplicaciones 306 contienen instrucciones ejecutables por procesador que, cuando se ejecutan por el procesador 302, configuran el procesador 302 para que lleve a cabo las operaciones descritas. Las aplicaciones 306 pueden incluir la aplicación 330 de cifrado automático de archivos. La aplicación 330 de cifrado automático de archivos, almacenada en la memoria 304, hace que el procesador 302 detecte un archivo recientemente creado o añadido en el sistema 314 de archivos por defecto. La aplicación 330 de cifrado automático de archivos entonces hace que el procesador 302 determine que el archivo contiene contenido sensible según las características del archivo, y cualquier patrón previamente identificado en determinaciones guardadas. La memoria 304 puede además guardar la determinación de que el archivo contiene contenido sensible, incluidas las características del archivo. Finalmente, la aplicación 330 de creación de directorio de archivos automática hace que el procesador 302 cifre el archivo, por ejemplo, moviendo el archivo a un directorio 316 de archivos con seguridad cifrado. El dispositivo 300 informático puede además incluir una visualización 308 y un módulo 310 de comunicaciones. La visualización 308 puede mostrar al usuario una interfaz gráfica de usuario (GUI, por sus siglas en inglés) como parte de la aplicación 330 de cifrado automático de archivos. Dicha GUI puede permitir al usuario interactuar con la aplicación 330 de cifrado automático de archivos con el fin de establecer ciertas preferencias como, por ejemplo, características de un archivo que indican que este contiene contenido sensible, o tipos de archivo especificados para incluir en el escaneado por la aplicación. Según se ha descrito previamente, el módulo 310 de comunicaciones puede facilitar la comunicación con un directorio de archivos con seguridad basado en la nube y, de manera específica, el movimiento de archivos que se ha determinado que contienen contenido sensible a un directorio de archivos con seguridad basado en la nube. La comunicación y transferencia de archivos entre el módulo 310 de comunicaciones y el directorio de archivos con seguridad basado en la nube puede tener lugar en cualquier enlace adecuado como, por ejemplo, Internet.

Ahora se hace referencia a la Figura 4 que muestra, en forma de diagrama de bloques, una configuración a modo de ejemplo de un dispositivo 400 informático para cifrar, de manera automática, archivos. En el presente ejemplo, una aplicación de cifrado gestiona el cifrado y descifrado manuales o automáticos de archivos en el dispositivo 400 informático. Los archivos se almacenan en una porción de memoria de zona protegida, a veces llamada un “directorio 402 de archivos con seguridad”. Los archivos en el directorio 402 de archivos con seguridad se almacenan en forma cifrada, como se indica por los archivos 404 cifrados. Cada archivo 404 cifrado en el presente ejemplo se cifra con su propia clave de cifrado única. La clave de cifrado puede generarse usando un método de clave simétrica en algunos casos. En el presente ejemplo, la clave de cifrado es una clave AES (estándar de cifrado avanzado, AES, por sus siglas en inglés) de una longitud de clave adecuada. Otros mecanismos de cifrado o tipos de clave pueden usarse en otras implementaciones.

El dispositivo 400 informático puede incluir una base 406 de datos de protección de medios que almacena registros de archivos en el directorio 402 de archivos con seguridad. En particular, los registros pueden incluir, en algunos ejemplos, un identificador único, un nombre de archivo cifrado, un nombre de archivo real, una ubicación o fuente original, y la clave AES. La clave AES puede, en sí misma, almacenarse en el registro en forma cifrada. La clave puede cifrarse con un enlace vinculado a la contraseña global para el directorio 402 de archivos con seguridad. La clave para cifrar la clave AES puede ser una clave pública parte de un par de claves pública-privada asimétricas.

