(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 710 437**

(51) Int. CI.:

G03G 15/08 (2006.01)
G03G 21/18 (2006.01)

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(96) Fecha de presentación y número de la solicitud europea: **19.07.2013 E 13177300 (4)**

(97) Fecha y número de publicación de la concesión europea: **23.01.2019 EP 2746859**

(54) Título: **Chip de CRUM y dispositivo de formación de imágenes para autenticación y comunicación, y métodos de los mismos**

(30) Prioridad:

24.12.2012 KR 20120152433
30.04.2013 KR 20130048712

(45) Fecha de publicación y mención en BOPI de la traducción de la patente:
25.04.2019

(73) Titular/es:

HP PRINTING KOREA CO., LTD. (100.0%)
129, Samsung-ro, Yeongtong-gu, Suwon-si
Gyeonggi-do 16677 , KR

(72) Inventor/es:

LEE, JAE-YOON y
WOO, HONG-ROK

(74) Agente/Representante:

ELZABURU, S.L.P

DESCRIPCIÓN

Chip de CRUM y dispositivo de formación de imágenes para autenticación y comunicación, y métodos de los mismos

Antecedentes

Campo

Las realizaciones tratadas en la presente memoria se relacionan con un chip de CRUM y un dispositivo de formación de imágenes para autenticación y comunicación y métodos de los mismos, y más particularmente, con un chip de Monitorización de Unidad Sustituible por el Cliente (CRUM) y un dispositivo de formación de imágenes para autenticación y comunicación para detectar si los datos son integrales, usando datos de detección de integridad en un proceso de comunicación, y un método de los mismos.

Descripción de la técnica relacionada

A medida que los ordenadores llegan a estar cada vez más extendidos, la velocidad de diseminación de los dispositivos periféricos de ordenadores también está aumentando. Los dispositivos periféricos de ordenadores incluyen dispositivos de formación de imágenes, tales como impresoras, facsímiles, escáneres, copiadoras 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 imagen, y de esta manera 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 ha de ser sustituida. Tales piezas o componentes que son sustituibles en el proceso de uso de un dispositivo de formación de imágenes se pueden definir como unidades consumibles o unidades sustituibles. Por comodidad de explicación, se hará referencia a éstos en este documento como unidades consumibles.

Además de estas unidades que se deben sustituir debido al agotamiento de la tinta o del tóner, como se ha tratado anteriormente, también hay unidades consumibles que tienen características que cambian cuando las unidades se usan durante más de un cierto período de tiempo, y de este modo se sustituyen para lograr una calidad de impresión satisfactoria. Unidades consumibles incluyen sustitución de color para máquinas de revelado, y piezas tales como correas de transferencia intermedia.

En el caso de dispositivos de formación de imágenes por láser, se pueden usar unidades de electrificación, unidades intermedias o unidades de asentamiento, en las que se pueden desgastar o degenerar diversos tipos de rodillos y correas usados en cada unidad cuando se usan durante más tiempo que la vida útil marginal. Por consiguiente, la calidad de imagen se puede deteriorar gravemente. Un usuario debe sustituir cada componente, es decir, cada unidad consumible en un período de sustitución adecuado de modo que se pueda realizar la operación de impresión para producir imágenes limpias.

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

Es decir, es posible registrar diversa información de uso, tal como el número de papel impreso, el número de puntos de salida y el período de uso en la memoria de la unidad consumible, para gestión de un tiempo para sustituir la unidad consumible.

Como ejemplo, las organizaciones a gran escala, tales como oficinas públicas, universidades y empresas, emplean Servicios de Impresión Gestionados (MPS) para intentar gestionar una pluralidad de aparatos de formación de imágenes con facilidad. Un servicio de soluciones integradas que usa MSP puede proporcionar las funciones de cálculo de tarifas de uso de consumibles para cada grupo o cada individuo y tarificarles en consecuencia y las funciones de comprobación de la vida útil de los consumibles y encargar los consumibles antes de que se agoten. Tales funciones se pueden proporcionar en base a la información de uso exacta de los consumibles.

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 uno con otro. No obstante, hay numerosas variables en el proceso de comunicación. Por ejemplo, puede haber un ataque por un pirata informático que intenta controlar el controlador o la unidad de memoria con propósitos maliciosos.

Además, puede haber una interrupción por ruido causada, por ejemplo, por un circuito electrónico o un motor proporcionado en un dispositivo de formación de imágenes. Pueden ocurrir incidentes inesperados, tales como una sustancia extraña que se introduce en una parte de conexión entre un cuerpo principal y una unidad consumible de un dispositivo de formación de imágenes, un corte de conexión debido a la vibración durante las operaciones, y/o una señal de interferencia eléctrica que se aplica a través de la parte de conexión.

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 el número de páginas de impresión, número de puntos y el volumen de tóner restante a un controlador, y copia la información en una memoria no volátil del

controlador. Después de que sean leídos los datos como un valor incorrecto, por ejemplo, tal como 0xFFFFFFFF, hay un riesgo de que el controlador pueda percibir que la vida útil de la unidad consumible correspondiente ha finalizado. En este caso, la unidad consumible ya no será capaz de ser usada.

Además, la unidad consumible de un dispositivo de formación de imágenes puede tener una estructura que puede ser desmontable. Normalmente no se accede a la memoria de una unidad consumible y solamente se usa la memoria de un dispositivo de formación de imágenes durante una operación de impresión del dispositivo de formación de imágenes debido, por ejemplo, a la vibración del motor y al ruido del circuito que pueden ocurrir durante la operación. De este modo, la comunicación entre la memoria de la unidad consumible y el dispositivo de formación de imágenes se puede realizar solamente en ocasiones limitadas, por ejemplo, cuando la unidad consumible se monta en el dispositivo de formación de imágenes de modo que la memoria de la unidad consumible y la memoria del dispositivo de formación de imágenes están sincronizados una con otra, o cuando la unidad consumible se actualiza para cambios después de que se completa una operación de impresión y se detiene un motor.

Como puede haber una cantidad considerable de datos almacenados y gestionados en la unidad consumible, se pueden requerir varias funciones complementarias, que llevan un tiempo de comunicación prolongado. Por consiguiente, cuando una unidad consumible se sustituye durante la comunicación, pueden ocurrir problemas. Como ejemplo, una información de uso de consumibles de una unidad de consumibles 1 indica, por ejemplo, 100 páginas de impresión, 200 puntos de salida y 300 veces de accionamiento del motor, y una información de uso de consumibles de una unidad consumibles 2 indica, por ejemplo, 200 páginas de impresión, 300 puntos de salida, y 400 veces de accionamiento del motor. En este caso de ejemplo, si la unidad consumible 1 está montada en un dispositivo de formación de imágenes, la unidad consumible 1 se puede sincronizar con la memoria y los datos del dispositivo de formación de imágenes. Si la unidad consumible 1 se sustituye por la unidad consumible 2 en el proceso de sincronización, es decir, solamente los datos de 100 páginas de impresión y 200 puntos de salida de la unidad consumible 1 se almacenan en la memoria del dispositivo de formación de imágenes y entonces la unidad consumible 1 se sustituye por la unidad consumible 2, se puede realizar de nuevo la autenticación. Posteriormente, los datos de 400 veces de accionamiento del motor se pueden copiar en la memoria del dispositivo de formación de imágenes. Como resultado, la memoria del dispositivo de formación de imágenes indica, por ejemplo, 100 páginas de impresión, 200 puntos de salida y 400 veces de accionamiento del motor, que no son los valores correctos. En este caso de ejemplo, si la unidad consumible 2 se actualiza para cambios después de que se complete una operación de impresión en el dispositivo de formación de imágenes, los datos de 100 páginas de impresión y 200 puntos de salida almacenados en la memoria del dispositivo de formación de imágenes se pueden almacenar en la unidad consumible 2, mientras que los datos reales de la unidad consumible 2 indican 200 páginas de impresión y 300 puntos de salida. En la medida que las páginas de impresión llegan a ser 100 en lugar de 200, la unidad consumible correspondiente tiene valores de datos incorrectos y, de este modo, puede causar problemas.

Además, un dispositivo de formación de imágenes puede tener y usar una pluralidad de unidades consumibles en un canal del Circuito Inter-Integrado (I2C), en cuyo caso, las unidades consumibles se pueden categorizar por una dirección de esclavo en el canal I2C. En este caso, si una dirección de esclavo se modifica al ID de otra unidad consumible debido a algunos problemas temporales, los datos incorrectos se pueden almacenar en la memoria de la otra unidad consumible.

Además, con respecto a una unidad consumible cuya vida útil ha finalizado, un pirata informático puede intentar reiniciar la información de usuario consumible, por ejemplo, a un valor de “0” con un propósito malicioso, con el fin de reciclar inadecuadamente la unidad consumible. Por consiguiente, un usuario puede intentar usar una unidad consumible cuya vida ha finalizado, causando problemas tales como la rotura del dispositivo de formación de imágenes o el deterioro de la definición, y el usuario puede no ser provisto con información exacta con respecto a las unidades consumibles y, además, un servicio de solución integrado puede no estar disponible debido a los problemas de MPS causados por información de consumibles incorrecta.

Por consiguiente, se requiere la necesidad de una tecnología que detecte eficientemente errores de comunicación entre una unidad consumible y un dispositivo de formación de imágenes para buscar la seguridad de los datos.

El documento US 2009/222664 A1 describe un chip que se puede montar en una unidad sustituible usada en un trabajo de formación de imágenes. El documento EP 0 281 223 A2 describe un sistema de mensajería seguro para terminales interconectados.

Compendio

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

Un aspecto de una realización ejemplar se refiere a un chip de CRUM y un dispositivo de formación de imágenes para la seguridad de comunicación, que usan datos de detección de integridad, y un método de comunicación de los mismos.

Según la presente invención, se proporciona un aparato y un método como se expone en las reivindicaciones

adjuntas. Otras características de la invención serán evidentes a partir de las reivindicaciones dependientes, y la descripción que sigue.

Un aparato de formación de imágenes según una realización ejemplar incluye un cuerpo principal que incluye un controlador principal capaz de controlar las operaciones del aparato de formación de imágenes, una unidad consumible que está montada en el cuerpo principal para comunicarse con el controlador principal, y un chip de Monitorización de Unidad Sustituible por el Cliente (CRUM) que se proporciona en la unidad consumible y almacena información con respecto a la unidad consumible, y el controlador principal y el chip de CRUM realizan la comunicación de datos si la autenticación tiene éxito, en donde la autenticación se realiza a través de una pluralidad de procesos de autenticación, y los datos de detección de integridad que se generan reflejando los datos de detección de integridad previos se usan en al menos dos procesos de autenticación de entre la pluralidad de procesos de autenticación.

El controlador principal y el chip de CRUM pueden generar datos de detección de integridad finales reflejando de manera acumulativa todos los datos de detección de integridad que se han transmitido o recibido en procesos de autenticación previos en un proceso de autenticación final de entre la pluralidad de procesos de autenticación.

El controlador principal y el chip de CRUM pueden transmitir/recibir una señal que incluye los datos de detección de integridad en un proceso de autenticación para generar una clave de sesión y un proceso de autenticación para verificar la compatibilidad de entre la pluralidad de procesos de autenticación.

El controlador principal y el chip de CRUM pueden realizar al menos un proceso de autenticación entre el proceso de autenticación para generar una clave de sesión y el proceso de autenticación para verificar la compatibilidad.

Cuando comienza el proceso de autenticación para generar una clave de sesión, el controlador principal puede transmitir una señal incluyendo primeros datos y primeros datos de detección de integridad al chip de CRUM, y el chip de CRUM puede generar segundos datos de detección de integridad usando segundos datos y los primeros datos de detección de integridad y transmitir una señal que incluye los segundos datos y los segundos datos de detección de integridad al controlador principal, y cada uno de los primeros datos y los segundos datos pueden incluir datos relacionados con una clave de sesión con el fin de generar una clave de sesión.

Cuando comienza el proceso de autenticación para verificar la compatibilidad, el controlador principal puede generar terceros datos de detección de integridad usando terceros datos, los primeros datos de integridad y los segundos datos de integridad y transmiten una señal que incluye los terceros datos y los terceros datos de detección de integridad al chip de CRUM, el chip de CRUM puede generar cuartos datos de detección de integridad usando cuartos datos, y los primeros a los terceros datos de detección de integridad y transmitir una señal que incluye los cuartos datos y los cuartos datos de detección de integridad, y los terceros datos puede incluir información de índice en una tabla almacenada previamente en el aparato de formación de imágenes, y los cuartos datos pueden incluir un valor correspondiente a la información del índice.

