(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 781 766**

(51) Int. CI.:

G03G 21/18 (2006.01)

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(96) Fecha de presentación y número de la solicitud europea: **20.03.2012 E 16197092 (6)**

(97) Fecha y número de publicación de la concesión europea: **04.03.2020 EP 3168691**

(54) Título: **Chip crum y dispositivo de formación de imágenes para comunicarse mutuamente, y método del mismo**

(30) Prioridad:

09.09.2011 KR 20110092060

(45) Fecha de publicación y mención en BOPI de la traducción de la patente:
07.09.2020

(73) Titular/es:

HEWLETT-PACKARD DEVELOPMENT COMPANY, L.P. (100.0%)
10300 Energy Drive
Spring, TX 77389, US

(72) Inventor/es:

LEE, JAE-YOON y
WOO, HONG-ROK

(74) Agente/Representante:

SÁNCHEZ SILVA, Jesús Eladio

DESCRIPCIÓN

Chip crum y dispositivo de formación de imágenes para comunicarse mutuamente, y método del mismo

Antecedentes

Campo

Las modalidades analizadas en la presente descripción se refieren a un chip de Monitoreo de Unidad Reemplazable por el Cliente (CRUM) y un dispositivo de formación de imágenes para comunicarse mutuamente y al método del mismo, y más particularmente, a un chip CRUM y un dispositivo de formación de imágenes para comunicarse mutuamente para detectar si los datos son integrales, mediante el uso de datos de detección integridad en un proceso de comunicación, y un método del mismo.

Descripción de la técnica relacionada

A medida que los ordenadores se expanden cada vez más, la tasa de difusión de los dispositivos periféricos de los ordenadores también aumenta. Los dispositivos periféricos de ordenadores incluyen dispositivos de formación de imágenes tales como impresoras, facsímiles, escáneres, fotocopiadoras e impresoras multifunción.

Los dispositivos de formación de imágenes pueden usar tinta o tóner para imprimir imágenes en papel. Se usa tinta o tóner cada vez que se realiza una operación de formación de imágenes, y por lo tanto se agota cuando se usa durante más de un período de tiempo predeterminado. En tal caso, la unidad en la que se almacena la tinta o el tóner debe reemplazarse. Tales partes o componentes que son reemplazables en el proceso de uso de un dispositivo de formación de imágenes pueden definirse como unidades consumibles o unidades reemplazables. Para conveniencia de la explicación, estas se denominarán unidades consumibles en este documento.

Además de estas unidades que deben reemplazarse debido al agotamiento de la tinta o el tóner como se analizó anteriormente, también hay unidades consumibles que tienen características que cambian cuando las unidades se usan durante más de un cierto período de tiempo, y por lo tanto se reemplazan para lograr una calidad de impresión satisfactoria. Las unidades consumibles incluyen el reemplazo de color para máquinas en desarrollo, y piezas como cintas de transferencia intermedias.

En el caso de los dispositivos de formación de imágenes láser, pueden usarse unidades de electrificación, unidades intermedias o unidades de asentamiento, en las que varios tipos de rodillos y cintas usados en cada unidad pueden desgastarse o degenerarse cuando se usan durante más de la vida útil marginal. En consecuencia, la calidad de la imagen puede deteriorarse severamente. Un usuario debe reemplazar cada componente, es decir, cada unidad consumible en un período de reemplazo apropiado para que la operación de impresión pueda realizarse para producir imágenes limpias.

Para gestionar las unidades consumibles de manera más eficiente, pueden adjuntarse memorias a las unidades consumibles, para intercambiar información con el cuerpo de un dispositivo de formación de imágenes.

Es decir, es posible grabar diversas informaciones de uso, tal como la cantidad de papel impreso, la cantidad de puntos de salida, y el período de uso en la memoria de la unidad consumible, para gestionar un tiempo para reemplazar la unidad consumible.

Para tal gestión de información, un controlador proporcionado en el cuerpo de un dispositivo de formación de imágenes y una unidad de memoria proporcionada en la unidad consumible se comunican entre sí. Sin embargo, existen numerosas variables en el proceso de comunicación. Por ejemplo, puede haber una interrupción de ruido provocada, por ejemplo, por un circuito electrónico o motor proporcionado, por ejemplo, en el dispositivo de formación de imágenes, o un ataque de un pirata informático que intenta controlar el controlador o la unidad de memoria con fines maliciosos.

Los datos de comunicación pueden cambiar debido a estas variables. Por ejemplo, una vez que se completa un trabajo, una unidad consumible puede transmitir información tal como la cantidad de páginas de impresión, la cantidad de puntos y el volumen de tóner restante a un controlador, y copia la información en una memoria no volátil del controlador. Al leer los datos como un valor incorrecto, por ejemplo, tal como 0xFFFFFFFF, existe un riesgo de que el controlador pueda percibir que la vida útil de la unidad consumible correspondiente ha terminado. En este caso, la unidad consumible ya no podrá usarse. Por el contrario, con respecto a una unidad consumible cuya vida útil ha terminado, un pirata informático puede restablecer la información de usuario del consumible, por ejemplo, a un valor de "0" con un propósito malicioso, para reciclar inapropiadamente la unidad consumible. En consecuencia, un usuario puede intentar usar una unidad consumible cuya vida ha terminado, lo que provoca problemas tales como la ruptura del dispositivo de formación de imágenes o el deterioro de la definición.

En consecuencia, se requiere la necesidad de una tecnología que detecte eficientemente los errores de comunicación entre una unidad consumible y un dispositivo de formación de imágenes para buscar la seguridad de los datos. El documento US20090222664A1 describe un método para inicializar un chip CRUM y realizar la autenticación y

comunicación criptográfica. El documento EP0281223A2 describe un sistema de mensajería seguro con varios terminales.
Resumen

Los aspectos y/o ventajas adicionales se expondrán en parte en la descripción que sigue y, en parte, serán evidentes a partir de la descripción, o pueden aprenderse mediante la práctica de la invención.

Un aspecto de modalidades ilustrativas se refiere a un chip CRUM y un dispositivo de formación de imágenes para la seguridad de la comunicación, mediante el uso de datos de detección de integridad, y un método de comunicación de los mismos.

De acuerdo con la presente invención, se proporciona un aparato y método como se establece en las reivindicaciones adjuntas. Otras características de la invención serán evidentes a partir de las reivindicaciones dependientes, y de la descripción que sigue.

Como se mencionó anteriormente, de acuerdo con varias modalidades ilustrativas de la presente descripción, es posible perseguir la seguridad de toda la comunicación mediante el uso de forma acumulativa de los datos de detección de integridad usados en comunicaciones anteriores. En consecuencia, la información de las unidades consumibles y los dispositivos de formación de imágenes puede gestionarse de forma segura.

Breve descripción de los dibujos

Los aspectos anteriores y/u otros de la presente descripción serán más evidentes al describir cierta presente descripción con referencia a los dibujos adjuntos, en los que:

la Figura 1 ilustra un dispositivo de formación de imágenes de acuerdo con una modalidad ilustrativa;
la Figura 2 es una vista de temporización que ilustra un proceso de comunicación entre un controlador y un chip CRUM en un dispositivo de formación de imágenes de acuerdo con una modalidad ilustrativa;
la Figura 3 es una vista de temporización que ilustra un proceso de examen de integridad de una señal mediante el uso de datos de examen de integridad;
la Figura 4 es una vista de temporización que ilustra un proceso de comunicación entre un controlador y un chip CRUM en un dispositivo de formación de imágenes de acuerdo con una modalidad ilustrativa;
la Figura 5 es un diagrama de bloques que ilustra un dispositivo de formación de imágenes ilustrativo montado en una unidad consumible;
las Figuras 6 y 7 ilustran un dispositivo de formación de imágenes ilustrativo de acuerdo con varias modalidades ilustrativas;
la Figura 8 ilustra una configuración de un chip CRUM de acuerdo con una modalidad ilustrativa de la presente descripción; y las Figuras 9 y 10 ilustran un método de comunicación de acuerdo con varias modalidades ilustrativas.

Descripción detallada

Ahora se hará referencia en detalle a las modalidades, ejemplos de las cuales se ilustran en los dibujos adjuntos, en donde los números de referencia similares se refieren a los elementos similares en todas partes. Las modalidades se describen a continuación para explicar la presente invención con referencia a las figuras.

Las modalidades ilustrativas se analizan en detalle a continuación con referencia a los dibujos adjuntos.

En la siguiente descripción, se usan números de referencia de los dibujos similares para los elementos similares. Los asuntos definidos en la descripción, tales como la construcción detallada y los elementos, se proporcionan para ayudar a una comprensión integral de las modalidades ilustrativas.

La Figura 1 ilustra una configuración de un dispositivo de formación de imágenes de acuerdo con una modalidad ilustrativa. Como se ilustra en la Figura 1, por ejemplo, un dispositivo de formación de imágenes incluye un cuerpo 100, un controlador 110 proporcionado en el cuerpo 100, y una unidad consumible 200 que puede montarse en el cuerpo 100. Un dispositivo de formación de imágenes puede realizarse como varios tipos de dispositivos, tales como una impresora, escáner, dispositivo multifunción, facsímil, o fotocopiadora, que pueden formar imágenes en papel o en otros medios de grabación. De acuerdo con una modalidad ilustrativa, el cuerpo 100 puede ser un cuerpo principal del dispositivo de formación de imágenes y el controlador 110 puede ser un controlador principal.

El controlador 110 puede montarse en el cuerpo 100 del dispositivo de formación de imágenes para controlar las funciones del dispositivo de formación de imágenes. De acuerdo con una modalidad ilustrativa, el controlador 110 es un controlador principal que controla todas las funciones del dispositivo de formación de imágenes.

La unidad consumible 200 puede montarse en el cuerpo 100 del dispositivo de formación de imágenes, y puede ser uno de varios tipos de unidades que se involucran en el dispositivo de formación de imágenes, ya sea directa o indirectamente. Por ejemplo, en el caso de un dispositivo de formación de imágenes láser, las unidades de electrificación, las unidades de exposición a la luz, las unidades de desarrollo, las unidades de transferencia, las unidades de asentamiento, los

diversos tipos de rodillos, cintas y tambores OPC pueden ser unidades consumibles. Además, varios tipos de unidades que deben reemplazarse mediante el uso de un dispositivo de formación de imágenes pueden definirse como una unidad consumible 200.

Cada unidad consumible 200 puede tener una vida útil predeterminada. Por lo tanto, una unidad consumible 200 puede incluir un microprocesador y/o circuito tal como un chip CRUM (chip de Monitoreo de Unidad Reemplazable por el Cliente) 210 que permite el reemplazo en el momento apropiado.

Un chip CRUM 210 puede montarse en una unidad consumible 200 y grabar diversas informaciones. Un chip CRUM 210 incluye una memoria. Por lo tanto, puede hacerse referencia a un chip CRUM 210 en varios términos, tal como una unidad de memoria o memoria CRUM (memoria de Monitoreo de Unidad Reemplazable por el Cliente), pero por razones de conveniencia de la explicación, se usará el término “chip CRUM”.

En la memoria proporcionada en el chip CRUM, puede almacenarse información de diversas características con respecto a la unidad consumible 200, el chip CRUM en sí mismo, o el dispositivo de formación de imágenes, y también la información de uso o programas con respecto a la realización de un trabajo de formación de imágenes.