La aplicación de cifrado que regula el acceso al directorio 402 de archivos con seguridad puede incluir un par de claves asimétricas asociadas al bloqueo y desbloqueo del directorio 402 de archivos con seguridad. El par de claves asimétricas puede vincularse a una contraseña que puede ingresarse por el usuario, ya sea a través de una frase de pase, datos biométricos, un gesto, o en cualquier otro esquema de autenticación, incluida la autenticación multifactorial. La clave pública del par de claves asimétricas puede usarse para bloquear información en la base 406 de datos de protección de medios. El ingreso de la contraseña puede permitir la generación de la clave privada para permitir el desbloqueo de la base 406 de datos de protección de medios y sus registros y, por lo tanto, la recuperación de la clave AES simétrica para descifrar uno de los archivos 404 cifrados. La aplicación de cifrado puede incluir un gestor 408 de claves para gestionar las claves y, en particular, para obtener la clave AES de un registro en la base 406 de datos de protección de medios y descifrar y acceder a un archivo correspondiente de los archivos 404 cifrados.

La aplicación de cifrado puede también estar implicada en el cifrado de archivos recientemente creados, ya sea a través de una instrucción de usuario manual o cifrado automático como se describe más arriba. Por ejemplo, en el caso del cifrado automático, la aplicación de cifrado puede reconocer o recibir una instrucción externa para cifrar un archivo particular. En respuesta, puede generar, por ejemplo, a través del gestor 408 de claves, una nueva clave AES. Puede además obtener la clave pública asimétrica, que puede almacenarse en la memoria y ser accesible para el gestor 408 de claves. La aplicación de cifrado puede provocar el cifrado del archivo recientemente creado como un nuevo archivo 404 cifrado, y su almacenamiento en el directorio 402 de archivos con seguridad. También puede provocar la eliminación de cualquier versión no cifrada del archivo, si la hubiera, ubicada en cualquier otro lugar en una memoria persistente o temporal. La aplicación de cifrado puede además provocar la creación de un nuevo registro

en la base 406 de datos de protección de medios, el nuevo registro conteniendo detalles sobre el archivo recientemente creado y, en particular, la clave AES para descifrar el archivo. Dicha clave AES, o todo o parte del registro que contiene la clave AES, puede cifrarse usando la clave pública con anterioridad al almacenamiento en la base 406 de datos de protección de medios.

Aunque no se ilustra, el dispositivo 400 informático puede, en algunas implementaciones, incluir además una base de datos de claves u otro almacén que contenga material clave como, por ejemplo, al menos las claves privadas asociadas a las claves públicas usadas para cifrar las claves AES. En algunas instancias, la base de datos de claves o almacén de claves pueden permitir mecanismos de recuperación de claves. En algunas instancias, una contraseña de usuario se autentica y ello permite el acceso a una entrada particular en la base de datos de claves para recuperar la clave privada y, por consiguiente, descifrar la clave AES.

Ahora se hace referencia a la Figura 5 que muestra, en forma de diagrama de bloques, una arquitectura parcial a modo de ejemplo de un dispositivo 500 informático para cifrar, de manera automática, archivos. La arquitectura incluye una función 502 de interfaz de usuario para acceder a e interactuar con el almacenamiento de archivos cifrados. La función 502 de interfaz de usuario puede proveer operaciones relativas a, por ejemplo, cifrado seguro de datos o metadatos, por ejemplo, datos relativos a una aplicación o a un tipo de medio particular, u otras funciones en algunas implementaciones. La función 502 de interfaz de usuario puede proveer operaciones relativas al cifrado de medios, como se indica por el numeral 504 de referencia. La operación de cifrado de medios puede proveer funcionalidad para acceder a medios cifrados mediante una base 510 de datos de protección de medios, donde los medios u otros archivos se almacenan en un directorio 512 de archivos con seguridad en forma cifrada, y la base 510 de datos de protección de medios contiene los metadatos protegidos con contraseña y material clave para acceder a los archivos cifrados, como se describe en relación con la Figura 4.