Cada uno del controlador principal y el chip de CRUM, cuando una señal que incluye los datos de detección de integridad se recibe de una contraparte, puede separar los datos de detección de integridad de la señal recibida y comparar los datos de detección de integridad separados con datos de detección de integridad que se generan por sí mismo a partir de los datos restantes con el fin de verificar la integridad de la señal.

Un aparato de formación de imágenes según una realización ejemplar incluye una unidad de interfaz que está conectada a un chip de CRUM montado en una unidad consumible incorporada en el aparato de formación de imágenes y un controlador que, cuando ocurre un evento donde se requiere autenticación, autentica el chip de CRUM realizando una pluralidad de procesos de autenticación del chip de CRUM, y el controlador transmite/recibe una señal que incluye datos de detección de integridad en un proceso de autenticación para generar una clave de sesión y un proceso de autenticación para verificar la compatibilidad de entre la pluralidad de procesos de autenticación, y los datos de detección de integridad se generan reflejando de manera acumulativa al menos un dato de detección de integridad incluido en una señal recibida previamente.

Un chip de CRUM que se puede montar en una unidad consumible de un aparato de formación de imágenes según una realización ejemplar incluye una unidad de interfaz que recibe una señal que incluye primeros datos y primeros datos de detección de integridad con respecto a los primeros datos de un cuerpo principal del aparato de formación de imágenes, una unidad de prueba que separa los primeros datos de detección de integridad de la señal recibida con el fin de verificar la integridad de la señal, una unidad de generación que genera segundos datos de detección de integridad usando segundos datos para la autenticación con un cuerpo principal del dispositivo de formación de imágenes y los primeros datos de detección de integridad, y un controlador que realiza autenticación transmitiendo una señal que incluye los segundos datos y los segundos datos de detección de integridad a un cuerpo principal del dispositivo de formación de imágenes a través de la unidad de interfaz.

Cada uno de los primeros datos y los segundos datos pueden incluir datos relacionados con una clave de sesión con el fin de generar una clave de sesión, y el controlador puede generar la clave de sesión usando los primeros datos y los segundos datos, y realizar una pluralidad de procesos de autenticación posteriores.

La pluralidad de procesos de autenticación posteriores puede comprender un segundo proceso de autenticación para sincronizar una primera tabla almacenada en cada uno de un cuerpo principal del dispositivo de formación de imágenes y el chip de CRUM, un tercer proceso de autenticación para sincronizar una segunda tabla almacenada en cada uno del cuerpo principal del dispositivo de formación de imágenes y el chip de CRUM, y un cuarto proceso de autenticación para determinar la compatibilidad entre el dispositivo de formación de imágenes y el chip de CRUM en base a al menos una de la primera y segunda tablas.

El controlador puede generar y transmitir datos de detección de integridad finales reflejando todos los datos de detección de integridad que se han transmitido y recibido en el cuarto proceso de autenticación.

Un método para autenticar un aparato de formación de imágenes según una realización ejemplar incluye determinar si ocurre un evento que requiere autenticación de una unidad consumible montada en el dispositivo de formación de imágenes y, en caso de que ocurra el evento, realizar la autenticación de un chip de CRUM montado en la unidad consumible por un controlador principal del dispositivo de formación de imágenes para autenticar el chip de CRUM, y la autenticación se realiza a través de una pluralidad de procesos de autenticación, y los datos de detección de integridad generados reflejando datos de detección de integridad previos se usan en al menos dos procesos de autenticación de entre la pluralidad de procesos de autenticación.

Los datos de detección de integridad que se transmiten/reciben en un proceso de autenticación final de entre la pluralidad de procesos de autenticación se pueden generar reflejando de manera acumulativa todos los datos de detección de integridad que se han transmitido o recibido en procesos de autenticación previos.

La autenticación puede comprender una primera operación de autenticación en la que el controlador principal transmite una señal que incluye primeros datos y primeros datos de detección de integridad al chip de CRUM, y el chip de CRUM genera segundos datos de detección de integridad usando segundos datos y los primeros datos de detección de integridad y transmite una señal que incluye los segundos datos y los segundos datos de detección de integridad al controlador principal y una segunda operación de autenticación en la que el controlador principal genera terceros datos de detección de integridad usando terceros datos, los primeros datos de detección de integridad y los segundos datos de detección de integridad y transmite una señal que incluye los terceros datos y los terceros datos de detección de integridad al chip de CRUM, y el chip de CRUM genera cuartos datos de detección de integridad usando cuartos datos y los primeros a los terceros datos de detección de integridad y transmite una señal que incluye los cuartos datos y los cuartos datos de detección de integridad al controlador principal, en donde cada uno de los primeros datos y los segundos datos incluyen datos relacionados con una clave de sesión con el fin de generar una clave de sesión, en donde los terceros datos incluyen información de índice en una tabla almacenada previamente en el aparato de formación de imágenes, y los cuartos datos incluyen un valor correspondiente a la información de índice.

Un método para autenticar un chip de CRUM que se puede montar en una unidad consumible de un aparato de formación de imágenes según una realización ejemplar incluye recibir una señal que incluye primeros datos y primeros datos de detección de integridad para autenticación de un cuerpo principal del aparato de formación de imágenes, probar la integridad de la señal separando los primeros datos de detección de integridad de la señal recibida, generar segundos datos de detección de integridad usando segundos datos y los primeros datos de detección de integridad para autenticación con un cuerpo principal del aparato de formación de imágenes, y realizar autenticación transmitiendo una señal que incluye los segundos datos y los segundos datos de detección de integridad a un cuerpo principal del aparato de formación de imágenes.

El método puede incluir realizar una pluralidad de procesos de autenticación posteriores después de transmitir una señal que incluye los segundos datos y los segundos datos de detección de integridad a un cuerpo principal del aparato de formación de imágenes, y datos de detección de integridad que se transmiten/reciben en un proceso de autenticación final de entre la pluralidad de procesos de autenticación posteriores se pueden generar reflejando de manera acumulativa todos los datos de detección de integridad que se transmiten o reciben en procesos de autenticación previos.

El proceso de autenticación final puede incluir recibir terceros datos, los primeros datos de detección de integridad y una señal que incluye terceros datos de detección de integridad generados usando los segundos datos de detección de integridad y los terceros datos de un cuerpo principal del aparato de formación de imágenes, y generar cuartos datos y cuartos datos de detección de integridad usando los primeros a los terceros datos de detección de integridad y transmitir una señal que incluye los cuartos datos y los cuartos datos de detección de integridad a un cuerpo principal del aparato de formación de imágenes, y cada uno de los primeros datos y los segundos datos pueden incluir datos relacionados con una clave de sesión con el fin de generar una clave de sesión, y los terceros datos pueden incluir información de índice en una tabla almacenada previamente en el aparato de formación de imágenes, y los cuartos datos pueden incluir un valor correspondiente a la información de índice.

Un dispositivo de formación de imágenes según una realización ejemplar incluye un cuerpo principal que incluye un controlador principal capaz de controlar operaciones del aparato de formación de imágenes, y una unidad consumible donde se monta un chip de Monitorización de Unidad Sustituible por el Cliente (CRUM), y el controlador principal, cuando ocurre un evento donde se requiere autenticación del chip de CRUM, transmite una primera señal

que incluye primeros datos y primeros datos de detección de integridad al chip de CRUM, y el chip de CRUM genera segundos datos de detección de integridad usando segundos datos y los primeros datos de detección de integridad y transmite los segundos datos y una segunda señal que incluye los segundos datos y los segundos datos de detección de integridad al controlador principal con el fin de realizar un proceso de autenticación para generar una clave de sesión, y el controlador principal transmite una tercera señal que incluye terceros datos de detección de integridad y los terceros datos que se generan usando los primeros datos de detección de integridad y los segundos datos de detección de integridad al chip de CRUM, generan cuartos datos de detección de integridad usando los primeros a los terceros datos de detección de integridad, y transmiten una cuarta señal que incluye los cuartos datos y los cuartos datos de detección de integridad al controlador principal con el fin de realizar un proceso de autenticación para determinar la compatibilidad.

Los primeros datos pueden incluir un primer comando, primeros datos de autenticación y un primer asignador para asignar los primeros datos de detección de integridad, y los segundos datos pueden incluir segundos datos de autenticación y un segundo asignador para asignar los segundos datos de detección de integridad en base a un resultado de operación según el primer comando, los terceros datos pueden incluir un segundo comando, terceros datos de autenticación, y un tercer asignador para asignar los terceros datos de detección de integridad, y los cuartos datos pueden incluir cuartos datos de autenticación y un cuarto asignador para asignar los cuartos datos de detección de integridad en base a un resultado de operación según el segundo comando.

Como se ha mencionado anteriormente, según diversas realizaciones ejemplares de la presente descripción, es posible perseguir la seguridad de toda una comunicación usando de manera acumulativa datos de detección de integridad usados en comunicaciones previas. Por consiguiente, la información de las unidades consumibles y los dispositivos de formación de imágenes se pueden gestionar de forma segura.

Breve descripción de los dibujos

Los anteriores y/u otros aspectos de la presente descripción serán más evidentes describiendo cierta descripción presente con referencia a los dibujos que se acompañan, en los cuales:

la FIG. 1 ilustra un dispositivo de formación de imágenes según una realización ejemplar;

la FIG. 2 es una vista de temporización que ilustra un proceso de comunicación entre un controlador y un chip de CRUM en un dispositivo de formación de imágenes según una realización ejemplar;

la FIG. 3 es una vista de temporización que ilustra un proceso de examen de integridad de una señal usando unos datos de detección de integridad;

la FIG. 4 es una vista de temporización que ilustra un proceso de comunicación entre un controlador y un chip de CRUM en un dispositivo de formación de imágenes según una realización ejemplar;

la FIG. 5 es un diagrama de bloques que ilustra un dispositivo de formación de imágenes ejemplar montado en una unidad consumible;

las FIG. 6 y 7 un dispositivo de formación de imágenes ejemplar según varias realizaciones ejemplares;

la FIG. 8 ilustra una configuración de un chip de CRUM según una realización ejemplar de la presente descripción;

las FIG. 9 y 10 ilustran un método de comunicación según varias realizaciones ejemplares

las FIG. 11 a 18 son vistas que ilustran un método de autenticación de un dispositivo de formación de imágenes según una realización ejemplar;

la FIG. 19 es un diagrama de bloques que ilustra una configuración de un chip de CRUM según una realización ejemplar;

la FIG. 20 es una vista de temporización que ilustra un proceso de autenticación;

las FIG. 21 a 24 ilustran un método ejemplar para generar datos de detección de integridad usados para cada proceso de autenticación;

las FIG. 25 a 27 que ilustran una conexión ejemplar de una unidad consumible a un cuerpo principal de un aparato de formación de imágenes;

la FIG. 28 que ilustra una forma de onda ejemplar de una señal que se transmite y recibe según un método de interfaz I2C; y

la FIG. 29 es una vista ampliada en una parte ejemplar de la señal en la FIG. 28.

Descripción detallada

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

Las realizaciones ejemplares se tratan en detalle a continuación con referencia a los dibujos que se acompañan.

En la siguiente descripción, se usan números de referencia de dibujo iguales para los elementos similares. Las materias definidas en la descripción, tales como la construcción detallada y los elementos, se proporcionan para ayudar a una comprensión exhaustiva de las realizaciones ejemplares.

La FIG. 1 ilustra una configuración de un dispositivo de formación de imágenes según una realización ejemplar. Como se ilustra en la FIG. 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 se puede montar en el cuerpo 100. Un dispositivo de formación de imágenes se puede incorporar como diversos tipos de dispositivos tales como una impresora, un escáner, un dispositivo multifunción, un facsímil o una copiadora, que pueden formar imágenes en papel o en otros diversos medios de registro. Según una realización ejemplar, 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 se puede montar en el cuerpo 100 del dispositivo de formación de imágenes para controlar las funciones del dispositivo de formación de imágenes. Según una realización ejemplar, el controlador 110 es un controlador principal que controla todas las funciones del dispositivo de formación de imágenes.