Varios programas almacenados en el chip CRUM pueden incluir no solo aplicaciones generales, sino también programas de O/S (sistema operativo) y programas de cifrado. La información sobre el fabricante de la unidad consumible 200, la información sobre el fabricante del dispositivo de formación de imágenes, los nombres de los dispositivos de formación de imágenes que pueden montarse, la información sobre la fecha de fabricación, el número de serie, el nombre del modelo, la información de la firma electrónica, la clave de cifrado, y el índice de la clave de cifrado pueden incluirse en la información de características. La información de uso puede incluir información tal como cuántas hojas de papel se han impreso hasta ahora, cuántas hojas de papel pueden imprimirse a partir de ahora y cuánto tóner queda. La información de características también puede denominarse en cambio como información única.

De acuerdo con una modalidad ilustrativa, la información como se ilustra a continuación en la Tabla 1 puede almacenarse en un chip CRUM 210.

Tabla 1

Información general	
Versión OS Versión SPL-C Versión del motor Número de serie USB Modelo Fecha de inicio del servicio	CLP300_V1.30.12.35 22-02-2007 5.24 28-06-2006 6.01.00(55) BH45BAIP914466B. DOM 29-09-2007
Opción	
Tamaño de RAM Tamaño de EEPROM USB conectado (alto)	32 Mbytes 4096 bytes
Vida de los consumibles	
Recuento total de páginas Vida del fusor Vida del rodillo de transferencia Vida del rodillo de bandeja	774/93 páginas (color/mono) 1636 páginas 864 páginas 867 páginas
Recuento total de imágenes Vida de la unidad de imagen/rodillo de desarrollo Vida de la cinta de transferencia Recuento de imágenes de tóner	 3251 imágenes 61 imágenes/19 páginas 3251 imágenes 14/9/14/19 imágenes (C/M/Y/K)
Información de tóner	
Por ciento de tóner restante Cobertura promedio de tóner	99 %/91 %/92 %/100 % (C/M/Y/K) 5 %/53 %/31 %/3 % (C/M/Y/K)
Información de consumibles	
Tóner cian Tóner magenta Tóner amarillo	SAMSUNG (DOM) SAMSUNG (DOM) SAMSUNG (DOM)

Tóner negro Unidad de imagen	SAMSUNG (DOM) SAMSUNG (DOM)
Menú de colores	
Color personalizado	Ajuste manual (CMYK: 0,0,0,0)
Menú de configuración	
Ahorro de energía Continuar automáticamente Ajuste de altitud	20 minutos Encendido Llanura

En la memoria del chip CRUM 210, puede almacenarse información aproximada de la unidad consumible 200, e información sobre la vida, información y menú de configuración de la unidad consumible 200. Además del cuerpo del dispositivo de formación de imágenes, un O/S proporcionado para su uso en la unidad consumible puede almacenarse en la memoria.

El chip CRUM puede incluir una CPU (no ilustrada) que puede administrar la memoria, ejecutar varios programas almacenados en la memoria, y comunicarse con un cuerpo de un dispositivo de formación de imágenes o un controlador de otros dispositivos.

La CPU puede controlar el O/S almacenado en la memoria del chip CRUM, y realizar la inicialización de la unidad consumible 200 en sí, aparte de la inicialización del dispositivo de formación de imágenes. La CPU puede realizar la certificación entre el cuerpo del dispositivo de formación de imágenes cuando la inicialización se ha completado o durante la inicialización. Una vez que se completa la inicialización, puede realizar una comunicación de datos de cifrado con el cuerpo del dispositivo de formación de imágenes. Varios comandos y datos transmitidos desde el cuerpo del dispositivo de formación de imágenes pueden cifrarse de acuerdo con un algoritmo de cifrado arbitrario y transmitirse.

En un caso particular, por ejemplo, tal como cuando la alimentación del dispositivo de formación de imágenes que tiene la unidad consumible 200 está encendida, o cuando la unidad consumible 200 se desconecta y luego se conecta al cuerpo 100 del dispositivo de formación de imágenes nuevamente, la CPU puede realizar la inicialización por sí misma aparte de la inicialización del controlador 100. La inicialización incluye varios procesos tales como la activación inicial de varios programas de aplicación usados en la unidad consumible 200, calcular la información secreta necesaria en la comunicación de datos con el controlador 110 después de la inicialización, configurar un canal de comunicación, inicializar un valor de memoria, verificar cuándo reemplazar el mismo, establecer un valor de registro interno de la unidad consumible 200, y establecer una señal de reloj interna-externa.

El establecimiento de un valor de registro puede definirse como una operación de establecer valores de registro funcionales dentro de la unidad consumible 200 de manera que la unidad consumible 200 pueda operar de acuerdo con varios estados funcionales predeterminados por un usuario. El establecimiento de una señal de reloj interna-externa se refiere a una operación de ajuste de una frecuencia de una señal de reloj externa proporcionada desde el controlador 110 del dispositivo de formación de imágenes para que esté en línea con la señal de reloj interna que usa la CPU dentro de la unidad consumible 200.

La verificación de cuándo reemplazar el mismo puede ser una operación de identificar el volumen restante de un tóner o tinta usada hasta ahora, anticipar cuándo se agotará la tinta o tóner y notificar al controlador 110. Al determinar en el proceso de inicialización que el volumen del tóner ya se ha agotado, la unidad consumible 200 puede manifestarse para notificar al controlador 110 que está en un estado no operable. Dado que la unidad consumible 200 en sí tiene el O/S, pueden realizarse varios tipos de inicialización de acuerdo con los tipos y características de la unidad consumible 200.

Una vez que se ha montado la CPU y se ha proporcionado el O/S, puede identificarse el volumen restante de la unidad consumible almacenado en la unidad de memoria 210 o el número de veces de recarga, antes de que el controlador 110 solicite la comunicación con la unidad 200, cuando se enciende el dispositivo de formación de imágenes. En consecuencia, el tiempo de notificación de la escasez de la unidad consumible puede hacerse antes. Por ejemplo, cuando el tóner se está agotando, un usuario puede encenderlo, y luego hacer ajustes para la conversión al modo de ahorro de tóner y luego realizar la formación de imágenes. Lo mismo se aplica cuando solo un tóner en particular se está agotando también.

La CPU puede no responder a un comando del controlador 110 hasta que la inicialización esté en proceso y luego se complete. El controlador 110 espera una respuesta mientras transmite periódicamente el comando hasta que haya una respuesta.

En consecuencia, cuando se recibe una respuesta, es decir, un acuse de recibo, puede realizarse una certificación entre el controlador 110 y la CPU. En este caso, debido al O/S del mismo instalado en el chip CRUM 210, es posible realizar una certificación a través de la interacción entre la unidad CRUM 210 y el controlador 110.

El controlador 110 cifra los datos o un comando para la certificación y los transmite al chip CRUM 210. En los datos

transmitidos, puede incluirse un valor arbitrario R1. En la presente descripción, R1 puede ser un valor aleatorio que cambia en cada certificación, o un valor fijo predeterminado. El chip CRUM que recibió los datos genera una clave de sección mediante el uso de un valor arbitrario R2 y el R1 recibido, y luego genera un MAC (Código de autenticación de mensaje) mediante el uso de la clave de sección generada.

Una señal que incluye el MAC generado y el R2 como se mencionó anteriormente se transmite al controlador 110. El controlador 110 genera la clave de sección mediante el uso de los R2 y R1 recibidos, genera el MAC mediante el uso de la clave de sección generada, y luego certifica el chip CRUM 210 al comparar el MAC generado y el MAC en la señal recibida. De acuerdo con diversas modalidades ilustrativas, la información de la firma electrónica o la información de la clave puede transmitirse en tal proceso de certificación y usarse en la certificación.

Una vez que la certificación se realiza con éxito, el controlador 110 y el chip CRUM realizan una comunicación de datos de cifrado para la gestión de datos. Es decir, cuando se ha ingresado un comando de usuario o cuando se ha iniciado o completado un trabajo de formación de imágenes, el controlador 110 cifra el comando o los datos para realizar operaciones de lectura o escritura de datos mediante el uso de un algoritmo de cifrado, y luego los transmite al chip CRUM 210.

El chip CRUM 210 puede decodificar el comando o los datos recibidos, y realizar operaciones tales como la lectura o escritura de los datos correspondientes al comando decodificado. El algoritmo de cifrado usado en el chip CRUM 210 o el controlador 110 puede ser un algoritmo de cifrado estandarizado. Tal algoritmo de cifrado puede cambiar cuando la clave de cifrado se ha filtrado o cuando es necesario fortalecer la seguridad. Pueden usarse varios algoritmos de cifrado tales como el algoritmo de clave asimétrica RSA, ARIA, TDES, SEED, el algoritmo de clave simétrica AES.

Como tal, entre el chip CRUM 210 y el controlador 110, la comunicación para la certificación y el intercambio de datos puede realizarse numerosas veces. En cada comunicación, las señales se transmiten desde el controlador 110 al chip CRUM 210 o viceversa. En este caso, una señal transmitida incluye los datos de detección de errores para detectar la integridad de los datos incluidos en la señal correspondiente. Tales datos de detección de errores son datos generados por la acumulación de datos de detección de errores incluidos en la señal transmitida o recibida de la comunicación anterior.

Es decir, entre el controlador 110 y el chip CRUM 210, pueden realizarse una pluralidad de comunicaciones tales como la certificación 1, la certificación 2, la certificación 3, ..., la certificación n, la comunicación de datos 1, la comunicación de datos 2, ..., la datos comunicación m. En una señal transmitida en cada comunicación, pueden incluirse los datos de detección de integridad. En tales datos de detección de integridad, los datos de detección de integridad usados en la comunicación anterior se reflejan acumulativamente.

El lado que recibió la señal detecta la integridad de la señal correspondiente mediante el uso de los datos de detección de integridad en la señal. En consecuencia, cuando se determina que los datos correspondientes son integrales, los datos y los datos de detección de integridad incluidos en esa señal pueden almacenarse temporalmente. Pueden generarse nuevos datos de detección de integridad mediante el uso de datos posteriores que se transmitirán al lado que transmitió la señal y los datos de detección de integridad recibidos de la comunicación anterior y almacenados temporalmente. En consecuencia, una señal a la que se han agregado los nuevos datos de detección de integridad puede transmitirse a los datos posteriores. Entre el controlador 110 y el chip CRUM 210, tal comunicación que incluye tales datos de detección de integridad puede realizarse una pluralidad de veces. Cuando se realiza la última comunicación, puede realizarse una detección final mediante el uso de los datos de detección de integridad incluidos en la última señal recibida. Si no hay nada mal con la detección final, pueden registrarse todos los datos que se hayan almacenado temporalmente hasta entonces.

La Figura 2 ilustra un proceso de comunicación ilustrativo entre el controlador 110 y el chip CRUM 210 de acuerdo con una modalidad ilustrativa de la presente descripción. De acuerdo con la Figura 2, el controlador 110 transmite una primera señal 10 que incluye los datos 1 y los datos de detección de integridad 1. El chip CRUM 210 que recibió la primera señal 10 genera los datos de detección de integridad 2 mediante el uso de los datos de detección de integridad 1 incluidos en la primera señal 10 y los datos 2. El chip CRUM 210 transmite una segunda señal que incluye los datos 2 y los datos de integridad 2 al controlador 110. Como tal, las señales (30, ..., N) que incluyen los datos de detección de integridad generados mediante el uso de los datos de detección de integridad de la comunicación anterior se realizan una pluralidad de veces.

Un valor de resultado del cálculo lógico en los datos a transmitir, un valor de resultado generado al aplicar una fórmula matemática predeterminada a los datos o un valor de resultado del cifrado de los datos, es decir, MAC puede usarse como los datos de detección de integridad.

La Figura 3 ilustra un método de detección mediante el uso de datos de detección de integridad. De acuerdo con la Figura 3, cuando se recibe una señal que incluye los datos a y los datos de detección de integridad a (S310), el chip CRUM 210 separa los datos de detección de integridad a (S320).