La función 502 de interfaz de usuario puede también proveer una operación 506 de cámara segura. La operación 506 de cámara segura puede interactuar con una aplicación 508 de cámara normal en el dispositivo informático, y puede provocar modificaciones al funcionamiento de la aplicación 508 de cámara normal. En particular, la operación 506 de cámara segura, si se invoca, puede provocar la captura de imágenes o vídeo usando la aplicación 508 de cámara normal que se almacenarán en el directorio 512 de archivos con seguridad en formato cifrado. Con respecto a ello, evita que la aplicación 508 de cámara normal almacene cualquier imagen o vídeo capturado en una memoria no cifrada salvo que, en algunos casos, la memoria caché temporal durante un tiempo antes de que la imagen o vídeo se cifre y se elimine de la memoria caché temporal. Puede además evitar que la aplicación 508 de cámara normal almacene cualquier imagen en miniatura de las imágenes o vídeo y/o que registre las imágenes o vídeo capturados en una lista o registro de imágenes recientes u otro registro.

Realizaciones a modo de ejemplo de la presente solicitud no se encuentran limitadas a un sistema operativo, arquitectura de sistema, arquitectura de dispositivo móvil, arquitectura de servidor, o lenguaje de programación informático particulares.

Se comprenderá que las aplicaciones, módulos, rutinas, procesos, subprocesos, u otros componentes de software que implementan el método/proceso descrito pueden realizarse usando técnicas y lenguajes de programación informática estándares. La presente solicitud no se encuentra limitada a procesadores, lenguajes de ordenador, convenciones de programación de ordenador, estructuras de datos u otros detalles de implementación particulares. Las personas con experiencia en la técnica reconocerán que los procesos descritos pueden implementarse como parte de un código ejecutable por ordenador almacenado en una memoria permanente o no permanente, como parte de un chip integrado para aplicaciones específicas (ASIC, por sus siglas en inglés), etc.

Pueden llevarse a cabo ciertas adaptaciones y modificaciones de las realizaciones descritas.

REIVINDICACIONES

1. Un dispositivo (300) informático que comprende:

un procesador (302);

una memoria (304); y

una aplicación (330) de cifrado automático de archivos almacenada en la memoria (304) y

que contiene instrucciones ejecutables por procesador para cifrar, de manera automática, un archivo, en donde las instrucciones, cuando se ejecutan por el procesador (302), hacen que el procesador:

identifique (202) una característica asociada al contenido probablemente sensible según una comunicación recibida de un servidor remoto que especifica la característica del archivo y según un patrón de uso, en donde el patrón de uso deriva en el servidor remoto de operaciones previas de cifrado de archivos en otros dispositivos informáticos que cifran diferentes archivos que tienen la característica,

detecte (204) la creación del archivo,

determine (206) que el archivo contiene contenido sensible sobre la base de que este tiene la característica, y

cifre (208) el archivo según la determinación de que el archivo contiene contenido sensible.

2. El dispositivo informático de la reivindicación 1, en donde la característica del archivo incluye al menos uno de:

datos de geoubicación asociados a la creación del archivo;

datos de marca de tiempo asociados a la creación del archivo.

3. El dispositivo (300) informático de cualquier reivindicación precedente, en donde las instrucciones, cuando se ejecutan, hacen que el procesador (302) cifre mediante al menos uno del movimiento del archivo a una memoria cifrada basada en el disco local y el movimiento del archivo a una memoria cifrada basada en la nube.

4. El dispositivo (300) informático de cualquier reivindicación precedente, en donde el archivo comprende uno de una foto, un vídeo o una grabación de audio.

5. El dispositivo (300) informático de cualquier reivindicación precedente, en donde el dispositivo informático es un dispositivo móvil.

6. Un método (200) implementado por ordenador para cifrar, de manera automática, un archivo almacenado en un dispositivo (300) informático, el método comprendiendo:

identificar (202) una característica asociada al contenido probablemente sensible según una comunicación recibida de un servidor remoto que especifica la característica del archivo y según un patrón de uso, en donde el patrón de uso deriva en el servidor remoto de operaciones previas de cifrado de archivos en otros dispositivos informáticos que cifran diferentes archivos que tienen la característica;

detectar (204) la creación del archivo;

determinar (206) que el archivo contiene contenido sensible sobre la base de que este tiene la característica; y

cifrar (208) el archivo según la determinación de que el archivo contiene contenido sensible.