La unidad consumible 200 se puede montar en el cuerpo 100 del dispositivo de formación de imágenes, y puede ser una de los diversos tipos de unidades que intervienen en el dispositivo de formación de imágenes o bien de manera directa o bien indirecta. Por ejemplo, en el caso de un dispositivo de formación de imágenes láser, unidades de electrificación, unidades de exposición a la luz, unidades de revelado, unidades de transferencia, unidades de asentamiento, diversos tipos de rodillos, correas y tambores OPC pueden ser unidades consumibles. Además, diversos tipos de unidades que se deben sustituir en el uso de un dispositivo de formación de imágenes se pueden definir como 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 de CRUM (chip de Monitorización de Unidad Sustituible por el Cliente) 210 que permite la sustitución en un momento apropiado.

Un chip de CRUM 210 se puede montar en una unidad consumible 200 y registrar diversa información. Un chip de CRUM 210 incluye una memoria. Por lo tanto, se puede hacer referencia a un chip de CRUM 210 en varios términos tales como unidad de memoria, o memoria de CRUM (memoria de Monitorización de Unidad Sustituible por el Cliente), pero por el bien de la comodidad de explicación, se usará el término “chip de CRUM”.

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

Diversos programas almacenados en el chip de CRUM pueden incluir no solamente aplicaciones generales, sino también programas de O/S (sistema operativo) y programas de cifrado. Se puede incluir en la información de características información sobre el fabricante de la unidad consumible 200, información sobre el fabricante del dispositivo de formación de imágenes, nombres de los dispositivos de formación de imágenes que se pueden montar, información sobre la fecha de fabricación, número de serie, nombre del modelo, información de firma electrónica, clave de cifrado e índice de clave de cifrado. La información de uso puede incluir información tal como cuántas hojas de papel se han impreso hasta el momento, cuántas hojas de papel se pueden imprimir a partir de ahora y cuánto tóner queda. También se puede hacer referencia a la información de características como información única en su lugar.

Según una realización ejemplar, la información que se ilustra a continuación en la Tabla 1 se puede almacenar en un chip de CRUM 210.

Información General	
Versión de OS Versión de SPL-C	CLP300_V1.30.12.35 02-22-2007 5.24 06-28-2006
Información General	
Versión de Motor	6.01.00(55)

Número de Serie USB	BH45BAIP914466B
Modelo de Conjunto	DOM
Fecha de Inicio de Servicio	2007-09-29
Opción	
Tamaño de RAM	32 Mbytes
Tamaño de EEPROM	4096 bytes
USB Conectado (Alto)	
Vida de Consumibles	
Recuento de Páginas Total	774/93 Páginas (Color/mono)
Vida del Fusor	1636 Páginas
Vida del Rodillo de Transferencia	864 Páginas
Vida del Rodillo de Bandeja	867 Páginas
Recuento de Imágenes Total	3251 Imágenes
Vida de Rodillo de Reve/Unidad de Imagen	61 Imágenes/19 Páginas
Vida de Correa de Transferencia	3251 Imágenes
Recuento de Imágenes de Tóner	14/9/14/19 Imágenes (C/M/Y/K)
Información de Tóner	
Porcentaje Restante de Tóner	99%/91%/92%/100% (C/M/Y/K)
Cobertura Media de Tóner	5%/53%/31%/3% (C/M/Y/K)
Información de Consumibles	
Tóner Cian	SAMSUNG(DOM)
Tóner Magenta	SAMSUNG(DOM)
Tóner Amarillo	SAMSUNG(DOM)
Tóner Negro	SAMSUNG(DOM)
Unidad de Imagen	SAMSUNG(DOM)
Menú de Color	
Color Personalizado	Ajuste Manual (CMYK : 0,0,0,0)
Menú de Configuración	
Ahorro de Energía	20 minutos
Continuar Automático	Encendido
Ajuste de Altitud	Plano

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

El chip de CRUM puede incluir una CPU (no ilustrada) que puede gestionar la memoria, ejecutar diversos programas almacenados en la memoria y realizar comunicación con el cuerpo de un dispositivo de formación de imágenes o un

controlador de otros dispositivos.

La CPU puede accionar el O/S almacenado en la memoria del chip de CRUM, y realizar la inicialización de la unidad consumible 200 en sí misma, aparte de la inicialización del dispositivo de formación de imágenes. La CPU puede realizar la autenticación 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. Diversos comandos y datos transmitidos desde el cuerpo del dispositivo de formación de imágenes se pueden cifrar según un algoritmo de cifrado arbitrario y transmitir.

En un evento particular, por ejemplo, tal como cuando la alimentación del dispositivo de formación de imágenes que tiene la unidad consumible 200 está activada, o cuando la unidad consumible 200 se separa y luego se une al cuerpo 100 del dispositivo de formación de imágenes de nuevo, la CPU puede realizar la inicialización por sí misma aparte de la inicialización del controlador 100. La inicialización incluye diversos procesos, tales como el accionamiento inicial de varios programas de aplicaciones usados en la unidad consumible 200, calcular 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, comprobar cuándo sustituirse a sí misma, establecer un valor de registro interno de la unidad consumible 200 y establecer una señal de reloj interno-externo.

El establecimiento de un valor de registro se puede definir como una operación de establecimiento de valores de registro funcional dentro de la unidad consumible 200, de modo que la unidad consumible 200 pueda operar según diversos estados funcionales que un usuario predeterminó. El establecimiento de una señal de reloj interno-externo se refiere a una operación de ajuste de una frecuencia de una señal de reloj externo proporcionada desde el controlador 110 del dispositivo de formación de imágenes para estar en línea con la señal de reloj interno que usa la CPU dentro de la unidad consumible 200.

La comprobación de cuándo sustituirse a sí misma puede ser una operación de identificación del volumen restante de un tóner o una tinta usada hasta el momento, anticipando cuándo se agotará la tinta o el tóner y notificando al controlador 110. Tras la determinación en el proceso de inicialización de que el volumen de tóner ya se ha agotado, la unidad consumible 200 se puede incorporar para notificar al controlador 110 que está en un estado no operable. Dado que la unidad consumible 200 en sí misma tiene el O/S, se pueden realizar diversos tipos de inicialización según los tipos y características de la unidad consumible 200.

Después de que se monta la CPU y se proporciona el O/S, se puede identificar el volumen restante de la unidad consumible almacenada en la unidad de memoria 210 o el número de veces de rellenado, antes de que el controlador 110 solicite comunicación con la unidad 200, cuando el dispositivo de formación de imágenes se enciende. Por consiguiente, el tiempo de notificación de la escasez de la unidad consumible se puede hacer más pronto que antes. Por ejemplo, cuando el tóner se está quedando corto, un usuario puede encender la alimentación, y entonces hacer ajustes para la conversión a un modo de ahorro de tóner y luego realice la formación de imágenes. Lo mismo se aplica a cuando solamente se está quedando corto también un tóner particular.

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

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

El controlador 110 cifra datos o un comando para autenticación y los transmite al chip de CRUM 210. En los datos transmitidos, se puede incluir un valor arbitrario R1. En la presente memoria, el R1 puede ser un valor aleatorio que cambia en cada autenticación, o un valor fijo predeterminado. El chip de CRUM que recibió los datos genera una clave de sección usando un valor arbitrario R2 y el R1 recibido, y entonces genera un MAC (Código de Autenticación de Mensaje) usando la clave de sección generada.

Una señal que incluye el MAC generado y el R2 como se ha mencionado anteriormente se transmite al controlador 110. El controlador 110 genera la clave de sección usando los R2 y R1 recibidos, genera el MAC usando la clave de sección generada, y entonces certifica el chip de CRUM 210 comparando el MAC generado y el MAC en la señal recibida. Según diversas realizaciones ejemplares, información de firma electrónica o información clave se puede transmitir en tal proceso de autenticación y usar en la autenticación.

Una vez que la autenticación se hace con éxito, el controlador 110 y el chip de CRUM realizan una comunicación de datos de cifrado para gestión de datos. Es decir, cuando se ha introducido 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 la lectura, escritura o funciones adicionales de datos usando un algoritmo de cifrado, y entonces los transmite al chip de CRUM 210.

El chip de CRUM 210 puede decodificar el comando o los datos recibidos, y realizar operaciones tales como lectura

o escritura de datos correspondientes al comando decodificado. El algoritmo de cifrado usado en el chip de CRUM 210 o el controlador 110 puede ser un algoritmo de cifrado estandarizado. Tal algoritmo de cifrado se puede cambiar cuando la clave de cifrado se ha filtrado o cuando hay una necesidad de reforzar la seguridad. Se pueden usar diversos algoritmos de cifrado tales como el algoritmo de clave asimétrico de RSA, ARIA, TDES, SEED, algoritmo de clave simétrica AES.

Por tanto, entre el chip de CRUM 210 y el controlador 110, la comunicación para autenticación e intercambio de datos se puede realizar numerosas veces. En cada comunicación, las señales se transmiten desde el controlador 110 al chip de CRUM 210 o viceversa. En este caso, una señal transmitida incluye 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 mediante acumulación de datos de detección de errores incluidos en la señal transmitida o recibida de la comunicación previa.

Es decir, entre el controlador 110 y el chip de CRUM 210, se puede realizar una pluralidad de comunicaciones tales como autenticación 1, autenticación 2, autenticación 3, ..., autenticación n, comunicación de datos 1, comunicación de datos 2, ... comunicación de datos m. Según una realización ejemplar, en una señal transmitida en cada comunicación o en algún proceso de la comunicación, se pueden incluir datos de detección de integridad. En tales datos de detección de integridad, los datos de detección de integridad usados en la comunicación previa se reflejan de manera acumulativa.

El lado que recibió la señal detecta integridad de la señal correspondiente usando datos de detección de integridad en la señal. Por consiguiente, cuando se determina que los datos correspondientes son integrales, se realiza una siguiente operación o una comunicación posterior. Si es necesario registrar los datos recibidos, los datos y los datos de detección de integridad incluidos en esa señal se puede almacenar temporalmente. Se pueden generar unos nuevos datos de detección de integridad usando unos datos posteriores a ser transmitidos al lado de los que transmitió la señal y los datos de detección de integridad recibidos de la comunicación previa y almacenar temporalmente. Por consiguiente, una señal a la que se han añadido los nuevos datos de detección de integridad se puede transmitir para los datos posteriores. Entre el controlador 110 y el chip de CRUM 210, tal comunicación que incluye tales datos de detección de integridad se puede realizar una pluralidad de veces. Cuando se realiza la comunicación incluyendo los últimos datos de detección de integridad, se puede realizar una detección final usando los datos de detección de integridad incluidos en la última señal recibida. Si no hay nada erróneo con la detección final, se pueden registrar todos los datos que se han almacenado temporalmente hasta entonces.

La FIG. 2 ilustra un proceso de comunicación ejemplar entre el controlador 110 y el chip de CRUM 210 según una realización ejemplar de la presente descripción. Según la FIG. 2, el controlador 110 transmite una primera señal 10 que incluye datos 1 y datos 1 de detección de integridad. El chip de CRUM 210 que recibió la primera señal 10 genera datos de detección de integridad 2 usando los datos 1 de detección de integridad incluidos en la primera señal 10 y los datos 2. El chip de CRUM 210 transmite una segunda señal que incluye los datos 2 y los datos de integridad 2 al controlador 110. Por tanto, las señales (30, ..., N) que incluyen datos de detección de integridad generados usando los datos de detección de integridad de la comunicación previa se realizan durante una pluralidad de veces.

Un valor de resultado del cálculo lógico sobre datos a ser transmitidos, un valor de resultado generado aplicando una fórmula predeterminada matemáticamente a los datos o un valor de resultado de cifrar los datos, es decir, se puede usar MAC como datos de detección de integridad.

La FIG. 3 ilustra un método de detección usando datos de detección de integridad. Según la FIG. 3, cuando se recibe una señal que incluye datos a y datos de detección de integridad a (S310), el chip de CRUM 210 separa los datos de detección de integridad a (S320).

El chip de CRUM 210 genera datos de detección de integridad a' usando los datos restantes y los datos de detección de integridad que había transmitido durante la comunicación previa (S330). El chip de CRUM 210 entonces 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 es integral (S350). Si no son idénticos, el chip de CRUM 210 determina que los datos están en un estado de error, y detiene la comunicación (S360). Por la comodidad de la explicación, en lo sucesivo, se hará referencia a los datos de detección de integridad a' como los datos sujetos a comparación.