El chip CRUM 210 genera los datos de detección de integridad a' mediante el uso de los datos restantes y los datos de

detección de integridad que había transmitido durante la comunicación anterior (S330). El chip CRUM 210 luego compara los datos de detección de integridad a' generados en consecuencia con los datos de detección de integridad a separados (S340), y si son idénticos, determina que son integrales (S350). Si no son idénticos, el chip CRUM 210 determina que los datos están en un estado de error, y detiene la comunicación (S360). Para la conveniencia de la explicación, en lo sucesivo, los datos de detección de integridad a' se denominarán como los datos sujetos a comparación.

Cuando se determina que los datos correspondientes son integrales, los datos de detección de integridad b se generan mediante el uso de los datos b que se transmitirán y los datos de detección a (S370). En consecuencia, una señal que incluye los datos b y los datos de detección de integridad b se transmite al controlador 110 (S380).

La Figura 3 ilustra un proceso de detección ilustrativo realizado, por ejemplo, en el chip CRUM 210, pero el mismo proceso puede realizarse también en el controlador 110. Es decir, cuando el controlador 110 recibe una señal que incluye los datos b y los datos de detección de integridad b, separa los datos de detección de integridad b, y realiza la detección. Este método de detección es similar a (S330) a (S370), por lo que se omitirán las explicaciones e ilustraciones repetidas.

La configuración de las señales transmitidas y recibidas entre el controlador 110 y el chip CRUM 210 puede diseñarse en varios tipos. Es decir, los datos incluidos en las señales pueden incluir al menos uno de un comando, la información que se grabará, la información del resultado de las operaciones de acuerdo con el comando, la información del resultado de la detección de integridad con respecto a las señales recibidas anteriormente, y la información del indicador para notificar una ubicación de los datos de detección de integridad. La información del resultado sobre la detección de integridad puede excluirse de las señales inicialmente transmitidas y recibidas entre el controlador 110 y el chip CRUM 210.

La Figura 4 ilustra una modalidad ilustrativa de un proceso de detección de integridad mediante el uso de señales que tienen formatos diferentes, por ejemplo, diferentes de los de la Figura 2. De acuerdo con la Figura 4, el controlador 110 transmite una señal que incluye los datos y los datos de detección de integridad 1 (S410). En la presente descripción, los datos incluyen unos datos de comando (CMD) de lectura 1 y un indicador U1. Los datos de comando (CMD) de lectura 1 incluyen no solo un comando sino también un objetivo de lectura o una dirección de memoria. El U1 se refiere a la información del indicador que sigue a los datos de comando (CMD) de lectura 1. La información del indicador U1 se refiere a un símbolo para notificar una ubicación de análisis de los datos de detección de integridad en la señal. La información del indicador puede expresarse como un número de bytes fijo. Por ejemplo, pueden usarse cinco bytes para la información del indicador. Por otro lado, los datos de comando (CMD) de lectura 1 son variables de acuerdo con el contenido de los datos y, por lo tanto, el tamaño de los datos de detección de integridad 1 también es variable.

Cuando se recibe la señal, el chip CRUM 210 realiza la detección de integridad mediante el uso de los datos de detección de integridad 1 incluidos en la señal (S415). El chip CRUM 210 es capaz de generar los datos de detección de integridad 2 mediante el uso de los datos a transmitir y los datos de detección de integridad 1, y transmite la señal que incluye estos (S420). Como se ilustra en la Figura 4, en la señal a transmitir, se incluyen unos datos de lectura 1 que son los datos leídos desde la memoria proporcionada en la unidad consumible 100 de acuerdo con los datos de comando (CMD) de lectura 1, unos datos de resultado 2 que indican el resultado de la operación realizada de acuerdo con los datos de comando (CMD) de lectura 1, un indicador U2, y los datos de detección de integridad 2.

El controlador 110 separa los datos de detección de integridad 2 de la señal recibida y realiza la detección de integridad (S425). Entonces, si existen unos datos de comando (CMD) de lectura 3 posteriores, el controlador 110 genera unos datos de detección de integridad 3 mediante el uso de los datos de comando (CMD) de lectura 3 y los datos de detección de integridad 2, y luego transmite una señal que incluye los datos de comando (CMD) de lectura 3, un indicador U3, y unos datos de detección de integridad 3 al chip CRUM 210 (S430).

Como se ilustra en la Figura 4, por ejemplo, se realizan comunicaciones mediante el uso de una pluralidad de datos de detección de integridad 4, 5, 6, T1, y T2 (S440, S450, S460, S470, S485), seguidas por las detecciones de integridad en consecuencia (S435, W445, S455, S465). Cuando se recibe la señal de comunicación final desde el chip CRUM 210 (S470), el chip CRUM 210 detecta la integridad de los datos que se han transmitido y recibido en todo el proceso de comunicación y almacenado temporalmente mediante el uso de los datos de detección de integridad T1 incluidos en la señal de comunicación final (S475). Si se determina que los datos son integrales como un resultado de la detección final, los datos que se han almacenado temporalmente se almacenan en una memoria no volátil (no ilustrada) (S480). Del mismo modo, cuando la señal de comunicación final se transmite desde el chip CRUM 210, el controlador 110 realiza además la detección de integridad completa mediante el uso de los datos de detección de integridad T2 incluidos en la señal de comunicación final (S490). En consecuencia, los datos que se han almacenado temporalmente se almacenan en la memoria no volátil, si se determina que los datos son integrales (S495).

Los datos de detección de integridad usados en tales procesos de comunicación se generan al acumular los datos de detección de integridad usados en las comunicaciones anteriores.

De acuerdo con una modalidad ilustrativa, los datos de detección de integridad pueden procesarse como sigue:

Datos de detección de integridad 1 = E(Datos de CMD de lectura 1 | U1)

Datos de detección de integridad 2 = E(Datos de CMD de lectura 2 | Datos de resultado 2 | U2 | Datos de detección de integridad 1

Datos de detección de integridad 3 = E(Datos de CMD de lectura 3 | U3 | Datos de detección de integridad 2

Datos de detección de integridad 4 = E(Datos de CMD de lectura 4 | Datos de resultado 4 | U4 | Datos de detección de integridad 3

Datos de detección de integridad 5 = E(Datos de CMD de escritura 5 | U5 | Datos de detección de integridad 4)

Datos de detección de integridad 6 = E(Datos de lectura 6 | U6 | Datos de detección de integridad 5)

Datos de detección de integridad T1 = E(Datos de CMD de escritura L1 | U-T1 | Datos de detección de integridad T1-1)

Datos de detección de integridad T2 = E(Datos de resultado L2 | U-T2 | Datos de detección de integridad T1)

En las fórmulas mencionadas anteriormente, el término "E()" indica una función para aplicar una fórmula predeterminada para obtener un valor de resultado. Como tal, los datos de detección de integridad pueden generarse al agregar los datos de detección de integridad anteriores y los datos completos a transmitir, aplicar varios cálculos lógicos tales como XOR(OR exclusivo), a partir del valor resultante de sustituir los datos en otras fórmulas conocidas entre el controlador 110 y el chip CRUM 210, y a partir del valor resultante de los cifrados al aplicar varios algoritmos de cifrado mencionados anteriormente.

La Figura 5 ilustra un dispositivo de formación de imágenes ilustrativo donde se proporcionan una pluralidad de unidades consumibles 200-1, 200-2, ..., 200-n dentro del cuerpo 500 de acuerdo con una modalidad ilustrativa de la presente descripción.

Como se ilustra en la Figura 5, un dispositivo de formación de imágenes incluye un controlador 510, una unidad de interfaz de usuario 120, una unidad de interfaz 130, una unidad de memoria 140, y una pluralidad de unidades consumibles 200-1, 200-2, ..., 200-n.

La unidad de interfaz de usuario 120 realiza una función de recibir varios comandos desde el usuario, o mostrar y notificar diversas informaciones. La unidad de interfaz de usuario 120 puede incluir una pantalla LCD o LED, al menos un botón, o un altavoz. También puede incluir una pantalla táctil en dependencia de las circunstancias.

La unidad de interfaz 130 se refiere a una configuración que puede conectarse con una conexión por cable y/o de forma inalámbrica con una PC servidor o varios dispositivos externos para realizar la comunicación. La unidad de interfaz 130 puede incluir varios tipos de interfaces tales como una interfaz local, una interfaz USB (BUS Serie Universal), y una interfaz de red inalámbrica.

La unidad de memoria 140 realiza una función de almacenar diversos programas o datos necesarios para accionar el dispositivo de formación de imágenes.

El controlador 510 cumple una función de controlar todas las operaciones del dispositivo de formación de imágenes. El controlador 510 procesa los datos recibidos a través de la unidad de interfaz 130, y convierte los datos procesados en un formato en el que puede formarse la imagen.

El controlador 510 realiza un trabajo de formación de imágenes en los datos convertidos mediante el uso de una pluralidad de unidades consumibles 200-1, 200-2, ..., 200-n. La unidad consumible puede proporcionarse de varias maneras en dependencia del tipo de dispositivo de formación de imágenes.

En el caso de una impresora láser, las unidades de electrificación, las unidades de exposición a la luz, las unidades de desarrollo, las unidades de transferencia, las unidades de asentamiento, los diversos tipos de rodillos, cintas y tambores OPC pueden ser unidades consumibles.

En cada unidad consumible 200-1, 200-2, ..., 200-n, puede incluirse un primer chip CRUM hasta n chips CRUM 210-1, 210-2, ..., 210-n.

Cada chip CRUM puede incluir una memoria y una CPU, etc. Puede incluirse al menos uno de un módulo criptográfico, un detector de manipulación, una unidad de interfaz, una unidad de reloj (no ilustrada) que emite señales de reloj, o una unidad de generación de valores aleatorios (no ilustrada) que genera un valor aleatorio para la certificación.

La unidad criptográfica (no ilustrada) soporta el algoritmo de cifrado para que la CPU (no ilustrada) pueda realizar la certificación o la comunicación cifrada con el controlador 510. La unidad criptográfica puede soportar un algoritmo determinado entre 4 algoritmos de cifrado, tales como ARIA, TDES, SEED y el algoritmo de clave simétrica AES. El controlador 510 también puede soportar un algoritmo correspondiente entre 4 algoritmos de cifrado. En consecuencia, el

controlador 510 puede identificar qué tipo de algoritmo de cifrado se usa en la unidad consumible 200, proceder con el algoritmo de cifrado, y realizar la comunicación de cifrado.

Por consiguiente, incluso cuando se emite una clave, independientemente del tipo de algoritmo de cifrado aplicado a la unidad consumible 200, la clave puede montarse fácilmente en el cuerpo 100 y realizar la comunicación de cifrado.

Un detector de manipulación (no ilustrado) es una unidad para defender varios intentos de piratería física, es decir, manipulación. Un detector de manipulación monitorea un entorno de operación tal como voltaje, temperatura, presión, luz y frecuencia, y cuando hay un intento, borra o bloquea físicamente los datos. En este caso, el detector de manipulación puede tener una energía separada.

La memoria proporcionada dentro del chip CRUM 210 puede incluir una memoria de O/S, una memoria no volátil o una memoria volátil. La memoria del O/S (no ilustrada) puede almacenar el O/S para accionar la unidad consumible 200. La memoria no volátil (no ilustrada) puede almacenar varios datos sin volatilidad. En la memoria no volátil, pueden almacenarse diversas informaciones, tal como la información de la firma electrónica, la información de varios algoritmos de cifrado, la información sobre el estado de la unidad consumible 200 (por ejemplo, el volumen de tóner restante, cuándo cambiar el tóner, el número restante de hojas de impresión etc.), la información única (por ejemplo, la información del fabricante, la información de la fecha de fabricación, el número de serie, el nombre del modelo del producto, etc.), y la información de A/S. Los datos recibidos en el proceso de comunicación con el controlador pueden almacenarse en la memoria no volátil.