7. El método implementado por ordenador de la reivindicación 6, en donde la característica del archivo incluye al menos uno de:

datos de geoubicación asociados a la creación del archivo.

8. El método implementado por ordenador de la reivindicación 7, que además comprende identificar la característica del archivo según una cantidad umbral de otros dispositivos informáticos que llevan a cabo la operación previa de cifrado de archivos con respecto a un archivo respectivo que tiene la característica.

9. El método implementado por ordenador de cualquiera de las reivindicaciones 6 a 8, en donde el cifrado incluye al menos uno de mover el archivo a una memoria cifrada basada en el disco local y mover el archivo a una memoria cifrada basada en la nube.

10. Un programa de ordenador configurado para cifrar, de manera automática, un archivo en un dispositivo (300) informático, el programa configurándose cuando se ejecuta por un procesador (302) del dispositivo informático para hacer que el procesador lleve a cabo el método de cualquiera de las reivindicaciones 6 a 9.

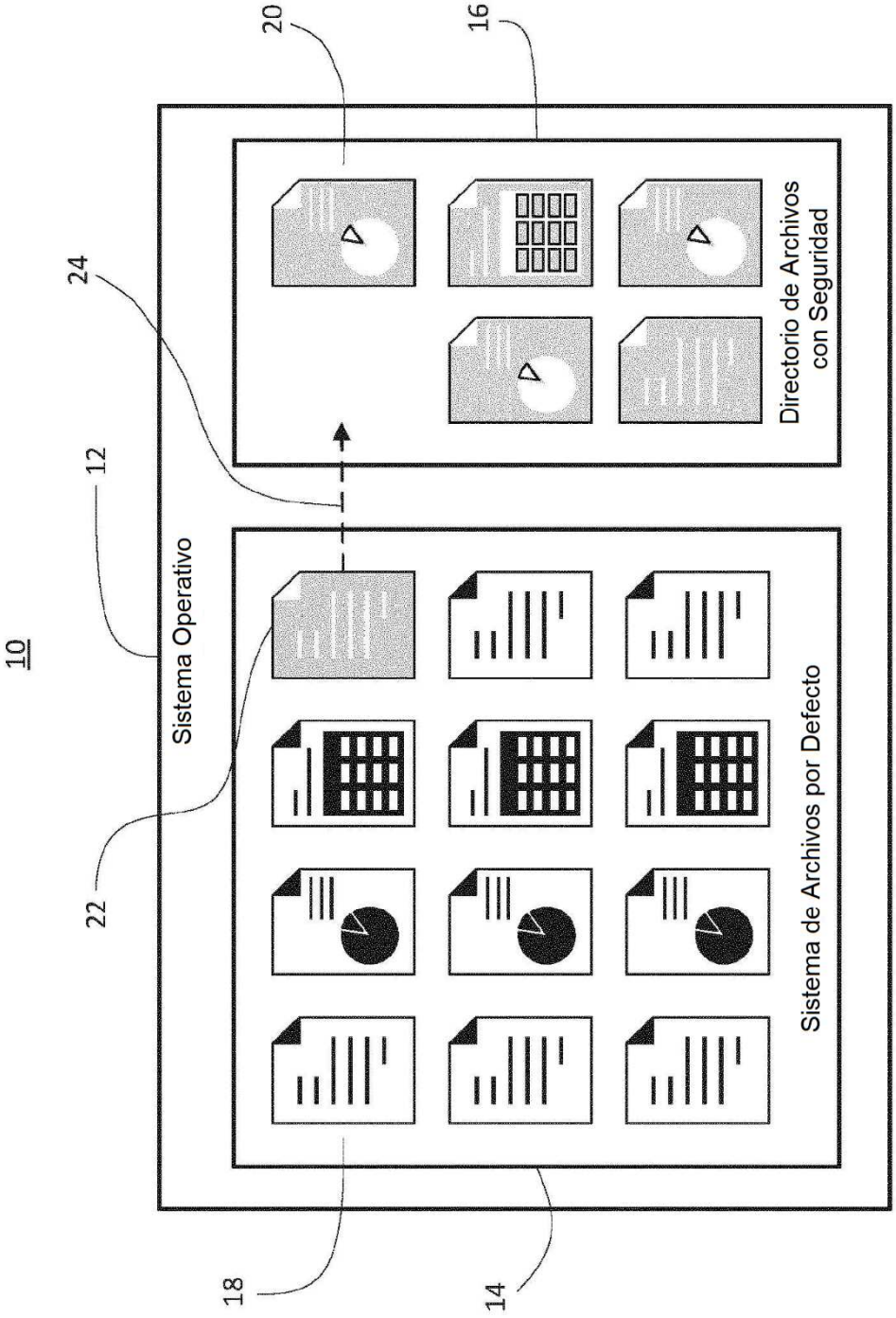
10
12
Sistema Operativo
14
Sistema de Archivos por Defecto
16
Directorio de Archivos con Seguridad
18
20
22
24