Cuando se determina que los datos correspondientes son integrales, datos de detección de integridad b se generan usando datos b a ser transmitidos y los datos de detección de integridad a (S370). Por consiguiente, una señal que incluye los datos b y los datos de detección de integridad b se transmiten al controlador 110 (S380).

La FIG. 3 ilustra un proceso de detección ejemplar realizado, por ejemplo, en el chip de CRUM 210, pero el mismo proceso también se puede realizar 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), y de este modo se omitirá una explicación e ilustración repetidas.

La configuración de señales transmitidas y recibidas entre el controlador 110 y el chip de CRUM 210 se puede diseñar en diversos tipos. Es decir, los datos incluidos en las señales pueden incluir al menos uno de un comando, información a ser registrada, información de resultado sobre operaciones según el comando, información de resultado sobre detección de integridad con respecto a señales recibidas previamente, e información de indicador para notificar una ubicación de los datos de detección de integridad. La información de resultado sobre detección de integridad se puede excluir de las señales transmitidas inicialmente y recibidas entre el controlador 110 y el chip de CRUM 210. El método para detectar datos de integridad se puede usar para cada operación de comunicación en el proceso de comunicación anterior, pero también se puede aplicar solamente a algunas operaciones de comunicación importantes durante todo el proceso de comunicación, si es necesario.

La FIG. 4 ilustra una realización ejemplar de un proceso de detección de integridad usando señales que tienen diferentes formatos, por ejemplo, diferentes de los de la FIG. 2. Según la FIG. 4, el controlador 110 transmite una señal que incluye datos y datos 1 de detección de integridad (S410). En la presente memoria, los datos incluyen datos de un Comando (CMD) de Lectura 1 y un indicador U1. Los datos del comando (CMD) de lectura 1 incluyen no solamente un comando sino también un destino de lectura o una dirección de memoria. El U1 se refiere a información de indicador que sigue a los datos de Comando (CMD) de Lectura 1. La información de indicador U1 se refiere a un símbolo para notificar una ubicación de análisis sintáctico de los datos de detección de integridad en la señal. La información de indicador se puede expresar como un número fijo de bytes. Por ejemplo, se pueden usar cinco bytes para la información de indicador. Por otra parte, los datos del Comando (CMD) de Lectura 1 son variables según el contenido de los datos y, de este modo, el tamaño de los datos 1 de detección de integridad también es variable.

Cuando se recibe la señal, el chip de CRUM 210 realiza detección de integridad usando los datos 1 de detección de integridad incluidos en la señal (S415). El chip de CRUM 210 es capaz de generar datos de detección de integridad 2 usando los datos a ser transmitidos y los datos 1 de detección de integridad, y transmite la señal que incluye éstos (S420). Como se ilustra en la FIG. 4, en la señal a ser transmitida, se incluyen unos datos de Lectura 1 que son datos leídos de la memoria proporcionada en la unidad consumible 100 según los datos del Comando (CMD) de Lectura 1, unos datos de Resultado 2 que indican el resultado de la operación realizada según los datos del Comando (CMD) de Lectura 1, un indicador U2 y unos datos de detección de integridad 2.

El controlador 110 separa los datos de detección de integridad 2 de la señal recibida y realiza 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 usando los datos de Comando (CMD) de Lectura 3 y los datos de detección de integridad 2, y entonces transmite una señal que incluye los datos de Comando (CMD) de Lectura 3, un indicador U3, y unos datos de detección de integridad 3 en el chip de CRUM 210 (S430).

Como se ilustra en la FIG. 4, por ejemplo, comunicaciones que usan una pluralidad de datos de detección de integridad 4, 5, 6, T1 y T2 se realizan (S440, S450, S460, S470, S485), seguidas de las detecciones de integridad en consecuencia (S435, W445, S455, S465). Cuando se recibe la señal de comunicación final desde el chip de CRUM 210 (S470), el chip de CRUM 210 detecta la integridad de los datos que se han transmitido y recibido en todo el proceso de comunicación y almacenados temporalmente usando datos de detección de integridad T1 incluidos en la señal de comunicación final (S475). Si se determina que los datos son integrales como 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 de CRUM 210, el controlador 110 también realiza toda la detección de integridad usando los datos de detección de integridad T2 incluidos en la señal de comunicación final (S490). Por consiguiente, 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 acumulando datos de detección de integridad usados en las comunicaciones previas.

Según una realización ejemplar, los datos de detección de integridad se pueden procesar como sigue:

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

Datos de detección de integridad 2 = E(Datos de CMD de Lectura 2 | Datos de Resultado | U2 | Datos 1 de detección de integridad)

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 | 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 antes mencionadas, el término “E( )” indica una función de aplicación de una fórmula predeterminada para obtener un valor de resultado. Por tanto, los datos de detección de integridad se pueden generar a partir de añadir los datos de detección de integridad previos y todos los datos a ser transmitidos, aplicando diversos cálculos lógicos, tales como XOR (OR exclusiva), a partir del valor resultante de sustitución de datos en otras fórmulas conocidas entre el controlador 110 y el chip de CRUM 210, y a partir del valor resultante de los cifrados aplicando diversos algoritmos de cifrado mencionados anteriormente.

La FIG. 5 ilustra un dispositivo de formación de imágenes ejemplar donde una pluralidad de unidades consumibles 200-1, 200-2, ..., 200-n se proporcionan dentro del cuerpo 500 según una realización ejemplar de la presente descripción.

Como se ilustra en la FIG. 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 un papel de recibir diversos comandos del usuario, o mostrar y notificar información diversa. La unidad de interfaz de usuario 120 puede incluir un visualizador LCD o LED, al menos un botón o un altavoz. También puede incluir una pantalla táctil dependiendo de las circunstancias.

La unidad de interfaz 130 se refiere a una configuración que se puede conectar con una conexión cableada y/o inalámbricamente con un PC central o diversos dispositivos externos para realizar la comunicación. La unidad de interfaz 130 puede incluir diversos 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 un papel de almacenar diversos programas o datos necesarios para accionar el dispositivo de formación de imágenes.

El controlador 510 realiza un papel de control de todas las operaciones del dispositivo de formación de imágenes. El controlador 510 procesa datos recibidos a través de la unidad de interfaz 130, y convierte los datos procesados en un formato en el que se puede formar una imagen.

El controlador 510 realiza un trabajo de formación de imágenes en los datos convertidos usando una pluralidad de unidades consumibles 200-1, 200-2, ..., 200-n. La unidad consumible se puede proporcionar de varias formas dependiendo del tipo de dispositivo de formación de imágenes.

En el caso de una impresora láser, unidades de electrificación, unidades de exposición a la luz, unidades de revelado, unidades de transferencia, unidades de asentamiento, varios tipos de rodillos, correas y tambores OPC pueden ser unidades consumibles.

En cada unidad consumible 200-1, 200-2, ..., 200-n, se puede incluir un primer chip de CRUM a n chips de CRUM 210-1, 210-2, ..., 210-n.

Cada chip de CRUM puede incluir una memoria y una CPU, etc. Se puede incluir 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 autenticación.

La unidad criptográfica (no ilustrada) soporta el algoritmo de cifrado, de modo que la CPU (no ilustrada) puede realizar autenticación o comunicación cifrada con el controlador 510. La unidad criptográfica puede soportar un algoritmo determinado entre una pluralidad de algoritmos de cifrado, tales como RSA, algoritmo de clave asimétrica ECC y ARIA, TDES, SEED y algoritmo de clave simétrica AES. El controlador 510 también puede soportar un algoritmo correspondiente entre una pluralidad de algoritmos de cifrado. Por consiguiente, 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 comunicación de cifrado.

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

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

La memoria proporcionada dentro del chip de CRUM 210 puede incluir una memoria O/S, una memoria no volátil o una memoria volátil. La memoria O/S (no ilustrada) puede almacenar el O/S para accionar la unidad consumible 200. La memoria no volátil (no ilustrada) puede almacenar diversos datos de no volatilidad. En la memoria no volátil, se

puede almacenar diversa información, tal como información de firma electrónica, diversa información de algoritmo de cifrado, 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.), información única (por ejemplo, información del fabricante, información de la fecha de fabricación, número de serie, nombre del modelo del producto, etc.), y la información de A/S. Los datos recibidos en el proceso de comunicación con el controlador se pueden almacenar en la memoria no volátil.

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

La unidad de interfaz (no ilustrada) toma el papel de conectar la CPU con el controlador y se puede incorporar como una interfaz serie o una interfaz inalámbrica. Dado que la interfaz serie usa un número menor de señales que una interfaz paralela, tiene un efecto de ahorro de costes y, además, es apropiada en entornos de operación donde hay mucho ruido, tal como en una impresora.

Se puede proporcionar un chip de CRUM en cada unidad consumible. Cada chip de CRUM puede realizar comunicación con el controlador y otros chips de CRUM. Durante la comunicación, se transmiten unos nuevos datos de detección de integridad generados acumulando los datos de detección de integridad usados en la comunicación previa.

La FIG. 6 ilustra un dispositivo de formación de imágenes según una realización ejemplar de la presente invención. Como se ilustra en la FIG. 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 datos a ser transmitidos al chip de CRUM montado en la unidad consumible que se puede montar en el dispositivo de formación de imágenes. Los datos incluyen al menos uno de un comando e información a ser procesada por ese comando. Es decir, en el caso de un comando de lectura, una dirección de una memoria a ser leída o información sobre el tema a ser leído se pueden transmitir juntos. En el caso de un comando de escritura, la información a ser registrada puede ser transmitida conjuntamente. La unidad de procesamiento de datos 111 puede emitir datos como están o puede cifrar los datos y luego emitirlos. Diversos comandos, tales como un comando para autenticación e información relacionada con esos comandos se pueden generar en la unidad de procesamiento de datos 111. Estos comandos e información se pueden generar 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 separa y luego se agrega de nuevo, o cuando se introduce un comando de inicialización en el trabajo de formación de imágenes, el controlador 110 puede transmitir el comando de autenticación o el comando de lectura para autenticación en la unidad consumible 200. Por consiguiente, el controlador 610 puede identificar diversa información que se gestiona en la unidad consumible 200 en sí misma, o puede almacenarla en la unidad de memoria 140 del cuerpo del dispositivo de formación de imágenes 100.

Durante o después de la terminación de la realización del trabajo de formación de imágenes, la unidad de procesamiento de datos 111 puede generar un comando de escritura e información correspondiente para registrar información con respecto al elemento consumido, es decir, información sobre la tinta o el tóner, el número de páginas impresas, el número de puntos impresos, e información histórica acerca del usuario que realizó la impresión, para la unidad consumible 200.

La unidad de generación 112 genera datos de detección de integridad usando datos emitidos desde la unidad de procesamiento de datos 111. La unidad de generación 112 puede simplemente sumar los datos emitidos desde la unidad de procesamiento de datos 111, realizar un cálculo lógico tal como XOR, sustituirlo por una fórmula matemática predeterminada, o cifrar los datos usando el algoritmo de cifrado, y emitir el valor del resultado como datos de detección de integridad. Si hay datos de detección de integridad usados en la comunicación previa, la unidad de generación 112 acumula y refleja incluso esos datos de detección de integridad previos juntos y genera los datos de detección de integridad.

Los datos de detección de integridad generados en la unidad de generación 112 se añaden a los datos generados en la unidad de procesamiento de datos 111 y se transmiten a la unidad de interfaz 630. En la FIG. 6, se ilustra como si la salida de la unidad de procesamiento de datos 111 solamente se proporcionase a la unidad de generación 112, pero la salida de la unidad de procesamiento de datos 111 se puede proporcionar directamente a la unidad de interfaz 630 o proporcionar a un multiplexor (no ilustrado). En el caso donde se proporciona un multiplexor, la salida de la unidad de generación 112 también se proporciona en cuanto al multiplexor, y se puede transmitir a la unidad de interfaz 630 en una forma de señal donde datos y 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 de CRUM 210.

La unidad de interfaz 630 puede recibir una señal de respuesta del chip de CRUM 210. Por la comodidad de la explicación, se hará referencia a la señal transmitida desde la unidad de interfaz como primera señal, y se hará referencia a la señal transmitida desde el chip de CRUM como segunda señal.

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

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 integridad de los datos incluidos en la segunda señal. Más específicamente, la unidad de detección 113 aplica un método conocido entre el chip de 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 previamente, y genera datos de detección de integridad.