La memoria volátil (no ilustrada) puede usarse como un espacio de almacenamiento temporal necesario para la operación. En la memoria volátil, pueden almacenarse temporalmente los datos determinados como integrales en cada comunicación y los datos de detección de integridad usados en cada determinación.

La unidad de interfaz (no ilustrada) tiene una función de conectar la CPU con el controlador y puede incorporarse como una interfaz serie o una interfaz inalámbrica. Dado que la interfaz serie usa un menor número de señales que una interfaz paralela, tiene un efecto de ahorro de costos y, además, es adecuada en entornos operativos donde hay mucho ruido, tal como en una impresora.

Un chip CRUM puede proporcionarse en cada unidad consumible. Cada chip CRUM puede realizar la comunicación con el controlador y otros chips CRUM. Durante la comunicación, se transmiten nuevos datos de detección de integridad generados al acumular los datos de detección de integridad usados en la comunicación anterior.

La Figura 6 ilustra un dispositivo de formación de imágenes de acuerdo con una modalidad ilustrativa de la presente invención. Como se ilustra en la Figura 6, por ejemplo, un dispositivo de formación de imágenes incluye un controlador 610 y una unidad de interfaz 630, y el controlador 610 incluye una unidad de procesamiento de datos 111, una unidad de generación 112, una unidad de detección 113 y una unidad de control 114.

La unidad de procesamiento de datos 111 genera los datos para ser transmitidos al chip CRUM montado en la unidad consumible que puede montarse en el dispositivo de formación de imágenes. Los datos incluyen al menos uno de un comando y la información que debe procesar ese comando. Es decir, en el caso de un comando de lectura, una dirección de una memoria a leer o la información sobre el tema a leer pueden transmitirse juntas. En el caso de un comando de escritura, la información a grabar puede transmitirse conjuntamente. La unidad de procesamiento de datos 111 puede generar los datos como son o puede cifrar los datos y luego generarlos. Varios comandos tales como un comando para la certificación y la información relacionada con esos comandos pueden generarse en la unidad de procesamiento de datos 111. Estos comandos y la información pueden generarse con frecuencia antes, durante o después de realizar el trabajo de formación de imágenes. Por ejemplo, cuando el dispositivo de formación de imágenes se enciende o cuando la unidad consumible 200 se desconecta y luego se vuelve a conectar, o cuando se ingresa un comando de inicialización en el trabajo de formación de imágenes, el controlador 110 puede transmitir el comando de certificación o el comando de lectura para la certificación en la unidad consumible 200. En consecuencia, el controlador 610 puede identificar diversas informaciones que se gestionan en la propia unidad consumible 200, o puede almacenarlas en la unidad de memoria 140 del cuerpo del dispositivo de formación de imágenes 100.

Durante o después de completar la realización del trabajo de formación de imágenes, la unidad de procesamiento de datos 111 puede generar un comando de escritura y la información correspondiente para grabar la información sobre el artículo consumido, es decir, la información sobre la tinta o el tóner, el número de páginas impresas, el número de puntos impresos, y la información del historial sobre el usuario que realizó la impresión, a la unidad consumible 200.

La unidad de generación 112 genera los datos de detección de integridad mediante el uso de la salida de datos de la unidad de procesamiento de datos 111. La unidad de generación 112 puede simplemente sumar la salida de datos de la unidad de procesamiento de datos 111, realizar un cálculo lógico tal como XOR, sustituir en una fórmula matemática predeterminada, o cifrar los datos mediante el uso del algoritmo de cifrado, y generar el valor de resultado como los datos de detección de integridad. Si se usan datos de detección de integridad en la comunicación anterior, la unidad de generación 112 acumula y refleja incluso esos datos de detección de integridad anteriores juntos, y genera los datos de detección de integridad.

Los datos de detección de integridad generados en la unidad de generación 112 se agregan a los datos generados en la unidad de procesamiento de datos 111 y se transmiten a la unidad de interfaz 630. En la Figura 6, se ilustra como si la salida de la unidad de procesamiento de datos 111 solo se proporciona a la unidad de generación 112, pero la salida de la unidad de procesamiento de datos 111 puede proporcionarse directamente a la unidad de interfaz 630 o proporcionarse a un multiplexor (no ilustrado). En el caso donde se proporciona un multiplexor, la salida de la unidad de generación 112 también se proporciona al multiplexor, y puede transmitirse a la unidad de interfaz 630 en forma de señal donde los datos y los datos de detección de integridad se incluyen juntos.

La unidad de interfaz 630 transmite la señal que incluye los datos y los primeros datos de detección de integridad al chip CRUM 210.

La unidad de interfaz 630 puede recibir una señal de respuesta desde el chip CRUM 210. Para la conveniencia de explicación, la señal transmitida desde la unidad de interfaz se denominará como una primera señal, y la señal transmitida desde el chip CRUM se denominará como una segunda señal.

Unos segundos datos de detección de integridad incluidos en la segunda señal son datos donde los primeros datos de detección de integridad se han acumulado y reflejado.

La unidad de detección 113 separa los segundos datos de detección de integridad incluidos en la segunda señal recibida a través de la unidad de interfaz 630, y detecta la integridad de los datos incluidos en la segunda señal. Más específicamente, la unidad de detección 113 aplica un método conocido entre el chip CRUM 210 con respecto a los datos restantes después de la separación de los segundos datos de detección de integridad y los datos de detección de integridad que el controlador 610 transmitió anteriormente, y genera los datos de detección de integridad.

La unidad de detección 113 compara los datos de detección de integridad generados en consecuencia con los segundos datos de detección de integridad separados de la segunda señal, y determina si son idénticos. Si son idénticos, la unidad de detección 113 determina que los datos correspondientes son integrales, y si no son idénticos, la unidad de detección 113 determina que los datos correspondientes están en un estado de error.

La unidad de control 114 realiza una comunicación posterior de acuerdo con el resultado de detección mediante la unidad de detección 114. Es decir, si se determina que la segunda señal incluye datos en un estado de error, la unidad de control 114 puede detener la comunicación posterior o hacer otro intento. Si se determina que la segunda señal está en un estado normal, es decir, en un estado integral, la unidad de control 114 realiza la comunicación posterior.

De acuerdo con una modalidad ilustrativa, al determinar que los datos correspondientes están en un estado integral, la unidad de control 114 puede almacenar los datos correspondientes directamente en la unidad de memoria 140.

De acuerdo con una modalidad ilustrativa, la unidad de control 114 puede almacenar temporalmente los datos obtenidos en cada comunicación y los datos de detección de integridad, y una vez que se completa la comunicación final, grabar los datos almacenados temporalmente en la unidad de memoria 140.

La Figura 7 ilustra un dispositivo de formación de imágenes de acuerdo con una modalidad ilustrativa. Como se ilustra en la Figura 7, el cuerpo 700 incluye la unidad de memoria 740 además del controlador 710 que incluye la unidad de procesamiento de datos 711, la unidad de generación 712, y la unidad de detección 713, y la unidad de control 714, y la unidad de interfaz 730. La unidad de memoria 740 incluye una unidad de almacenamiento temporal 741 y una unidad de almacenamiento 742.

En consecuencia, en la unidad de almacenamiento temporal 741, los datos determinados como integrales y los datos de detección de integridad pueden almacenarse temporalmente. Los datos de detección de integridad almacenados temporalmente pueden usarse durante la detección de integridad en el proceso de comunicación posterior.

Es decir, cuando la segunda señal con respecto a la primera señal se transmite después de que la primera señal que incluye los primeros datos de detección de integridad se transmite al chip CRUM 210, la unidad de detección 713 separa los segundos datos de detección de integridad de la segunda señal, y genera nuevos datos de detección de integridad, es decir, los datos sujetos a comparación, mediante el uso de los datos restantes y los datos de detección de integridad almacenados en la unidad de almacenamiento temporal 741. Posteriormente, la unidad de detección 713 compara los datos de detección de integridad recién generados con los segundos datos de detección de integridad en la unidad de almacenamiento temporal 741, y puede determinar la integridad de la segunda señal o los datos incluidos en la segunda señal.

La unidad de generación 712 puede generar, por ejemplo, unos terceros datos de detección de integridad basado en los datos posteriores y los segundos datos de detección de integridad, si existen datos posteriores a transmitir al chip CRUM 210 en el estado en que la segunda señal es integral. En consecuencia, la unidad de interfaz 730 transmite los terceros datos de detección de integridad y la tercera señal que incluye los datos posteriores en el chip CRUM 210. Es decir, como se ilustra en las Figuras 2 a la 4, el controlador y el chip CRUM realizan la comunicación en numerosas ocasiones.

La unidad de detección 713 puede realizar una detección final de la integridad de todas las señales recibidas durante la realización del trabajo de formación de imágenes, mediante el uso de los datos de detección de integridad finales incluidos en la señal recibida en el proceso de realización del trabajo de formación de imágenes. Es decir, como se mencionó anteriormente, los datos de detección de integridad transmitidos y recibidos en cada comunicación se generan al acumular y reflejar los datos de detección de integridad anteriores, y por lo tanto, los datos de detección de integridad finales incluyen todos los datos desde los primeros datos de detección de integridad hasta esos justo antes de los actuales. Por lo tanto, si se determina que los datos son integrales, mediante el uso de los datos de detección de integridad finales, todos los datos almacenados temporalmente se almacenan en la unidad de almacenamiento 742 en la unidad de memoria 740, en base al juicio de que todo el contenido de la comunicación es confiable.

Durante la primera comunicación, el controlador 710 y el chip CRUM 210 incluyen un indicador que notifica que es la primera comunicación, y luego transmiten la señal, y durante la comunicación final, incluyen un indicador que notifica que es la comunicación final, y luego transmiten la señal. En consecuencia, cuando se determina a partir de la señal recibida de la contraparte, el controlador 710 y el chip CRUM 210 realizan la detección final mencionada anteriormente, y almacenan los datos en la unidad de almacenamiento 742.

Tal detección final puede realizarse cuando se completa un trabajo de formación de imágenes, o en cada unidad de período de tiempo predeterminado de acuerdo con las modalidades ilustrativas. También puede realizarse cuando se ingresa un comando de usuario para el almacenamiento de datos, o cuando se ingresa un comando de apagado con respecto al dispositivo de formación de imágenes.

Las Figuras 6 y 7 ilustran una unidad de procesamiento de datos ilustrativa, la unidad de generación, la unidad de detección y la unidad de control se incluyen en el controlador, pero no se limitan necesariamente a tal modalidad. Es decir, al menos una de la unidad de procesamiento de datos, la unidad de generación, la unidad de detección y la unidad de control puede proporcionarse aparte del controlador. En este caso, a diferencia de lo ilustrado en las Figuras 1 a la 4, el controlador puede realizar solo la función original, y la comunicación con el chip CRUM 210 puede realizarse por la unidad de procesamiento de datos, la unidad de generación, la unidad de detección y la unidad de control.

La Figura 8 ilustra una configuración de un chip CRUM 810 de acuerdo con una modalidad ilustrativa de la presente descripción. Como se ilustra en la Figura 8, el chip CRUM 810 incluye una unidad de interfaz 811, una unidad de detección 812, una unidad de generación 813, una unidad de procesamiento de datos 814, una unidad de control 815, una unidad de almacenamiento temporal 816 y una unidad de almacenamiento 817.