FIG. 1

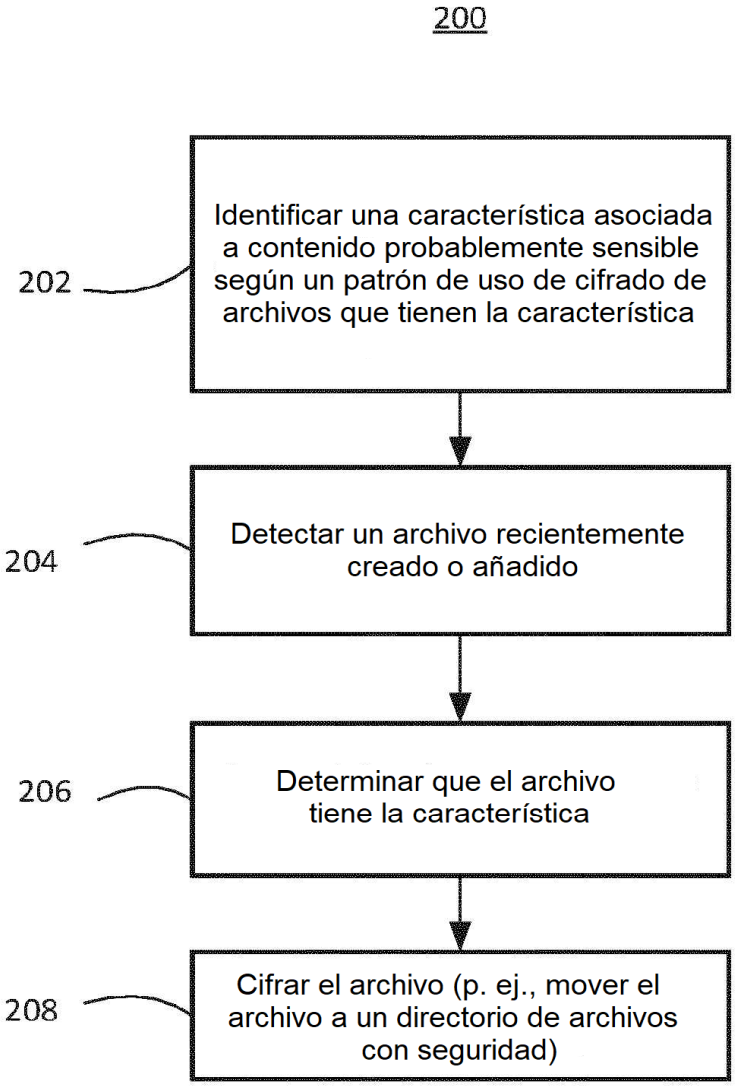
200
202
Identificar una característica asociada a contenido probablemente sensible según un patrón de uso de cifrado de archivos que tienen la característica
204
Detectar un archivo recientemente creado o añadido
206
Determinar que el archivo tiene la característica
208
Cifrar el archivo (p. ej., mover el archivo a un directorio de archivos con seguridad)