La unidad de detección 113 compara los datos de detección de integridad generados según 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 según 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.

Según una realización ejemplar, tras la determinación de 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.

Según una realización ejemplar, 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 la comunicación final está completa, registrar los datos almacenados temporalmente en la unidad de memoria 140.

La FIG. 7 ilustra un dispositivo de formación de imágenes según una realización ejemplar. Como se ilustra en la FIG. 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.

Por consiguiente, en la unidad de almacenamiento temporal 741, los datos determinados que son integrales y los datos de detección de integridad se pueden almacenar temporalmente. Los datos de detección de integridad almacenados temporalmente se pueden usar 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 transmita al chip de 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, datos sujetos a comparación, usando los datos restantes y los datos de detección de integridad almacenados en la unidad de almacenamiento temporal 741. A partir de entonces, 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 en base a los datos posteriores y los segundos datos de detección de integridad, si existen unos datos posteriores a ser transmitidos al chip de CRUM 210 en el estado que la segunda señal es integral. Por consiguiente, la unidad de interfaz 730 transmite los terceros datos de detección de integridad y la tercera señal que incluye los datos posteriores al chip de CRUM 210. Es decir, como se ilustra en las Fig. 2 a 4, el controlador y el chip de CRUM realizan la comunicación numerosas veces.

La unidad de detección 713 puede realizar una detección final sobre la integridad de todas las señales recibidas durante la comunicación, usando los datos de detección de integridad finales incluidos en la señal recibida en el proceso de comunicación. Es decir, como se ha mencionado anteriormente, los datos de detección de integridad transmitidos y recibidos durante la comunicación se generan acumulando y examinando los datos de detección de integridad previos, y de este modo los datos de detección de integridad finales incluyen todos los datos desde los primerísimos datos de detección de integridad hasta los justo antes de los actuales. Por lo tanto, si se determina que los datos son integrales, usando 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 cuando se realiza una comunicación que necesita registro, en base al criterio de que todos los contenidos de la comunicación son fiables.

Durante la primera comunicación, el controlador 710 y el chip de 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 entonces transmitir la señal. Por consiguiente, cuando se determina a partir de la señal recibida de la contraparte, el controlador 710 y el chip de CRUM 210 realizan la detección final mencionada anteriormente, y almacenan los datos en la unidad de almacenamiento 742.

Tal detección final se puede realizar cuando se completa un trabajo de formación de imágenes, o en cada unidad de período de tiempo predeterminado según realizaciones ejemplares. También se puede realizar cuando se introduce un comando de usuario para almacenamiento de datos, cuando se introduce un comando de apagado con respecto al dispositivo de formación de imágenes, o en el proceso de autenticación de un dispositivo de formación de imágenes y una unidad consumible.

Las Fig. 6 y 7 ilustran una unidad de procesamiento de datos ejemplar, una unidad de generación, una unidad de detección y la unidad de control que están incluidas en el controlador, pero no están necesariamente limitadas a tal realización. 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 se pueden proporcionar aparte del controlador. En este caso, a diferencia de lo ilustrado en las Fig. 1 a 4, el controlador puede realizar solamente la función original, y la comunicación con el chip de CRUM 210 se puede realizar por la unidad de procesamiento de datos, la unidad de generación, la unidad de detección y la unidad de control.

La FIG. 8 ilustra una configuración de un chip de CRUM 810 según una realización ejemplar de la presente descripción. Como se ilustra en la FIG. 8, el chip de CRUM 810 incluye una unidad de interfaz 811, unidad de detección 812, unidad de generación 2813, unidad de procesamiento de datos 814, unidad de control 815, unidad de almacenamiento temporal 816 y 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 del 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 de este modo se omitirá una 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 unos segundos datos que han de ser transmitidos al cuerpo del dispositivo de formación de imágenes.

La unidad de generación 813 genera los segundos datos de detección de integridad usando 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 de CRUM. Es decir, como se ha mencionado anteriormente, cuando el chip de CRUM en sí mismo tiene el O/S, la unidad de control 815 puede accionar el chip de CRUM usando el O/S. Después de que el programa de inicialización se almacena, la inicialización se puede realizar por separado desde el 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 según ese comando, y transmite los datos al dispositivo de formación de imágenes a través de la unidad de interfaz 811. En este proceso, se pueden añadir datos de detección de integridad.

Mientras tanto, la unidad de detección 812 realiza la detección de integridad sobre la tercera señal cuando la tercera señal que incluye los terceros datos de detección de integridad generados acumulando y examinando los segundos datos de detección de integridad.

Cuando se completa la comunicación, la unidad de detección 812 detecta todas las señales recibidas en el proceso de realización del trabajo de formación de imágenes, usando los datos de detección de integridad finales incluidos en la señal recibida en el proceso de la comunicación. 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, si es necesario.

Es decir, cuando se completa la comunicación, la unidad de control 815 controla la unidad de detección 812 para realizar la detección final usando los datos de detección de integridad finales. Por consiguiente, 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, si es necesario.

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

La FIG. 9 ilustra un método de comunicación según una realización ejemplar de la presente descripción. El método de comunicación ilustrado en la FIG. 9 se puede realizar en un controlador proporcionado en un cuerpo de un dispositivo de formación de imágenes, o en un chip de CRUM proporcionado en una unidad consumible.

Como se ilustra en la FIG. 9, cuando se generan datos a ser transmitidos (S910), los datos de detección de integridad se generan usando esos datos generados (S920).

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

Por consiguiente, una señal de respuesta correspondiente a la señal transmitida se recibe de la contraparte (S940). En la señal de respuesta, se incluyen unos nuevos datos de detección de integridad generados acumulando y examinando los datos de detección de integridad transmitidos desde el S930.

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

De este modo, según una realización ejemplar, es posible determinar la integridad de cada comunicación usando los datos de detección de integridad previos de manera acumulativa.

La FIG. 10 ilustra un método de comunicación según una realización ejemplar. Como se ilustra en la FIG. 10, cuando se generan datos a ser transmitidos (S1010), los datos de detección de integridad se generan en base a esos datos (S1020). A partir de entonces, la señal que incluye los datos y los datos de detección de integridad se transmite (S1030), y se recibe una señal de respuesta con respecto a esa señal (S1040). Por consiguiente, los datos de detección de integridad se separan de la señal de respuesta (S1050).

Si los datos son integrales se puede determinar usando los datos restantes de los cuales 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 se puede realizar otro intento.

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

En las realizaciones ejemplares mencionadas anteriormente, excepto a partir de 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 acumulando y examinando los datos de detección de integridad durante la comunicación previa. Como resultado, los datos de detección de integridad durante la comunicación final incluyen todos los datos de detección de integridad usados en algunos, por ejemplo, procesos de comunicación importantes. Por lo tanto, se puede registrar un dato exacto.

De este modo, es posible proteger de manera segura la información en el controlador y el chip de CRUM de efectos externos, tales como ruido, punto de contacto escaso, cambios anormales en consumibles, modificación intencional y piratería informática.

Según una realización ejemplar, se puede basar en el dispositivo de formación de imágenes y el chip de CRUM montado en la unidad consumible usada en el dispositivo de formación de imágenes, pero el método de comunicación mencionado anteriormente se puede aplicar a otros tipos de dispositivos también. Por ejemplo, una realización ejemplar incluida se puede aplicar al caso de comunicación entre un dispositivo fabricado para comunicación con el chip de CRUM y no con 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 datos de detección de integridad se pueden usar, por ejemplo, solamente para algunos procesos de la autenticación. Es decir, un controlador principal proporcionado en el cuerpo principal de un dispositivo de formación de imágenes puede realizar autenticación con el chip de CRUM de una unidad consumible en diversos casos, tales como cuando se sustituye una unidad consumible donde se monta un chip de CRUM, cuando se inicia un dispositivo

de formación de imágenes, cuando se requiere una actualización de datos, cuando llega un período de tiempo predeterminado, y similares.

El chip de CRUM se puede diseñar para realizar la autenticación con un aparato de formación de imágenes, y realizar operaciones tales como leer o escribir datos desde el chip de CRUM solamente cuando se confirma que el chip de CRUM es adecuado para el aparato de formación de imágenes correspondiente. Puede haber varios tipos de autenticación que se pueden seleccionar dependiendo de las circunstancias. Por ejemplo, en el caso donde la información del chip de CRUM previa no se pueda usar debido al inicio o sustitución de una unidad consumible, se puede usar un método de autenticación que tenga un alto nivel de cifrado, pero que tarde un tiempo relativamente más largo de ejecución para ser realizado. En el caso donde se requiera autenticación para actualizar algunos de los datos en el proceso de impresión, se puede realizar una autenticación más rápida y sencilla. Aunque la autentificación realizada en el proceso de impresión es relativamente simple, es un método sólido de autenticación en términos de cifrado, dado que se basa en datos generados durante la autenticación previa con un alto nivel de cifrado.

La FIG. 11 ilustra un proceso de autenticación ejemplar entre un cuerpo principal de un dispositivo de formación de imágenes y un chip de CRUM montado en una unidad consumible. Con referencia a la FIG. 11, el cuerpo principal 100 de un dispositivo de formación de imágenes y el chip de CRUM 210 realizan la autenticación final después de pasar por múltiples procesos de autenticación (Aut-1~4). El número y el orden del proceso de autenticación (Aut-1~4) pueden variar en diversas realizaciones ejemplares. El cuerpo principal 100 de un dispositivo de formación de imágenes y el chip de CRUM 210 pueden realizar el proceso de autenticación para generar una clave de sesión y el proceso de autenticación para verificar la compatibilidad de un chip de CRUM, y uno o más procesos de autenticación se pueden realizar antes, después o entre los procesos de autentificación.

Como se ilustra en la FIG. 11, la autenticación se puede dividir en una autenticación básica y una autenticación adicional. La autenticación básica incluye el primer proceso de autenticación (Aut-1) para realizar autenticación interna, y la autenticación adicional incluye múltiples operaciones tales como Aut-2, Aut-3 y Aut-4.

El primer proceso de autenticación (Aut-1) realiza autenticación entre el dispositivo de formación de imágenes 100 y el chip de CRUM 210, y realiza una operación para crear una clave de sesión común. El dispositivo de formación de imágenes 100 y el chip de CRUM 210 se comunican uno con otro cifrando todos, o parte, de los datos que se intercambian entre ellos durante la comunicación usando un algoritmo de cifrado, tal como una clave simétrica o una clave asimétrica, de modo que los datos no se puedan ver desde el exterior.

El dispositivo de formación de imágenes 100 y el chip de CRUM 210 crean una clave de sesión común usando datos intercambiados durante el primer proceso de autenticación (Aut-1) y usan la clave de sesión para cifrar datos para la comunicación posterior.

El segundo proceso de autenticación (Aut-2) se refiere a una operación para sincronizar la Tabla de Combinación (tabla C) del dispositivo de formación de imágenes 100 con la del chip de CRUM 210. La tabla C es información que se usa para el dispositivo de formación de imágenes 100 y el chip de CRUM 210 para autenticarse entre sí. Es decir, la tabla C se refiere a una tabla donde se registra un valor a ser operado cuando se envía un código de consulta, y también se puede hacer referencia a ella como la primera tabla.

Cuando se realiza el arranque en el dispositivo de formación de imágenes 100, o cuando se determina que la tabla C del dispositivo de formación de imágenes 100 no es coherente con la tabla C del chip de CRUM 210, se puede realizar el segundo proceso de autenticación para sincronizar las tablas C del dispositivo de formación de imágenes 100 y del chip de CRUM 210. Si la tabla C del dispositivo de formación de imágenes 100 es coherente con la tabla C del chip de CRUM 210 se puede determinar en el dispositivo de formación de imágenes 100.

La FIG. 12 es una vista de temporización para ilustrar un segundo proceso de autenticación ejemplar. Como se ilustra en la FIG. 12, el dispositivo de formación de imágenes 100 puede generar datos de PRT y un REQEST_CMD (comando de solicitud) (S 1210), y transmitir el mismo al chip de CRUM 210. El REQUEST_CMD se puede proporcionar en varios formatos. Por ejemplo, el REQUEST_CMD puede ser CMD || E(datos de PRT) || MAC || CRC (Comprobación de Redundancia Cíclica) o EDC (bits de Detección y Corrección de Errores). “E()” representa un Algoritmo de Criptografía, y “||” representa un símbolo de operación predeterminado, es decir, un símbolo de suma.