La unidad de interfaz 811 recibe la primera señal que incluye los primeros datos y los primeros datos de detección de integridad desde el cuerpo del dispositivo de formación de imágenes, especialmente el controlador montado en el cuerpo.

La unidad de detección 812 separa los primeros datos de detección de integridad de la primera señal y detecta la integridad de la primera señal. El método de detección de la unidad de detección 812 es similar al ilustrado anteriormente, y por lo tanto se omitirá la explicación repetida.

La unidad de almacenamiento temporal 816 almacena temporalmente los primeros datos y los primeros datos de detección de integridad, cuando se determina que la primera señal es integral.

La unidad de procesamiento de datos 814 genera los segundos datos cuando existen segundos datos que deben transmitirse al cuerpo del dispositivo de formación de imágenes.

La unidad de generación 813 genera los segundos datos de detección de integridad mediante el uso de los segundos datos generados y los primeros datos de detección de integridad.

La unidad de control 815 controla la unidad de interfaz para transmitir la segunda señal que incluye los segundos datos y los segundos datos de detección de integridad al cuerpo del dispositivo de formación de imágenes. Además, la unidad de control 815 controla todas las operaciones del chip CRUM. Es decir, como se mencionó anteriormente, cuando el chip CRUM en sí tiene el O/S, la unidad de control 815 puede accionar el chip CRUM mediante el uso del O/S. Una vez que se almacena el programa de inicialización, la inicialización puede realizarse por separado del cuerpo del dispositivo de formación de imágenes.

La unidad de control 815 realiza una operación correspondiente a cada comando recibido desde el cuerpo del dispositivo de formación de imágenes. Es decir, cuando se recibe el comando de lectura, la unidad de control 815 lee los datos almacenados en la unidad de almacenamiento 817 de acuerdo con ese comando, y transmite los datos al dispositivo de formación de imágenes a través de la unidad de interfaz 811. En este proceso, pueden agregarse los datos de detección de integridad.

Mientras tanto, la unidad de detección 812 realiza la detección de integridad en la tercera señal cuando la tercera señal que incluye los terceros datos de detección de integridad generados al acumular y reflejar los segundos datos de detección de integridad.

Cuando se completa el dispositivo de formación de imágenes, la unidad de detección 812 detecta todas las señales recibidas en el proceso de realizar el trabajo de formación de imágenes, mediante el uso de los datos de detección de integridad finales incluidos en la señal recibida en el proceso de realizar el trabajo de formación de imágenes. Cuando la comunicación se completa en el estado de integridad, la unidad de almacenamiento temporal 816 almacena los datos que se han almacenado temporalmente en la unidad de almacenamiento 817.

Es decir, cuando se completa la comunicación, la unidad de control 815 controla la unidad de detección 812 para realizar la detección final mediante el uso de los datos de detección de integridad finales. En consecuencia, cuando se determina que los datos correspondientes son integrales como resultado de la detección final en la unidad de detección 812, la unidad de control 815 almacena los datos que se han almacenado temporalmente en la unidad de almacenamiento temporal 816 en la unidad de almacenamiento 817.

Las operaciones del chip CRUM 810 en la Figura 8 son similares a las operaciones del dispositivo de formación de imágenes en la Figura 7. Es decir, el controlador del dispositivo de formación de imágenes y el chip CRUM de la unidad consumible realizan operaciones que corresponden de manera similar entre sí, como se ilustra en las Figuras 1 a la 4. Por lo tanto, ambas partes deberían generar los datos de detección de integridad y deberían tener algoritmos que realicen detecciones mediante el uso de los datos de detección de integridad generados.

La Figura 9 ilustra un método de comunicación de acuerdo con una modalidad ilustrativa de la presente descripción. El método de comunicación ilustrado en la Figura 9 puede realizarse en un controlador proporcionado en un cuerpo de un dispositivo de formación de imágenes, o en un chip CRUM proporcionado en una unidad consumible.

Como se ilustra en la Figura 9, cuando se generan los datos a transmitir (S910), los datos de detección de integridad se generan mediante el uso de esos datos generados (S920).

Posteriormente, se transmiten los datos de detección de integridad generados y la señal que incluye los datos (S930).

En consecuencia, una señal de respuesta correspondiente a la señal transmitida se recibe desde la contraparte (S940). En la señal de respuesta, se incluyen nuevos datos de detección de integridad generados al acumular y reflejar los datos de detección de integridad transmitidos desde el S930.

La detección de integridad se realiza mediante el uso de los datos de detección de integridad incluidos en la señal de respuesta (S950).

Por lo tanto, de acuerdo con una modalidad ilustrativa, es posible determinar la integridad de cada comunicación mediante el uso de los datos de detección de integridad anteriores de forma acumulativa.

La Figura 10 ilustra un método de comunicación de acuerdo con una modalidad ilustrativa. Como se ilustra en la Figura 10, cuando se generan los datos a transmitir (S1010), los datos de detección de integridad se generan en base a esos datos (S1020). Posteriormente, se transmite la señal que incluye los datos y los datos de detección de integridad (S1030), y se recibe una señal de respuesta con respecto a esa señal (S1040). En consecuencia, los datos de detección de integridad se separan de la señal de respuesta (S1050).

Puede determinarse si los datos son integrales mediante el uso de los datos restantes a partir de los que se han separado los datos de detección de integridad, y los datos de detección de integridad existentes (S1060).

Si se determina que los datos son integrales como resultado de la determinación, los datos se almacenan temporalmente (S1070), mientras que si se determina que los datos están en un estado de error, la comunicación se detiene (S1100) o puede realizarse otro intento.

Si existen datos posteriores en el estado almacenado temporalmente (S1080), la etapa mencionada anteriormente puede realizarse repetidamente. Si no existen datos posteriores, los datos almacenados temporalmente se almacenan de acuerdo con el resultado de detección de integridad de la señal recibida (S1090).

En las modalidades ilustrativas mencionadas anteriormente, excepto desde los datos de detección de integridad transmitidos desde el controlador del dispositivo de formación de imágenes durante la primera inicialización de la comunicación de datos, los datos de detección de integridad se generan al acumular y reflejar los datos de detección de integridad durante la comunicación anterior. Como resultado, los datos de detección de integridad durante la comunicación final incluyen todos los datos de detección de integridad usados en todos los procesos de comunicación. Por lo tanto, pueden registrarse datos exactos.

Por lo tanto, es posible proteger de forma segura la información en el controlador y el chip CRUM de efectos externos tales como el ruido, el punto de contacto deficiente y la piratería.

De acuerdo con una modalidad ilustrativa, puede basarse en el dispositivo de formación de imágenes y el chip CRUM

montado en la unidad consumible usada en el dispositivo de formación de imágenes, pero el método de comunicación mencionado anteriormente puede aplicarse también a otros tipos de dispositivos. Por ejemplo, una modalidad ilustrativa puede aplicarse al caso de comunicación entre un dispositivo fabricado para la comunicación con el chip CRUM y no el dispositivo de formación de imágenes, y también al caso de comunicación entre un dispositivo electrónico normal y una memoria montada en un componente usado en ese dispositivo.

Los programas para realizar los métodos de comunicación de acuerdo con las diversas modalidades ilustrativas de la presente descripción pueden almacenarse en diversos tipos de medios de grabación y usarse.

Un código para realizar los métodos mencionados anteriormente puede almacenarse en varios tipos de medios de grabación legibles en un terminal, tal como RAM (memoria de acceso aleatorio), memoria flash, ROM (memoria de solo lectura), EPROM (ROM programable borrable), EEPROM (ROM electrónicamente borrable y programable), registro, disco duro, disco extraíble, tarjeta de memoria, memoria USB y CD-ROM.

Todas las características descritas en esta especificación (incluidas cualquiera de las reivindicaciones, resumen y dibujos adjuntos), y/o todas las etapas de cualquier método o proceso así descrito, pueden combinarse en cualquier combinación, excepto combinaciones donde al menos algunas de tales características y/o etapas sean mutuamente excluyentes.

REIVINDICACIONES

1. Un chip de Monitoreo de Unidad Reemplazable por el Cliente, CRUM, (810) que se monta en una unidad consumible para un aparato de formación de imágenes y operable para comunicarse con el aparato de formación de imágenes, el chip CRUM (810) **caracterizado porque** comprende:

una unidad de interfaz (811) que es operable para recibir los primeros datos y los primeros datos de detección de integridad generados mediante el uso de los primeros datos de un controlador principal (110) del aparato de formación de imágenes; y
un controlador (815) que es operable, cuando se determina que los primeros datos son integrales, para generar los segundos datos de detección de integridad mediante el uso tanto de los segundos datos que se transmitirán al controlador principal (110) del aparato de formación de imágenes como de los primeros datos de detección de integridad, y para transmitir los segundos datos y los segundos datos de detección de integridad al controlador principal (110) del aparato de formación de imágenes.

2. El chip CRUM (810) de acuerdo con la reivindicación 1, en donde el controlador (815) es operable para transmitir los segundos datos y los segundos datos de detección de integridad al controlador principal (110) del aparato de formación de imágenes en respuesta a la integridad de los primeros datos que se verifican.

3. El chip CRUM de acuerdo con la reivindicación 1, que comprende además:
un almacenamiento temporal (816) para almacenar los primeros datos de detección de integridad y los segundos datos de detección de integridad cuando se determina que los primeros datos son integrales.

4. El chip CRUM (810) de acuerdo con la reivindicación 1, en donde el controlador (815) es operable para generar los cuartos datos de detección de integridad mediante el uso de los terceros datos de detección de integridad, y los cuartos datos a transmitir al controlador principal (110) del aparato de formación de imágenes, en respuesta a los terceros datos y los terceros datos de detección de integridad con respecto a los terceros datos que se reciben desde el controlador principal (110) del aparato de formación de imágenes, y para controlar la unidad de interfaz (811) para transmitir los cuartos datos y los cuartos datos de detección de integridad al controlador principal (110) del aparato de formación de imágenes.

5. El chip CRUM (810) de acuerdo con la reivindicación 4, en donde el controlador (815) es operable para detectar la integridad de los terceros datos mediante el uso de los terceros datos de detección de integridad.

6. El chip CRUM (810) de acuerdo con la reivindicación 4, en donde los primeros datos comprenden los primeros datos de comando y la primera información de indicador para notificar una ubicación de los primeros datos de detección de integridad, los segundos datos comprenden los segundos datos de comando, los segundos datos de resultado y la segunda información de indicador para notificar una ubicación de los segundos datos de detección de integridad, los terceros datos comprenden los terceros datos de comando y la tercera información de indicador para notificar una ubicación de los terceros datos de detección de integridad, y los cuartos datos comprenden los cuartos datos de comando, los cuartos datos de resultado y la cuarta información de indicador para notificar una ubicación de los cuartos datos de detección de integridad.

7. El chip CRUM (810) de acuerdo con la reivindicación 1, en donde los primeros datos comprenden el primer valor arbitrario, y los segundos datos comprenden el segundo valor arbitrario y en donde el chip CRUM (810) se configura para generar un Código de Autenticación de Mensaje mediante el uso de los primeros datos y los segundos datos.

8. Un método de autenticación de un chip de Monitoreo de Unidad Reemplazable por el Cliente, CRUM, (810) que se monta en una unidad consumible para un aparato de formación de imágenes y operable para comunicarse con el aparato de formación de imágenes, **caracterizado porque** comprende:

recibir desde un controlador principal (110) del aparato de formación de imágenes los primeros datos y los primeros datos de detección de integridad generados mediante el uso de los primeros datos;
generar los segundos datos de detección de integridad mediante el uso tanto de los segundos datos que se transmitirán al controlador principal (110) del aparato de formación de imágenes como de los primeros datos de detección de integridad cuando se determina que los primeros datos son integrales; y
transmitir los segundos datos y los segundos datos de detección de integridad al controlador principal (110) del aparato de formación de imágenes cuando se determina que los primeros datos son integrales.