FIG. 2

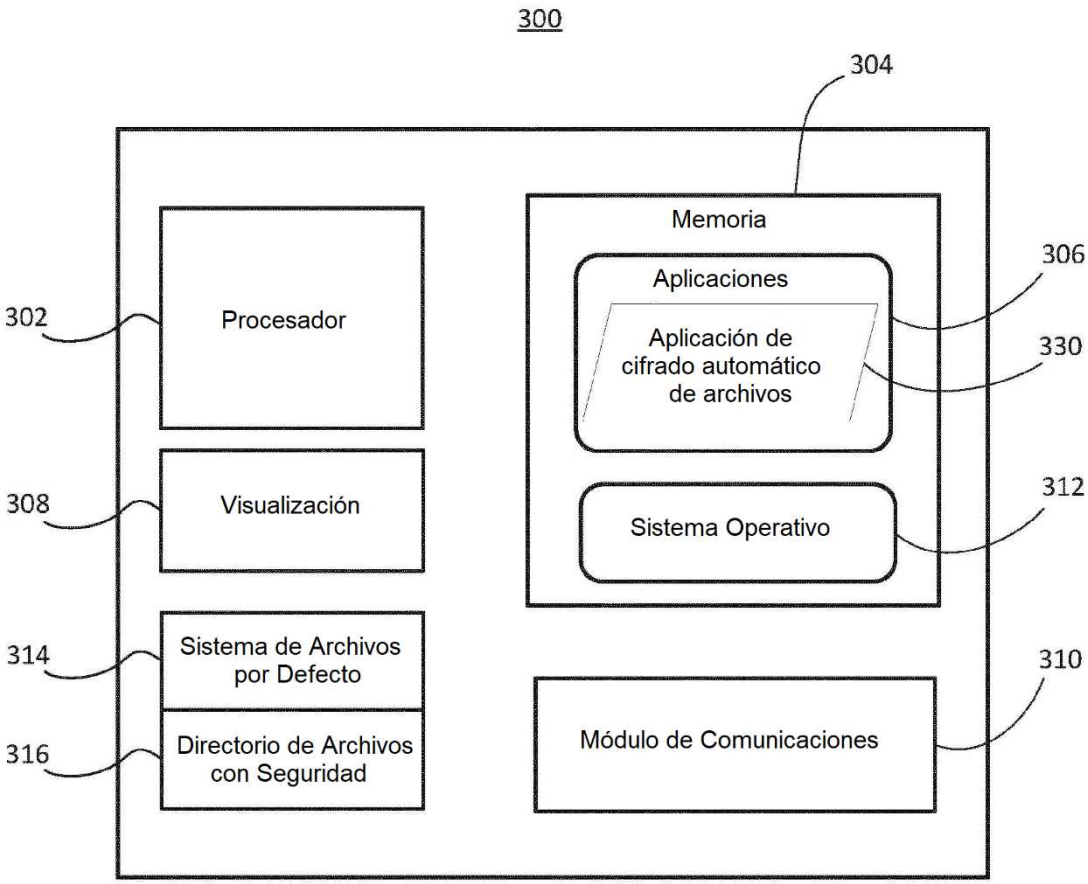
300
304
Memoria
306
Aplicaciones
Aplicación de cifrado automático de archivos
330
302
Procesador
308
Visualización
312
Sistema Operativo
314
Sistema de Archivos por Defecto
316
Directorio de Archivos con Seguridad
310
Módulo de Comunicaciones