Cuando se recibe el REQUEST_CMD, el chip de CRUM 210 genera datos de CRUM (S1230), y genera una tabla C que usa los datos de CRUM generados y los datos de PRT recibidos (S1240). El chip de CRUM 210 puede generar una tabla C aplicando una función de configuración predeterminada con respecto a los datos de CRUM y los datos de PRT.

El chip de CRUM 210 puede generar una RESPUESTA que incluye los datos de CRUM generados (S1250), y transmitir la RESPUESTA generada al dispositivo de formación de imágenes 100 (S1260). La RESPUESTA se puede generar usando los métodos de E(datos de CRUM) ||MAC||CMD de Resultado||CRC o EDC.

El dispositivo de formación de imágenes 100 genera una tabla C usando los datos de CRUM y los datos de PRT recibidos (S1270). El dispositivo de formación de imágenes 100 también puede generar una tabla C aplicando una

función de configuración predeterminada. En consecuencia, el dispositivo de formación de imágenes 100 y el chip de CRUM 210 pueden tener la misma tabla C, respectivamente.

Cuando se completa el segundo proceso de autenticación (Aut-2), se puede realizar el tercer proceso de autenticación (Aut-3). El tercer proceso de autenticación (Aut-3) puede ser un proceso donde el dispositivo de formación de imágenes 100 y el chip de CRUM 210 sincronizan la tabla de Consultas (tabla Q). La tabla Q se refiere a una tabla donde se registran datos para autenticación, tales como un código de consulta, y también se puede hacer referencia a ella como la segunda tabla.

La FIG. 13 ilustra un tercer proceso de autenticación ejemplar. Como se ilustra en la FIG. 13, cuando se completa el segundo proceso de autenticación, el cuerpo principal del dispositivo de formación de imágenes 100 determina si la versión de la tabla Q en el cuerpo principal (es decir, versión de PRT) es mayor que la versión de la tabla Q en el chip de CRUM 210 (S1310). Si se determina que la versión de PRT es mayor que la versión de CRUM, el cuerpo principal del dispositivo de formación de imágenes 100 proporciona información con respecto a la tabla Q al chip de CRUM 210. Por consiguiente, el chip de CRUM 210 actualiza la versión de CRUM para que coincida con la versión de la tabla Q del cuerpo principal del dispositivo de formación de imágenes (S1320).

Por otra parte, si la versión de PRT es menor que la versión de CRUM (S1330), el chip de CRUM 210 proporciona información con respecto a la tabla Q al cuerpo principal del dispositivo de formación de imágenes 100. Por consiguiente, el dispositivo de formación de imágenes 100 actualiza la versión de PRT para que coincida con la versión de la tabla Q del chip de CRUM 210 (S1340).

Por tanto, cuando las tablas Q de ambos lados han llegado a ser coherentes a través de actualización, o si son coherentes sin actualización, se realiza la operación de comprobación de un código de consulta, es decir, los valores registrados en la tabla Q (S1350). Tal operación de comprobación de un código de consulta puede ser el cuarto proceso de autenticación.

La FIG. 14 ilustra un proceso ejemplar de sincronización de una tabla Q con la tabla Q del cuerpo principal de un aparato de formación de imágenes. Como se ilustra en la FIG. 14, el dispositivo de formación de imágenes 100 genera REQUEST_CMD1 para solicitar datos de CRUM (S1410), y transmite el REQUEST_CMD1 al chip de CRUM 210 (S1415). El chip de CRUM 210 genera RESPUESTA 1 en respuesta a la REQUEST_CMD1 (S1420), y transmite la RESPUESTA 1 al dispositivo de formación de imágenes 100 (S1425). La RESPUESTA 1 se puede generar usando los métodos de E1(E2(Índice de DATOS Q de PRT)||Datos de CRUM) ||MAC||CMD1 de Resultado||CRC o EDC. En la presente memoria, E1 se refiere a un algoritmo de cifrado, y E2(Índice de DATOS Q de PRT) se puede definir como que obtiene datos Q aplicando un índice de tabla Q a una tabla Q y cifrando los datos Q usando un primer algoritmo de cifrado arbitrario.

Cuando se recibe la RESPUESTA 1, el dispositivo de formación de imágenes 100 compara los datos Q recibidos (S1430). Es decir, el dispositivo de formación de imágenes 100 detecta los datos Q correspondientes al índice que se ha transmitido al chip de CRUM 210 desde la tabla Q almacenada y compara los datos Q con los datos Q transmitidos desde el chip de CRUM 210 para determinar si son coherentes unos con otros. Si se determina que no son coherentes, el dispositivo de formación de imágenes 100 genera REQUEST_CMD2 (S1435) y transmite el REQUEST_CMD2 al chip de CRUM 210 (S1440). El REQUEST_CMD2 se puede generar usando los métodos de E1(E5(TBL Q DE PRT)||MAC||CRC o EDC. En la presente memoria, E5 se refiere al segundo algoritmo de cifrado que es diferente de E1 y E2.

Cuando se recibe el REQUEST_CMD2, el chip de CRUM 210 compara la versión de la tabla Q del dispositivo de formación de imágenes con la versión de la tabla Q del chip de CRUM 210, y si se determina que no son coherentes (S1445) o se aplica una regla que es diferente de la de la tabla Q del chip de CRUM 210 (S1450), se genera una respuesta de error. Por consiguiente, el chip de CRUM 210 actualiza su tabla Q para que coincida con la tabla Q de PRT (S1455), genera RESPUESTA 2 (S1460), y transmite la RESPUESTA 2 al dispositivo de formación de imágenes 100 (S1465). La RESPUESTA 2 se puede generar usando los métodos de CMD2 de Resultado||CRC o EDC.

La FIG. 15 es una vista de temporización que ilustra un proceso ejemplar de sincronización de una tabla Q con la tabla Q del chip de CRUM 210. Como se ilustra en la FIG. 15, el dispositivo de formación de imágenes 100 genera REQUEST_CMD (S1510), y transmite el REQUEST_CMD al chip de CRUM 210 (S1520). El chip de CRUM 210 genera una RESPUESTA según un comando recibido (S1530), y transmite la RESPUESTA al dispositivo de formación de imágenes 100 (S1540). La RESPUESTA se puede generar usando los métodos de E1(E2(DATOS Q DE CRUM)||E5(TBL Q DE CRUM))||MAC||CMD de Resultado||CRC o EDC. Cuando se recibe la RESPUESTA, el dispositivo de formación de imágenes 100 comprueba DATOS Q DE CRUM de la RESPUESTA recibida, y compara los DATOS Q DE CRUM con los DATOS Q DE CRUM DE RESPUESTA (S1550). Si se determina que no son coherentes unos con otros, se determina que es un estado de error. El dispositivo de formación de imágenes 100 comprueba si la tabla Q de CRUM recibida cumple con la regla para la tabla Q, y si se determina que la tabla Q no es válida, se determina que es un estado de error (S 1560).

Si se determina que la tabla Q no es coherente, el dispositivo de formación de imágenes 100 actualiza la tabla Q

según los datos recibidos (S1570). En consecuencia, la tabla Q de ambos lados se sincroniza una con otra.

El segundo y el tercer procesos de autenticación (Aut-2, Aut-3) son procesos para sincronizar información del dispositivo de formación de imágenes 100 y la unidad consumible 200 para analizar los datos que se intercambian durante el cuarto proceso de autenticación (Aut-4). Si los datos existentes ya son los mismos, el tercer proceso de autenticación (Aut-3) no se puede realizar.

El cuarto proceso de autenticación (Aut-4) es un proceso de autenticación para confirmar la compatibilidad. En el cuarto proceso de autenticación, el dispositivo de formación de imágenes 100 y la unidad consumible 200 usan la clave de sesión generada por el primer proceso de autenticación (Aut-1) y la información compartida durante el segundo y el tercer procesos de autenticación (Aut-2, 3) para confirmar si la unidad consumible 200 o el chip de CRUM 210 montado en la unidad consumible 200 es apropiado para el dispositivo de formación de imágenes 100.

La FIG. 16 es una vista de temporización para ilustrar un método ejemplar para realizar el cuarto proceso de autenticación (Aut-4). Como se ilustra en la FIG. 16, el dispositivo de formación de imágenes 100 selecciona el índice Q, el índice C, etc., genera REQUEST_CMD incluyendo los índices seleccionados (S1610), y transmite el REQUEST_CMD al chip de CRUM 210 (S1620). El chip de CRUM 210 genera datos de CRUM usando el REQUEST_CMD recibido, genera RESPUESTA que incluye lo mismo, y transmite la RESPUESTA al dispositivo de formación de imágenes 100 (S1640).

Cuando se recibe la RESPUESTA, el dispositivo de formación de imágenes 100 genera datos Q de RPT (S1650) y compara los datos Q de PRT con los datos de CRUM incluidos en la RESPUESTA (S1660). Si se determina que son coherentes unos con otros, se determina que el chip de CRUM 210 t es apropiado y se completa la autenticación.

El dispositivo de formación de imágenes 100 y la unidad consumible 200 pueden transmitir/recibir una señal que incluye datos de detección de integridad durante el primer proceso de autenticación (Aut-1) para crear una clave de sesión y durante el cuarto proceso de autenticación (Aut-4) para confirmar compatibilidad. Los datos de detección de integridad se refieren a datos que se generan reflejando de manera acumulativa datos de detección de integridad incluidos en las señales recibidas previamente. Si no se ha recibido previamente ninguna señal que incluya datos de detección de integridad, es decir, si necesitan ser generados datos de detección de integridad por primera vez, se pueden generar datos de detección de integridad usando solamente datos a ser transmitidos.

Los datos de comunicación intercambiados durante el segundo y el tercer procesos de autenticación (Aut-2, Aut-3) afectan al siguiente proceso de comunicación que es el cuarto proceso de autenticación (Aut-4). Por consiguiente, incluso si los datos de detección de integridad no se usan en el proceso de autenticación intermedio, el cuarto proceso de autenticación (Aut-4) puede fallar cuando hay un problema en el segundo y el tercer procesos de autenticación (Aut-2, Aut-3), dando como resultado por ello un fallo en la autenticación finalmente. Por lo tanto, no es necesario incluir datos de detección de integridad en todo el proceso de autenticación, y los datos de detección de integridad se pueden incluir solamente en Aut-1 y Aut-4, que son procesos de autentificación importantes. No obstante, esto es solamente un ejemplo, y los datos de detección de integridad se pueden transmitir/recibir en cada proceso de autenticación o en al menos uno del segundo y el tercer procesos de autenticación.

Según una realización ejemplar, se puede realizar autenticación entre el cuerpo principal 100 y el chip de CRUM 210, pero tal operación de autenticación se puede realizar entre el controlador principal 110 montado en el cuerpo principal 100 y el chip de CRUM 210. Un proceso de autenticación ejemplar entre el controlador principal 110 y el chip de CRUM 210 se explica con referencia a las FIG. 17 y 18.

La FIG. 17 ilustra un primer proceso de autenticación (Aut-1) ejemplar para generar una clave de sesión en el proceso de una pluralidad de procesos de autenticación. Por comodidad de explicación, el proceso de autenticación para generar una clave de sesión se puede definir como la primera autenticación en la realización ejemplar, pero se pueden realizar otros procesos de autenticación antes del proceso de autenticación para generar una clave de sesión.

Como se ilustra en la FIG. 17, el primer proceso de autenticación (Aut-1) se puede dividir en com-1 y com-2. El proceso de com-1 es un proceso para transmitir datos, de modo que el controlador principal 100 puede realizar una operación de autenticación usando el chip de CRUM 210. Las señales transmitidas durante el proceso de com-1 incluyen CMD1, DATOS1, CRC1, símbolo, VC1, etc. CMD1 representa un comando y puede incluir opciones relacionadas con la autenticación o información con respecto al tamaño de los datos a ser transmitidos. DATOS1 incluye datos aleatorios necesarios para autenticación, valores de datos relacionados con el cifrado para autenticación, información específica almacenada en un aparato de formación de imágenes, etc. En el caso del primer proceso de autenticación, no solamente los datos aleatorios (R1) mencionados anteriormente, sino también los datos relacionados con una clave de sesión, tales como información con respecto al tamaño de una clave, varias claves usadas en un algoritmo de clave asimétrica, etc. y otra información almacenada en el cuerpo principal del dispositivo de formación de imágenes 100 se pueden transmitir a DATOS1. Según una realización ejemplar, algo de la información mencionada anteriormente se puede omitir o sustituirse con otra información.