9. El método de acuerdo con la reivindicación 8, que comprende además:
probar, en un controlador del chip CRUM, la integridad de los primeros datos mediante el uso de los primeros datos de detección de integridad.

10. El método de acuerdo con la reivindicación 8, que comprende además:
almacenar temporalmente los primeros y segundos datos de detección de integridad cuando se determina que los primeros datos son integrales.

11. El método de acuerdo con la reivindicación 8, que comprende además:

recibir desde el controlador principal (110) del aparato de formación de imágenes, los terceros datos y los terceros datos de detección de integridad con respecto a los terceros datos;
generar los cuartos datos de detección de integridad mediante el uso de los cuartos datos a transmitir al controlador principal del aparato de formación de imágenes y los terceros datos de detección de integridad; y
transmitir los cuartos datos y los cuartos datos de detección de integridad al controlador principal del aparato de formación de imágenes.

12. El método de acuerdo con la reivindicación 11, que comprende además:
probar los terceros datos mediante el uso de los terceros datos de detección de integridad.

13. El método de acuerdo con la reivindicación 8, en donde los primeros datos comprenden el primer valor arbitrario, y los segundos datos comprenden el segundo valor arbitrario y en donde el método comprende generar un Código de Autenticación de Mensaje mediante el uso de los primeros datos y los segundos datos.

14. Un aparato consumible, que comprende:
una unidad consumible que se monta en un aparato de formación de imágenes; y
un chip de Monitoreo de Unidad Reemplazable por el Cliente, CRUM, de cualquiera de las reivindicaciones 1 a la 7.

15. El aparato consumible de acuerdo con la reivindicación 14, la unidad consumible es cualquiera de un dispositivo de electrificación, un dispositivo de exposición a la luz, un dispositivo de desarrollo, un dispositivo de transferencia, un dispositivo de asentamiento, un rodillo, una cinta y un tambor OPC.

FIGURA 1

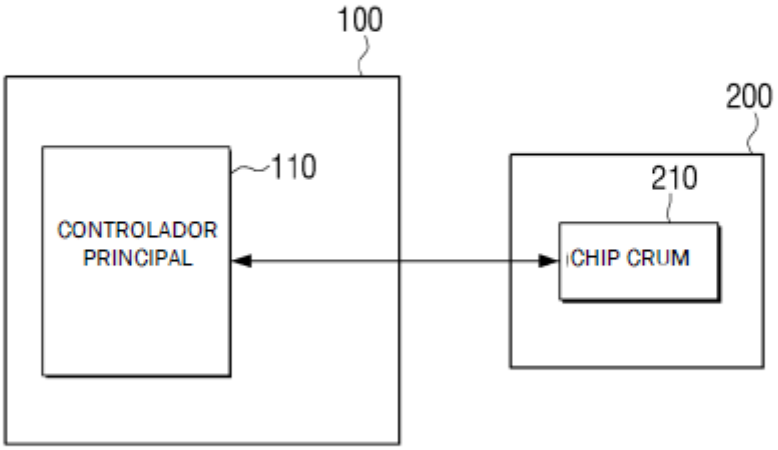


FIGURA 2

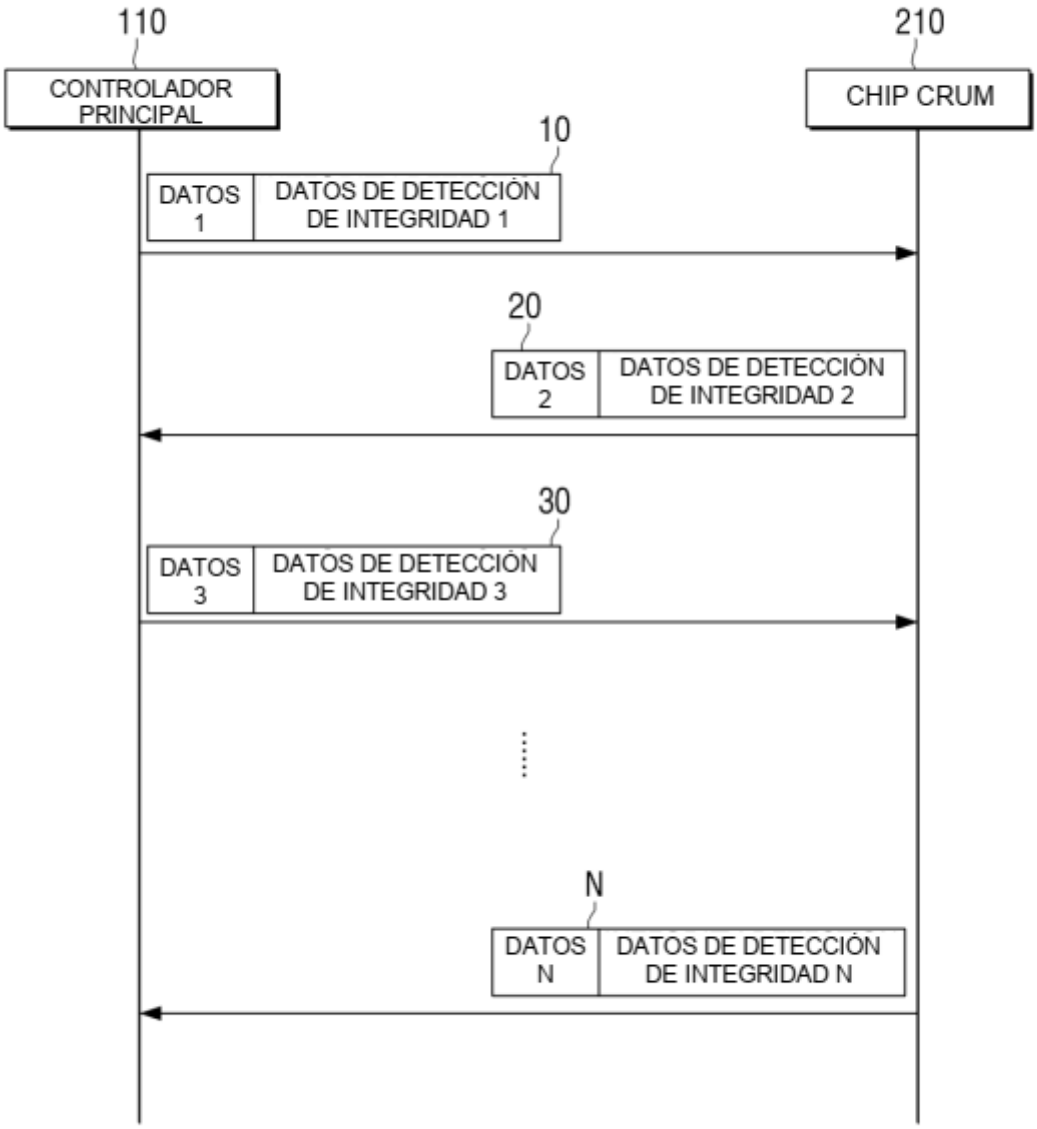

110
CONTROLADOR PRINCIPAL
210
CHIP CRUM
10
DATOS 1
DATOS DE DETECCIÓN DE INTEGRIDAD 1
20
DATOS 2
DATOS DE DETECCIÓN DE INTEGRIDAD 2
30
DATOS 3
DATOS DE DETECCIÓN DE INTEGRIDAD 3
N
DATOS N
DATOS DE DETECCIÓN DE INTEGRIDAD N

FIGURA 3

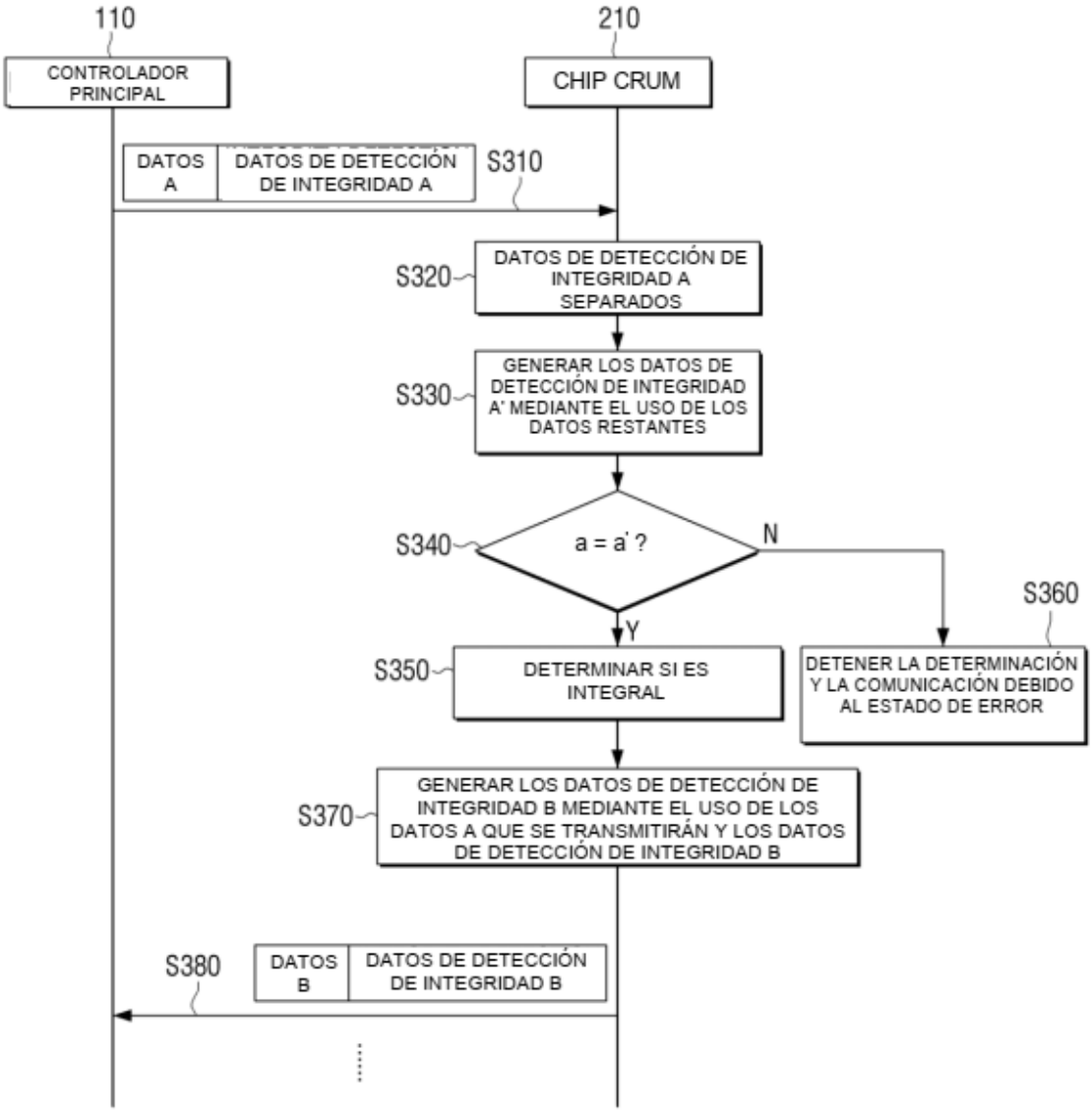

110
CONTROLADOR PRINCIPAL
210
CHIP CRUM
DATOS A
DATOS DE DETECCIÓN DE INTEGRIDAD A
S310
S320
DATOS DE DETECCIÓN DE INTEGRIDAD A SEPARADOS
S330
GENERAR LOS DATOS DE DETECCIÓN DE INTEGRIDAD A' MEDIANTE EL USO DE LOS DATOS RESTANTES
S340
a = a' ?
N
Y
S360
DETENER LA DETERMINACIÓN Y LA COMUNICACIÓN DEBIDO AL ESTADO DE ERROR
S350
DETERMINAR SI ES INTEGRAL
S370
GENERAR LOS DATOS DE DETECCIÓN DE INTEGRIDAD B MEDIANTE EL USO DE LOS DATOS A QUE SE TRANSMITIRÁN Y LOS DATOS DE DETECCIÓN DE INTEGRIDAD B
S380
DATOS B
DATOS DE DETECCIÓN DE INTEGRIDAD B