FIG. 3

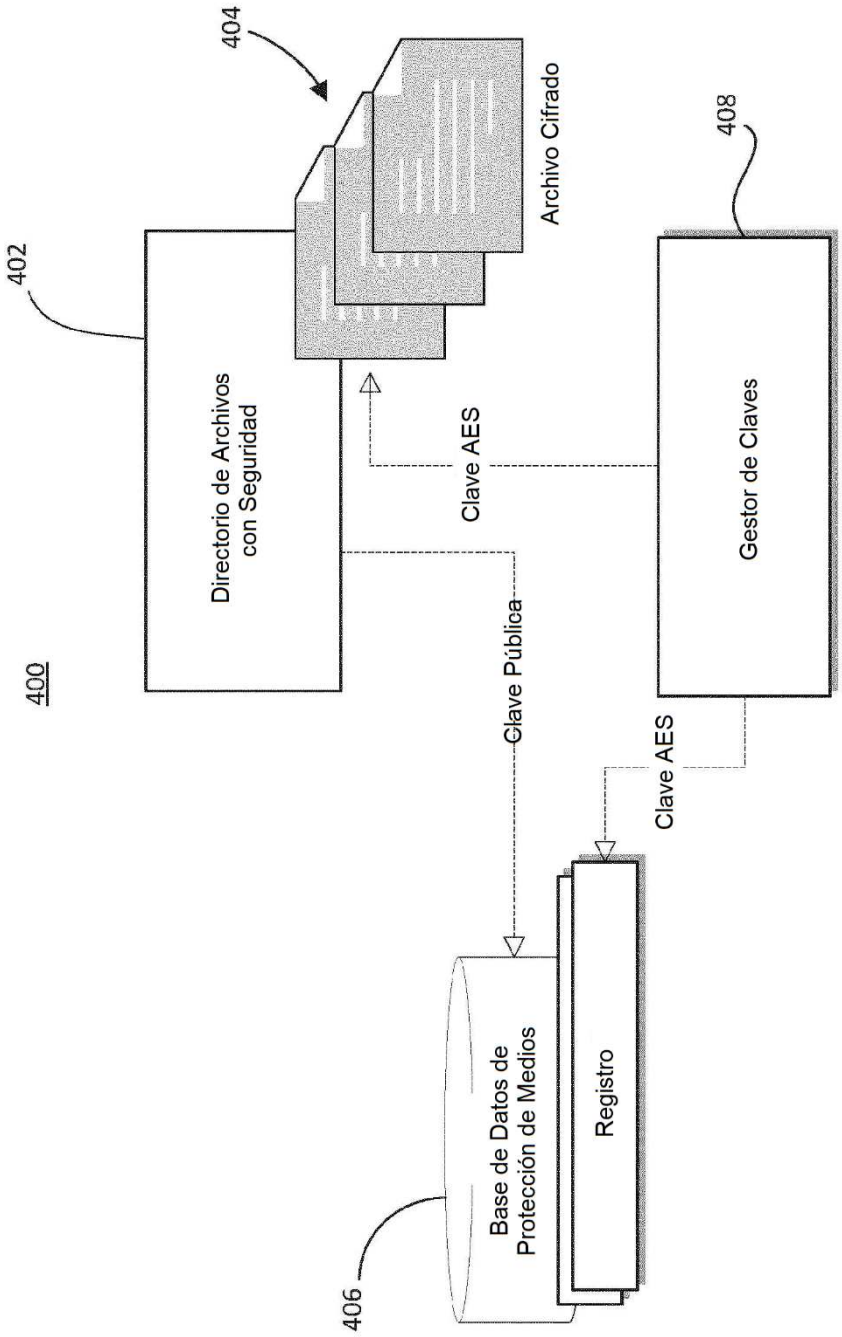
400
402
Directorio de Archivos con Seguridad
404
Archivo Cifrado
Clave AES
Clave Pública
408
Gestor de Claves
Clave AES
406
Base de Datos de Protección de Medios
Registro