Los datos aleatorios pueden ser un valor que el controlador principal 110 genera aleatoriamente para autenticación. Por consiguiente, los datos aleatorios pueden variar para cada autenticación, pero algunas veces se puede transmitir

un valor que se establece temporalmente en lugar de los datos aleatorios. CRC1 representa un código de detección de errores. CRC1 se transmite para comprobar errores en CMD1 y DATOS1. Se pueden usar otros métodos de detección de errores, tales como Suma de Comprobación o MAC, además de o en sustitución de CRC1.

El símbolo en com-1 designa datos de detección de integridad. La FIG. 17 ilustra un caso donde SECU1 se usa como un símbolo que puede identificar datos de detección de integridad de otros datos y mostrar el tipo de operación de datos de integridad. El SECU1 usado en la FIG. 17 es un símbolo que representa la primera comunicación que usa la función de datos de detección de integridad. VC1 son datos de detección de integridad que se generan por primera vez. VC1 genera contenidos que consisten en CMD1, DATOS1, CRC1 y cadena SECU1 según una ecuación específica. Dado que VC1 son datos de detección de integridad generados por primera vez, no se generan reflejando de manera acumulativa los datos de detección de integridad recibidos previamente, sino usando solamente los datos restantes. Se describe el método de generación de VC1.

Una vez que el chip de CRUM 210 recibe com-1, el chip de CRUM 210 transmite com-2 que incluye DATOS2, SW2, CRC2, SECU2, VC2, etc. Si el primer proceso de autenticación se refiere a un proceso de autenticación para generar una clave de sesión, los datos de com-2 pueden incluir los primeros datos aleatorios (R1), los segundos datos aleatorios (R2), un número de serie de chip (CSN), información con respecto a una clave usada para un algoritmo de clave asimétrica, parte de información interna del chip de CRUM, etc. Los primeros datos aleatorios (R1) son un valor recibido en com-1, y los segundos datos aleatorios (R2) son un valor que se genera a partir del chip de CRUM 210. La información incluida en com-2 se puede omitir o sustituir por otra información.

Además, SW2 representa datos de resultado que muestran el resultado de un trabajo realizado en el chip de CRUM 210 según el comando de com-1. Como CRC2 y SECU2 operan de la misma forma que CRC1 y SECU1 en com-1, se omitirán las descripciones con respecto a CRC2 y SECU2. VC2 son datos de detección de integridad que se generan reflejando de manera acumulativa VC1 que son datos de detección de integridad de com-1. El chip de CRUM 210 puede generar VC2 combinando DATOS2, SW2, CRC2 y SECU2 que se transmitirán a com-2 con VC1 según un método predeterminado, que se explicará más tarde con mayor detalle.

Si el primer proceso de autenticación se realiza como se ilustra en la FIG. 17, los primeros datos aleatorios (R1) generados por el controlador principal 110 y los segundos datos aleatorios (R2) generados en el chip de CRUM 210 se pueden compartir unos con otros. El controlador principal 110 y el chip de CRUM 210 pueden generar una clave de sesión usando R1 y R2, respectivamente.

Como se ilustra en la FIG. 11, se realiza una autenticación final después de pasar por una pluralidad de procesos de autenticación. De entre los procesos, el cuarto proceso de autenticación es para comprobar la compatibilidad del chip de CRUM 210 o la unidad consumible 200 montada en el chip de CRUM 210. Entre la primera autenticación y la cuarta autenticación, se puede añadir al menos un proceso de autenticación más con el fin de prepararse para la cuarta autentificación.

La FIG. 18 ilustra un proceso de autenticación ejemplar para confirmar la compatibilidad. En la FIG. 11, el proceso de autentificación para confirmar la compatibilidad que es la cuarta autenticación se realiza por última vez de entre una pluralidad de procesos de autenticación, pero el orden no se limita a los mismos.

Como se ilustra en la FIG. 18, el cuarto proceso de autenticación (Aut-4) comprende com-3 y com-4. Com-3 se refiere al proceso donde el controlador principal 110 transmite una señal al chip de CRUM 210, y com-4 se refiere al proceso donde el chip de CRUM 210 transmite una señal al controlador principal 110. En com-3, se transmiten CMD3, DATOS3, SECT1, y VC3. CMD3 es un comando que representa com-3, y DATOS3 representa los datos necesarios para realizar la operación Aut-4. El controlador principal 110 puede almacenar una tabla para confirmar por adelantado la compatibilidad del chip de CRUM 210 o la unidad consumible 200. Por ejemplo, si se almacena una pluralidad de tablas, DATOS3 puede incluir cualquiera de la primera información de índice (índice 1) de la tabla 1 y cualquiera de la segunda información de índice (índice 20 de la tabla 2. El controlador principal 110 puede cifrar DATOS3 usando una clave de sesión generada a través del primer proceso de autenticación. SECT1 es una cadena de símbolos para informar de la última operación de comunicación usando datos de detección de integridad, y VC3 son datos de detección de integridad. El controlador principal 110 puede generar VC3 usando una CMD3, DATOS3, CRC3, cadena SECT1 y VC1 y VC2, que son datos de detección de integridad que se han generado hasta el momento. El chip de CRUM 210 que recibe com-3 transmite com-4 al controlador principal 110. Com-4 puede incluir DATOS4, SW4, CRC4, SECT2, VC4, etc. DATOS4 puede incluir el tercer valor que se genera usando el primer valor (valor 1) y el segundo valor (valor 2) correspondientes a la primera y la segunda información de índice recibida de com-3, respectivamente. El controlador principal 110 puede confirmar si el chip de CRUM 210 o la unidad consumible 200 son apropiados para el dispositivo de formación de imágenes 100 comparando el primer, segundo y tercer valores confirmados a través de com-4 con la tabla. Se describen las funciones de SW4, CRC4 y SECT2. VC4 son datos de detección de integridad que se generan reflejando de manera acumulativa VC1, VC2 y VC3.

Los datos de detección de integridad se pueden transmitir/recibir durante al menos alguna parte de una pluralidad de procesos de autenticación. En este caso, si hay datos de detección de integridad usados previamente, los datos de detección de integridad correspondientes se pueden reflejar de manera acumulativa. Es decir, los datos de detección de integridad se pueden resumir como en la Ecuación 1:

[Ecuación 1]

VCn de SECU(n) = CMD(+)DATOS(+)SW(+)CRC(+)Símbolo(+)VC(n-1)

VCn de SECT(n) = CMD(+)DATOS(+)SW(+)CRC(+)Símbolo(+)VC(1)(+)VC(2) (+) … VC(n-2) (+)VC(n-1)

En la Ecuación 1, (+) puede representar una ecuación de operación lógica tal como XOR u otras ecuaciones de algoritmos de cifrado. Según la [Ecuación 1], VCn de SECU(n) que son datos de detección de integridad usados en los procesos de autenticación, excepto para el proceso de autenticación final, se puede generar combinando cada uno de los datos a ser transmitidos y VC(n-1) que son datos de detección de integridad recibidos previamente. Por otra parte, VCn de SECT(n) que son datos de detección de integridad usados para el proceso de autenticación final se puede generar combinando cada uno de los datos a ser transmitidos y todos los datos de detección de integridad transmitidos o recibidos en los procesos de autenticación previos. Por ejemplo, en el caso de datos de detección de integridad de orden n, se pueden reflejar datos de detección de integridad de 1, 2, ..., n-1. Por consiguiente, si hay un error en el proceso de autenticación, el error se puede encontrar en el proceso de autenticación final y la autenticación se puede completar, o se puede determinar que la autenticación ha fallado.

La FIG. 19 ilustra una configuración ejemplar de un chip de CRUM que usa datos de detección de integridad en un proceso de autenticación según una realización ejemplar. Un chip de CRUM 1400 se puede montar en varias unidades consumibles y luego usar. Como se ilustra en la FIG. 19, el chip de CRUM 1400 comprende una unidad de interfaz 1410, una unidad de prueba 1420, una unidad de generación 1430 y un controlador 1440. La unidad de interfaz 1410 es un componente que se puede conectar al cuerpo principal 100 de un aparato de formación de imágenes. La unidad de interfaz 1410 puede adoptar diversos métodos de interfaz. Por ejemplo, se puede usar el Circuito Inter-Integrado (I2C).

Si ocurre un evento que requiere autenticación, la unidad de interfaz 1410 puede recibir varias señales. Por ejemplo, la unidad de interfaz 1410 puede recibir una señal que incluye primeros datos para autenticación y primeros datos de detección de integridad con respecto a los primeros datos del cuerpo principal 100. Los primeros datos representan datos que excluyen los primeros datos de detección de integridad de entre las señales recibidas. Los primeros datos de la FIG. 17 representan CMD1, DATOS1, CRC1 y SECU1. DATOS1 puede incluir diversos datos, tales como primeros datos aleatorios.

La unidad de prueba 1420 puede probar la integridad de una señal separando los primeros datos de detección de integridad, es decir, VC1 de las señales recibidas. Según un primer proceso de autenticación de la FIG. 17, la unidad de prueba 1420 puede calcular VC1 operando CMD1(+)DATOS1(+)CRC1(+)SECU1. La unidad de texto 1420 puede comparar VC1 que se separa de com-1 con VC1 que se calcula directamente, y determinar que com-1 es integral si son coherentes uno con otro.

Si se determina que com-1 es integral, el controlador 1440 puede almacenar algunos datos necesarios incluyendo VC1 temporalmente. El controlador 1440 controla la unidad de generación 1430 para realizar el primer proceso de autenticación.

La unidad de generación 1430 genera segundos datos de detección de integridad usando segundos datos para autenticación con el cuerpo principal de un dispositivo de formación de imágenes y los primeros datos de detección de integridad. La unidad de generación 1430 puede generar segundos datos aleatorios usando un algoritmo de generación de valores aleatorios. Según una realización ejemplar donde se usa la Ecuación 1 identificada anteriormente, los segundos datos de detección de integridad se pueden calcular como un valor de resultado de DATOS2(+)SW2(+)CRC2(+)SECU2(+)VC1,

El controlador 1440 puede realizar la primera operación de autenticación usando datos recibidos del cuerpo principal 100. El controlador 1440 puede generar una clave de sesión usando los primeros datos aleatorios (R1) recibidos del cuerpo principal 100 y los segundos datos aleatorios (R2) generados por la unidad de generación 1430.

El controlador 1440 transmite una señal que incluye los segundos datos de detección de integridad calculados junto con los segundos datos, es decir, DATOS2, SW2, CRC2 y SECU2 al cuerpo principal 100 de un dispositivo de formación de imágenes a través de la unidad de interfaz 1410. El cuerpo principal 100 de un dispositivo de formación de imágenes también puede detectar los primeros y segundos datos aleatorios de la señal recibida y generar una clave de sesión usando los datos detectados.

La autenticación incluye una pluralidad de veces de autenticación. Es decir, el controlador 1440 puede realizar una pluralidad de procesos de autenticación posteriores después de generar una clave de sesión usando los primeros y segundos datos.

La pluralidad de procesos de autenticación posteriores puede incluir un proceso de autenticación para una prueba de compatibilidad como se ha descrito anteriormente con respecto al cuarto proceso de autenticación. Durante este proceso de autenticación, se pueden transmitir y recibir unos nuevos datos de detección de integridad que reflejen de manera acumulativa datos de detección de integridad que ya se han transmitido y recibido.

La unidad de interfaz 1410 puede recibir una señal que incluye terceros datos y terceros datos de detección de integridad del cuerpo principal 100 de un aparato de formación de imágenes. Los terceros datos de detección de integridad representan datos que se generan usando los datos de detección de integridad que han sido usados por el cuerpo principal 100 de un dispositivo de formación de imágenes y el controlador principal 110 hasta el momento y los terceros datos. Si el cuarto proceso de autenticación es el proceso de autenticación final, todos los primeros y segundos datos de detección de integridad se pueden reflejar con el fin de generar los terceros datos de detección de integridad.

Si se reciben terceros datos y los terceros datos de integridad, el controlador 1440 controla la unidad de prueba 1420 para probar los datos. Un método de prueba es como se ha descrito anteriormente.