FIGURA 4

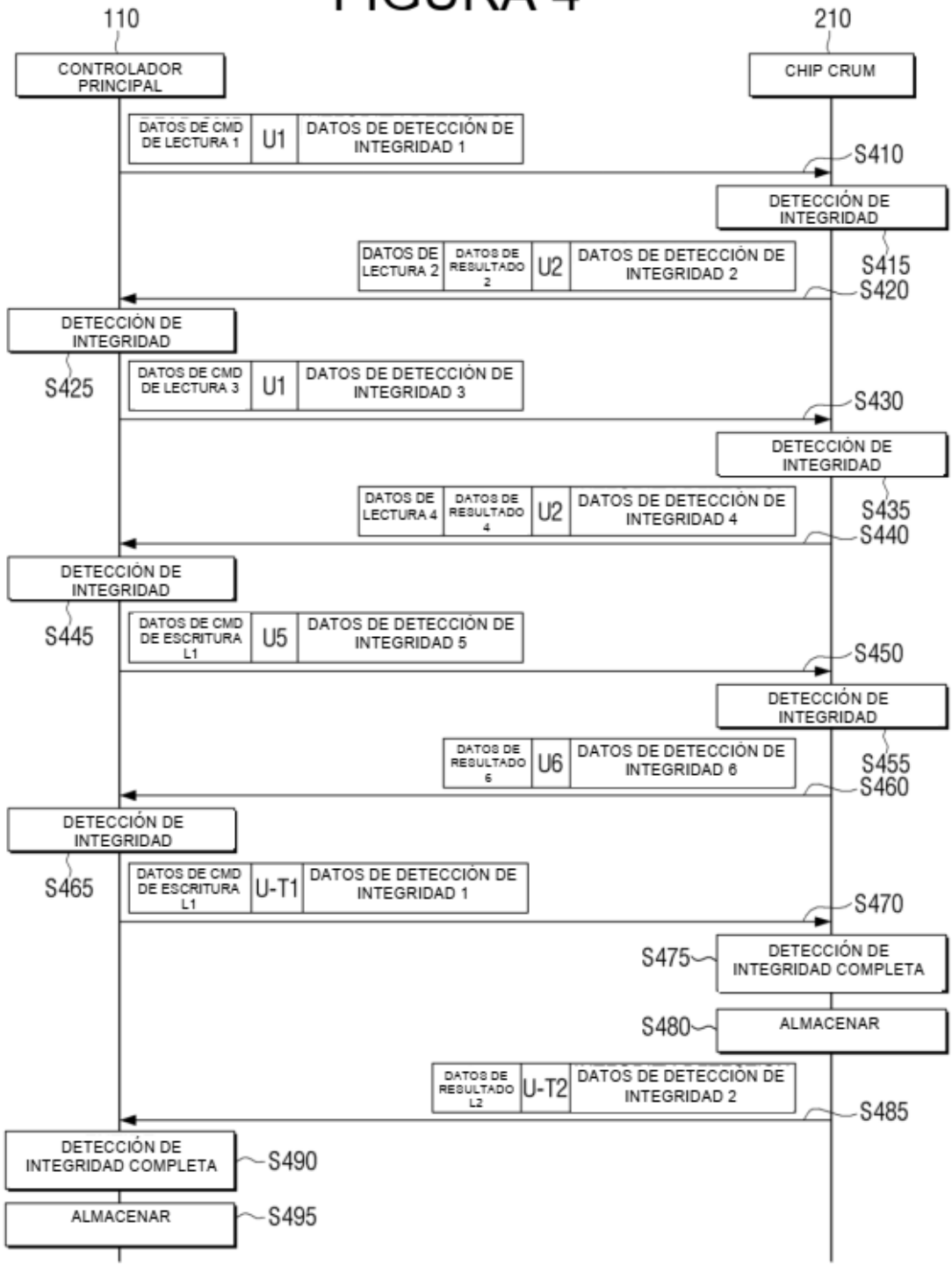

110
CONTROLADOR PRINCIPAL
210
CHIP CRUM
DATOS DE CMD DE LECTURA 1
U1
DATOS DE DETECCIÓN DE INTEGRIDAD 1
S410
DETECCIÓN DE INTEGRIDAD
S415
DATOS DE LECTURA 2
DATOS DE RESULTADO 2
U2
DATOS DE DETECCIÓN DE INTEGRIDAD 2
S420
DETECCIÓN DE INTEGRIDAD
S425
DATOS DE CMD DE LECTURA 3
U1
DATOS DE DETECCIÓN DE INTEGRIDAD 3
S430
DETECCIÓN DE INTEGRIDAD
S435
DATOS DE LECTURA 4
DATOS DE RESULTADO 4
U2
DATOS DE DETECCIÓN DE INTEGRIDAD 4
S440
DETECCIÓN DE INTEGRIDAD
S445
DATOS DE CMD DE ESCRITURA L1
U5
DATOS DE DETECCIÓN DE INTEGRIDAD 5
S450
DETECCIÓN DE INTEGRIDAD
S455
DATOS DE RESULTADO 6
U6
DATOS DE DETECCIÓN DE INTEGRIDAD 6
S460
DETECCIÓN DE INTEGRIDAD
S465
DATOS DE CMD DE ESCRITURA L1
U-T1
DATOS DE DETECCIÓN DE INTEGRIDAD 1
S470
S475
DETECCIÓN DE INTEGRIDAD COMPLETA
S480
ALMACENAR
DATOS DE RESULTADO L2
U-T2
DATOS DE DETECCIÓN DE INTEGRIDAD 2
S485
DETECCIÓN DE INTEGRIDAD COMPLETA
S490
ALMACENAR
S495

FIGURA 5

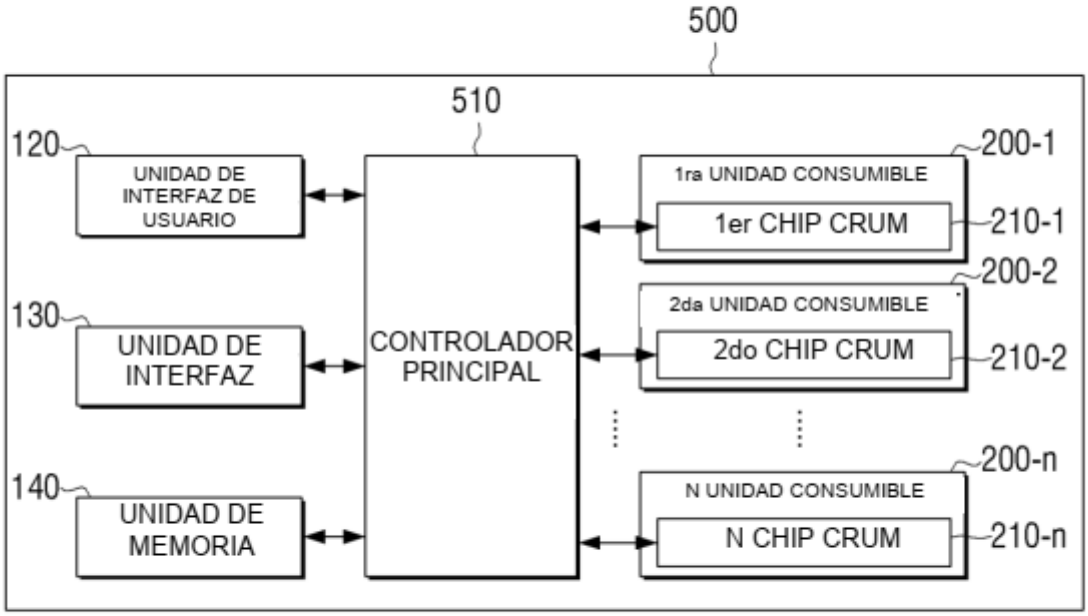

500
510
120
UNIDAD DE INTERFAZ DE USUARIO
130
UNIDAD DE INTERFAZ
140
UNIDAD DE MEMORIA
CONTROLADOR PRINCIPAL
200-1
1ra UNIDAD CONSUMIBLE
1er CHIP CRUM
210-1
200-2
2da UNIDAD CONSUMIBLE
2do CHIP CRUM
210-2
200-n
N UNIDAD CONSUMIBLE
N CHIP CRUM
210-n

FIGURA 6

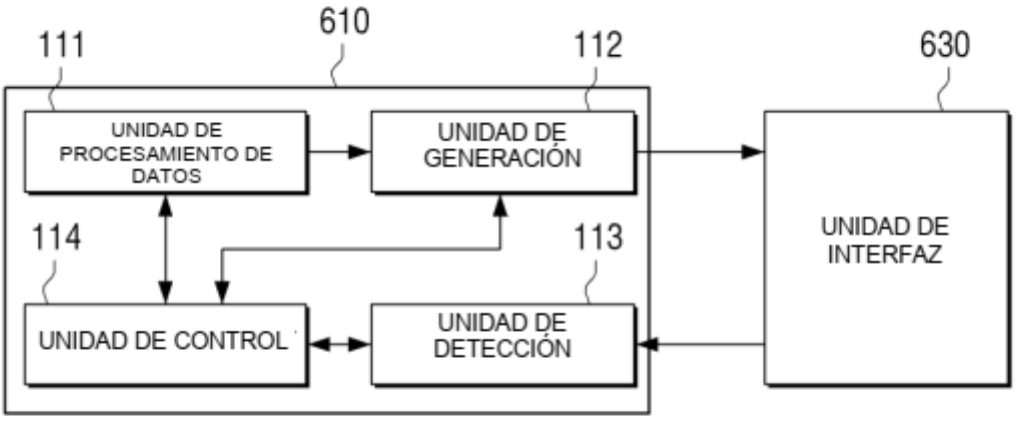

111
610
112
630
UNIDAD DE PROCESAMIENTO DE DATOS
UNIDAD DE GENERACIÓN
UNIDAD DE INTERFAZ
114
113
UNIDAD DE CONTROL
UNIDAD DE DETECCIÓN