FIG. 4

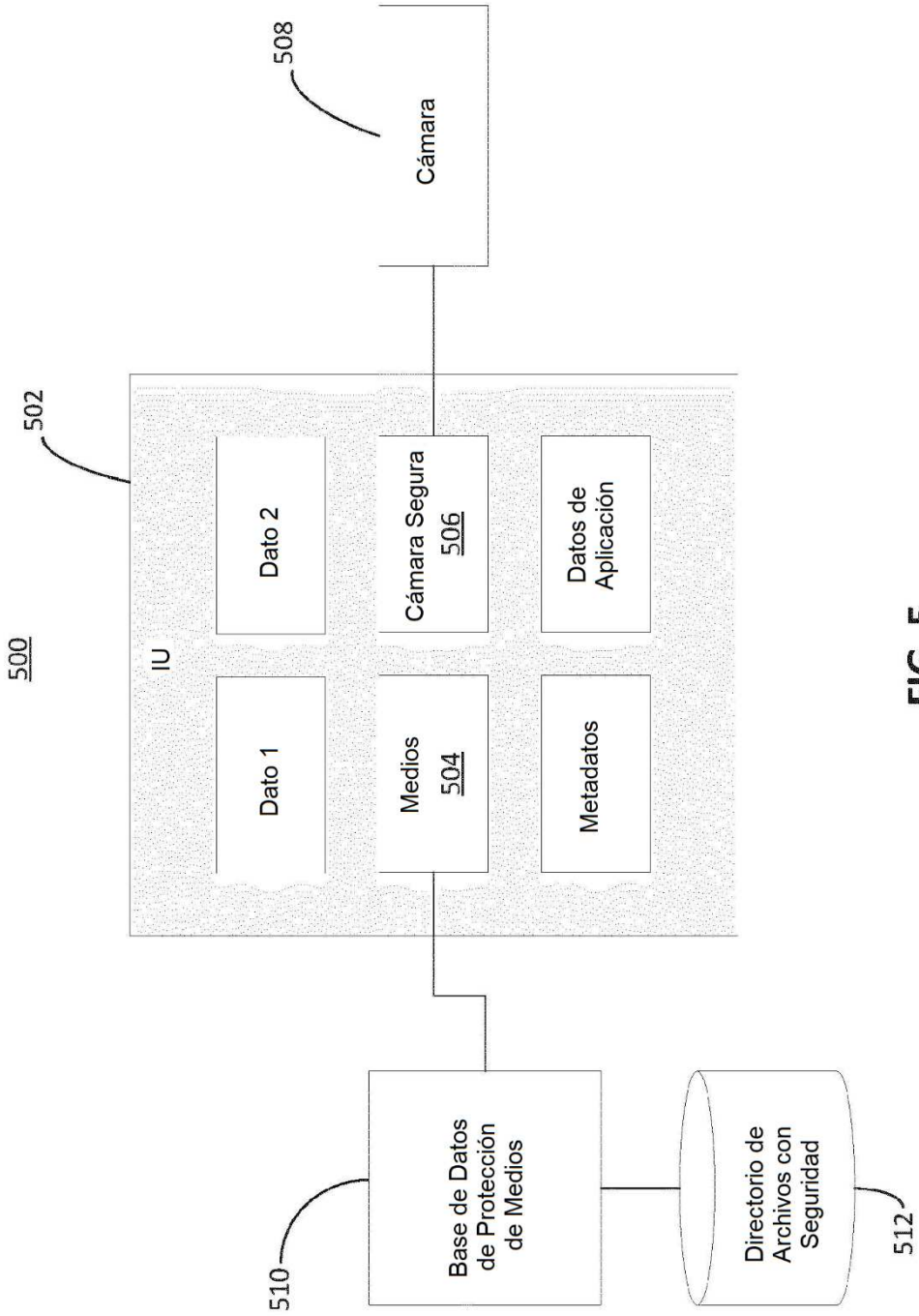
508
Cámara
502
500
IU
Dato 2
Cámara Segura
506
Datos de
Aplicación
Dato 1
Medios
504
Metadatos
510
Base de Datos
de Protección
de Medios
Directorio de
Archivos con
Seguridad
512

FIG. 5