FIGURA 7

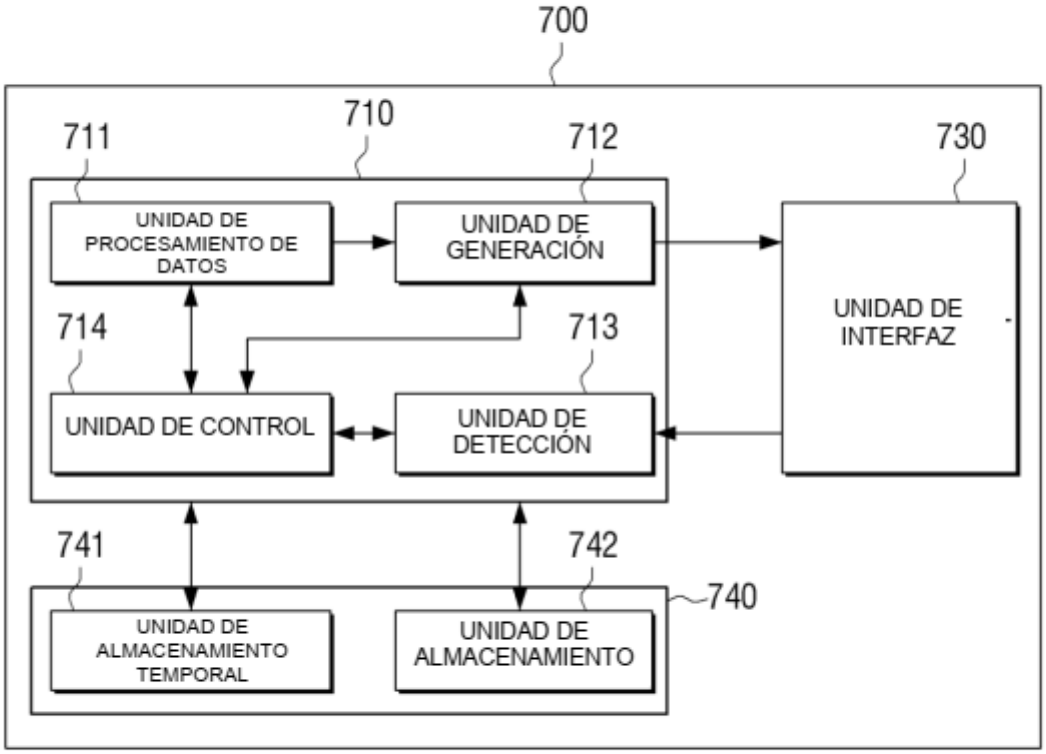

700
710
711
712
730
UNIDAD DE PROCESAMIENTO DE DATOS
UNIDAD DE GENERACIÓN
UNIDAD DE INTERFAZ
714
713
UNIDAD DE CONTROL
UNIDAD DE DETECCIÓN
741
742
740
UNIDAD DE ALMACENAMIENTO TEMPORAL
UNIDAD DE ALMACENAMIENTO

FIGURA 8

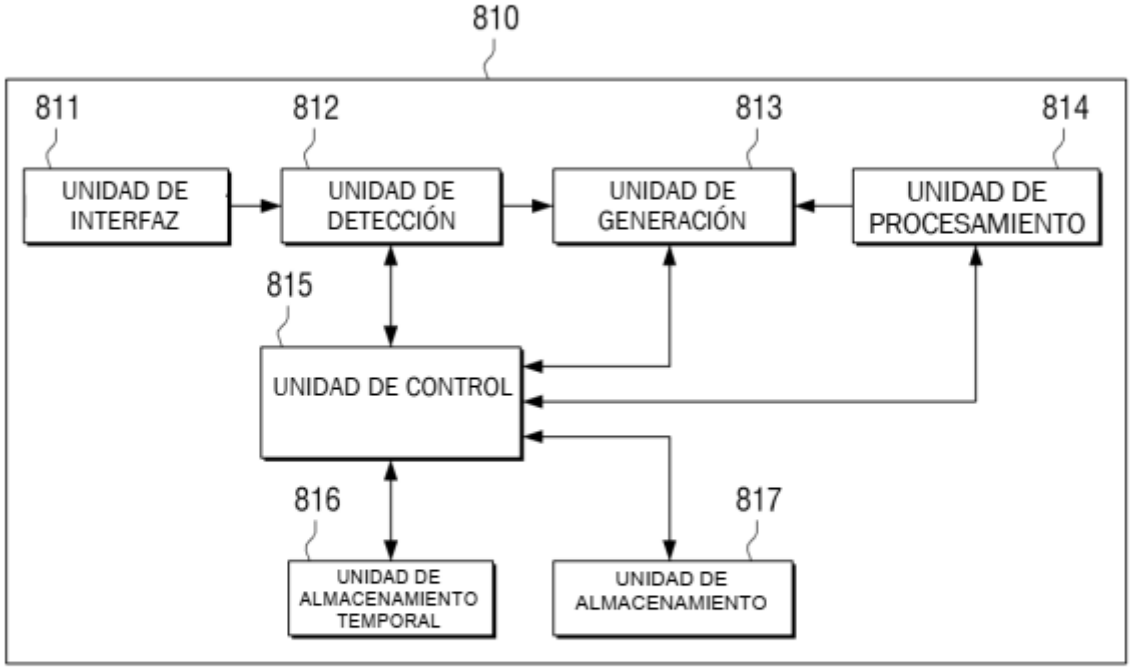

810
811
UNIDAD DE INTERFAZ
812
UNIDAD DE DETECCIÓN
813
UNIDAD DE GENERACIÓN
814
UNIDAD DE PROCESAMIENTO
815
UNIDAD DE CONTROL
816
UNIDAD DE ALMACENAMIENTO TEMPORAL
817
UNIDAD DE ALMACENAMIENTO

FIGURA 9

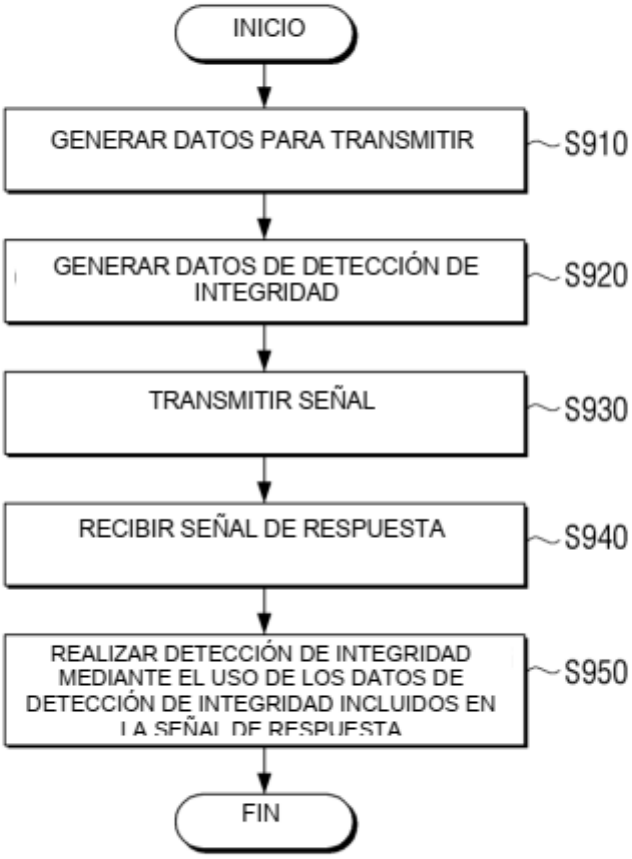
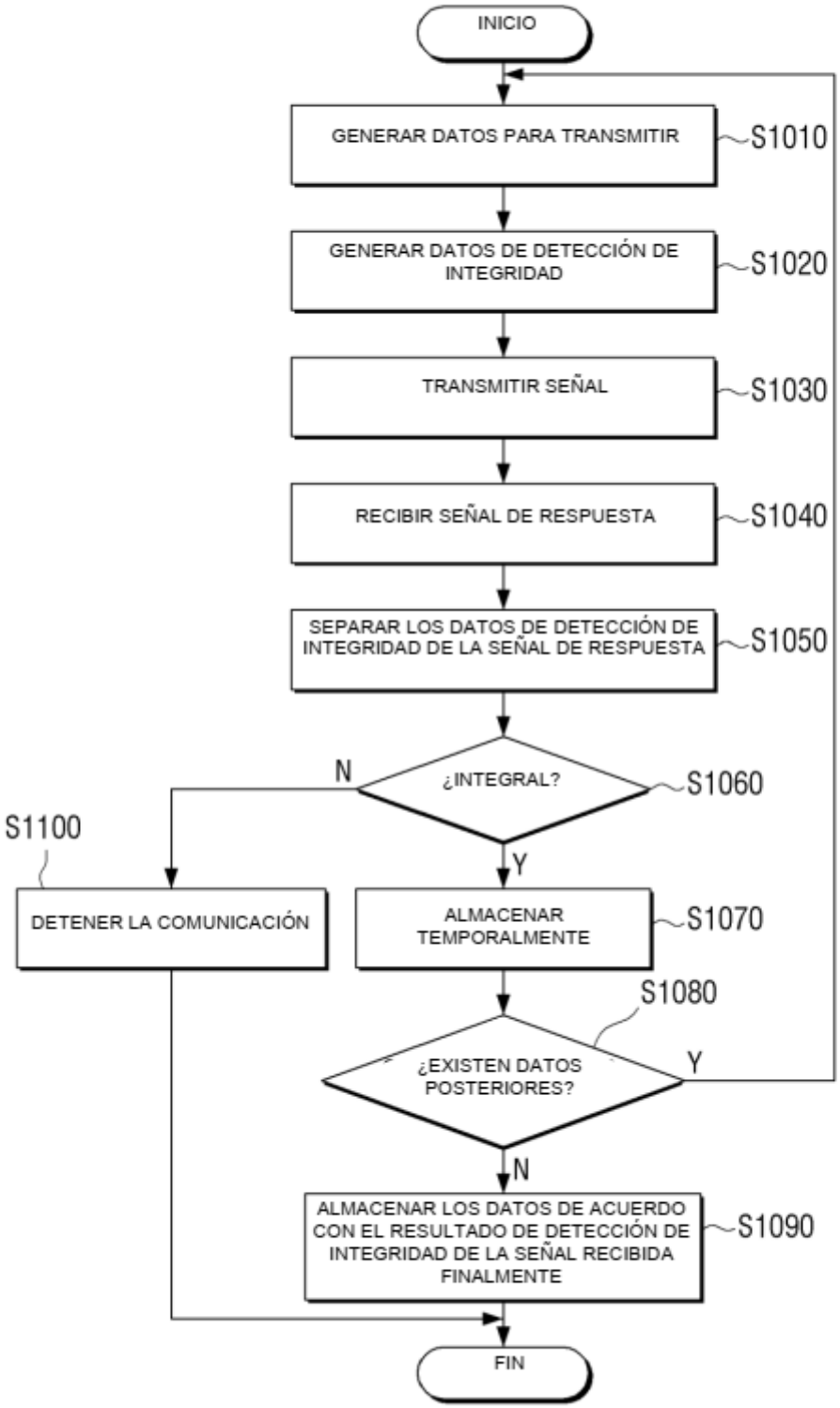

INICIO
GENERAR DATOS PARA TRANSMITIR
S910
GENERAR DATOS DE DETECCIÓN DE INTEGRIDAD
S920
TRANSMITIR SEÑAL
S930
RECIBIR SEÑAL DE RESPUESTA
S940
REALIZAR DETECCIÓN DE INTEGRIDAD MEDIANTE EL USO DE LOS DATOS DE DETECCIÓN DE INTEGRIDAD INCLUIDOS EN LA SEÑAL DE RESPUESTA
S950
FIN

FIGURA 10


INICIO
GENERAR DATOS PARA TRANSMITIR
S1010
GENERAR DATOS DE DETECCIÓN DE INTEGRIDAD
S1020
TRANSMITIR SEÑAL
S1030
RECIBIR SEÑAL DE RESPUESTA
S1040
SEPARAR LOS DATOS DE DETECCIÓN DE INTEGRIDAD DE LA SEÑAL DE RESPUESTA
S1050
¿INTEGRAL?
S1060
N
Y
S1100
DETENER LA COMUNICACIÓN
ALMACENAR TEMPORALMENTE
S1070
S1080
¿EXISTEN DATOS POSTERIORES?
Y
N
ALMACENAR LOS DATOS DE ACUERDO CON EL RESULTADO DE DETECCIÓN DE INTEGRIDAD DE LA SEÑAL RECIBIDA FINALMENTE
S1090
FIN