Si se determina que no hay ningún problema con los terceros datos en base al resultado de la prueba, el controlador 1440 controla la unidad de generación 1430 para generar los cuartos datos de detección de integridad. La unidad de generación 1430 puede generar los cuartos datos de detección de integridad reflejando los cuartos datos junto con los primeros, segundos y terceros datos de detección de integridad en la Ecuación 1 descrita anteriormente.

Si se generan los cuartos datos de detección de integridad, el controlador 1440 transmite una señal que incluye los cuartos datos y los cuartos datos de detección de integridad al cuerpo principal 100 de un aparato de formación de imágenes.

Si el cuarto proceso de autenticación es un proceso de autenticación para probar la compatibilidad, los terceros datos pueden incluir información de índice de una tabla almacenada previamente en un aparato de formación de imágenes, y los cuartos datos se pueden realizar como datos incluyendo un valor correspondiente a la información de índice.

La unidad de interfaz 1410 se puede realizar como una unidad de tipo contacto o una unidad de tipo conector. El tipo contacto o el método de comunicación de la unidad de interfaz 1410 se explicarán más tarde con mayor detalle.

Como se ha descrito anteriormente, los datos de detección de integridad se pueden usar en el proceso de autenticación o comunicación de datos, en parte o en su totalidad, dependiendo de las realizaciones ejemplares.

La FIG. 20 ilustra un método ejemplar de utilización de datos de detección de integridad en una situación de comunicación donde no se requiere registro en un dispositivo de formación de imágenes o una unidad consumible. Los datos de detección de integridad se pueden usar en parte de un proceso de autenticación.

Como se ilustra en la FIG. 20, el controlador principal 110 y el chip de CRUM 210 realizan comunicación un total de 8 veces para autenticación, y transmiten y comprueban datos de detección de integridad 4 veces durante el proceso.

La prueba de integridad final se completa en el último proceso de autenticación, que es un 8º proceso y no se usa más en el proceso posterior que es el proceso de lectura y escritura de datos. Es decir, el proceso de prueba de integridad se realiza solamente en la autenticación 1, 2, 7 y 8, y la prueba de integridad general se dirige en la autenticación 7 y 8. En la FIG. 20, se puede hacer referencia a un proceso de transmisión/recepción de una señal como proceso de autenticación. Por ejemplo, S1510 y S1530 pueden ser el primer proceso de autenticación, S1550 y S1560 pueden ser el segundo proceso de autenticación, S1570 y S1580 pueden ser el tercer proceso de autenticación, y S1590 y S1620 pueden ser el cuarto proceso de autenticación.

Como se ilustra en la FIG. 20, el controlador principal 110 transmite la señal com-1 que incluye datos 1 y datos 1 de detección de integridad (S1510). Los datos incluyen datos 1 de comando de inicio de autenticación (datos 1 de comando (CMD) de autenticación), DATOS1 de autenticación e indicador SEC U1. Los datos 1 de comando de inicio de autenticación incluyen no solamente un comando, sino también los datos necesarios para realizar la autenticación. El SEC U1 representa información de indicador que sigue a los datos 1 de comando de inicio de autenticación. La información de indicador SEC U1 representa un símbolo para informar de una ubicación de análisis sintáctico de datos de detección de integridad dentro de una señal. La información de indicador se puede representar como un número fijo de bytes. Por ejemplo, se pueden usar 5 bytes para la información de indicador. Por otra parte, el tamaño de los datos 1 de autenticación puede variar según el contenido de los datos, y por consiguiente, también puede variar el tamaño de los datos 1 de detección de integridad.

Tras recibir com-1, el chip de CRUM 210 realiza una prueba de integridad usando los datos 1 de detección de integridad incluidos en la señal (S1520). Posteriormente, el chip de CRUM 210 genera datos 2 de detección de integridad usando los datos a ser transmitidos y los datos 1 de detección de integridad y luego, transmite la señal com-2 que incluye los datos anteriores (S1530). El chip de CRUM 210 realiza la función de una unidad consumible según los datos 1 de comando de inicio de autenticación y configura los datos 2 de autenticación recogiendo datos aleatorios que se generan en consecuencia y datos necesarios para realizar otras funciones. El chip de CRUM 210 configura datos 2 de resultado que representan el resultado de un trabajo que se realiza según los datos 1 de comando de inicio de autenticación. El chip de CRUM 210 transmite com-2, que es una señal que incluye datos 2 de autenticación, datos 2 de resultado, indicador SEC U2 y datos 2 de detección de integridad (S1530).

Tras recibir el com-2, el controlador principal 110 separa los datos 2 de detección de integridad del com-2 recibido y

realiza la prueba de integridad (S1540).

Si se determina que hay un error en al menos una de las operaciones de prueba de integridad descritas anteriormente (S1520, S1540), el controlador principal 110 o el chip de CRUM 210 pueden detener el proceso de autenticación y determinar que la autenticación ha fallado. En este caso, el controlador principal 110 puede informar del fallo de la autenticación a través de la unidad de interfaz de usuario 120 que está formada en el controlador principal 100.

Por otra parte, si se confirma la integridad, el controlador principal 110 y el chip de CRUM 210 realizan los procesos de autenticación posteriores secuencialmente.

En la FIG. 20, los datos de detección de integridad no se usan en el segundo y tercer procesos de autenticación. En este caso, incluso si existen los siguientes datos 3 de trabajo de autenticación posteriores, el controlador principal 110 transmite com-3, que es una señal que incluye el comando 3 de autenticación y los datos 3 de autenticación al chip de CRUM 210 sin generación adicional de datos 3 de detección de integridad (S1550).

Cuando se recibe com-3, el chip de CRUM 210 realiza un trabajo sin realizar una prueba de integridad. Específicamente, el chip de CRUM 210 transmite com-4, que es una señal que incluye datos 4 de autenticación y datos 4 de resultado de autenticación al controlador principal 110 (S1560).

El controlador principal 110 también transmite com-5, que es una señal que incluye el comando 5 de autenticación y datos 5 de autenticación sin realizar una prueba de integridad (S1570), y el chip de CRUM 210 transmite com-6, que es una señal que incluye datos 6 de autenticación y datos 6 de resultado de autenticación (S1580). El segundo y el tercer procesos de autenticación se pueden realizar sin datos de detección de integridad.

El controlador principal 110 realiza datos de detección de integridad de nuevo en el proceso de autenticación final. Es decir, el controlador principal 110 genera datos 7 de detección de integridad usando datos 1 y 2 de detección de integridad, que son todos los datos de detección de integridad existentes junto con el comando 7 de autenticación, datos 7 de autenticación y SECT 7, y transmite com-7 que es una señal que incluye los datos anteriores al chip de CRUM 210 (S1590).

El chip de CRUM 210 en última instancia prueba los datos que se transmiten/reciben y se almacenan temporalmente a lo largo de todo el proceso de comunicación usando datos 7 de detección de integridad (S1600). Si la integridad se confirma según el resultado de prueba final, el chip de CRUM 210 determina que la autenticación tiene éxito (S1610) y realiza el siguiente proceso, tal como generar datos a ser transmitidos a un aparato de formación de imágenes. Si no hay nada que registrar en una memoria en el proceso de autenticación que indique que no hay datos almacenados temporalmente, se puede omitir la operación de almacenamiento de datos en una memoria no volátil (no mostrada).

El chip de CRUM 210 transmite com-8, que es una señal que incluye datos 8 de autenticación, datos 8 de resultado de autenticación, SEC T8 y datos 8 de detección de integridad al controlador principal 110 (S1620). Con el fin de generar los datos de detección de integridad 8, se usan los datos 1, 2 y 7 de detección de integridad, que son todos los datos que se han transmitidos/recibidos hasta el momento.

El controlador principal 110 también realiza toda la prueba de integridad usando los datos de detección de integridad SEC T8 incluidos en la señal de comunicación de autenticación 8 recibida desde el chip de CRUM (S1630). Si la integridad se confirma según la prueba de integridad (S1640), llega a ser en un estado de autenticación con éxito y el controlador principal 110 realiza las operaciones posteriores tales como generar una clave de sesión. Del mismo modo, si no hay nada que registrar en una memoria en el proceso de autenticación que indique que no hay datos almacenados temporalmente, se puede omitir la operación de almacenamiento de datos en una memoria no volátil (no mostrada).

Los datos de detección de integridad que se usan en tal proceso de comunicación se generan como los datos de detección de integridad usados previamente que se reflejan de manera acumulativa.

Por ejemplo, los datos de detección de integridad se pueden procesar como:

Datos 1 de detección de integridad = E(CMD de autenticación / DATOS1 de autenticación /SEC U1)

Datos 2 de detección de integridad = E(datos 2 de autenticación / resultado 2 de autenticación / SEC U2 / datos 1 de detección de integridad)

Datos T1 de detección de integridad = E(CMD 7 de autenticación / datos 7 de autenticación / datos 1 de detección de integridad / datos 2 de detección de integridad)

Datos T2 de detección de integridad = E(datos 8 de autenticación / resultado 8 de autenticación / SEC T2 / datos 1 de detección de integridad / datos 2 de detección de integridad / datos T1 de detección de integridad)

En las ecuaciones anteriores, E () representa una función para obtener un valor de resultado aplicando una ecuación

predeterminada. Como se ilustra en las FIG. 17 y 18, los datos que se representan como datos de autenticación o resultado de autenticación pueden incluir datos de verificación tales como suma de comprobación o MAC que se han usado para estabilidad de comunicación individual.

Los datos de detección de integridad que se usan para algo del proceso de autenticación se pueden configurar como se ilustra en las FIG. 21 - 24.

La FIG. 21 ilustra los primeros datos de detección de integridad que el controlador principal 110 transmite al chip de CRUM 210 durante el primer proceso de autentificación. Como se ilustra en la FIG. 21, el controlador principal 110 genera un nuevo valor de 8 bytes aplicando los primeros 8 bytes y los siguientes 8 bytes de datos de comunicación a una ecuación o algoritmo de cifrado específico, y genera el siguiente valor operando el valor de 8 bytes recién generado con los siguientes 8 bytes. Usando este método, el controlador principal 110 puede generar datos de detección de integridad generando la misma ecuación o algoritmo hasta SECU 1 y almacenar temporalmente los datos de detección de integridad generados. Si el número de datos de los 8 bytes finales no asciende a 8 bytes, un valor específico tal como 0x00 se puede rellenar para completar 8 bytes, y la operación de bytes insuficientes se puede omitir.

Cuando se generan datos de detección de integridad (VC), si los datos de detección de integridad son SECU, se deberían usar los datos de detección de integridad que se usaron justo antes. No obstante, los datos de detección de integridad ilustrados en la FIG. 21 se pueden transmitir por primera vez, y no hay datos de detección de integridad previos. En este caso, se pueden usar datos iniciales de integridad que se inicializan como un valor específico tal como 0x00, o se puede realizar una operación sin incluir los datos de integridad previos. Tales condiciones pueden no ser aplicables si un dispositivo de formación de imágenes y un chip de CRUM generan datos de integridad usando el mismo método.

Si se recibe com-1 durante el primer proceso de autenticación, el chip de CRUM prueba los valores de CMD y DATOS usando CRC para comprobar si hay un problema. El chip de CRUM genera un valor según el método para generar datos de detección de integridad explicado en la FIG. 21 usando los datos de comunicación anteriores, incluyendo la cadena SECU 1, y compara el valor con VC1 incluido en la señal recibida en el primer proceso de autenticación. Es decir, el chip de CRUM 210 genera y compara datos de detección de integridad de la misma forma que el controlador principal 110.

Si hay un problema en la verificación de datos de integridad, el chip de CRUM no realiza el siguiente proceso de autenticación. En este caso, el dispositivo de formación de imágenes puede comprobar un error del chip de CRUM y, por consiguiente, puede detener o reiniciar una operación. Si no hay ningún problema en verificar los datos de integridad, el dispositivo de formación de imágenes almacena temporalmente VC1 y realiza la siguiente operación.

El chip de CRUM 210 realiza una operación de autenticación de cifrado según el contenido de DATOS y genera com-2 que tiene datos relacionados con el cifrado a ser usados en un aparato de formación de imágenes, datos específicos almacenados en el chip de CRUM 210, un número de serie del chip de CRUM y datos aleatorios como DATOS. El chip de CRUM 210 se puede cifrar usando un método de cifrado que usa todo o parte de los DATOS como una clave simétrica o asimétrica. El contenido de com-2 incluye DATOS, SW que indica si un trabajo ha tenido éxito o ha fallado según un comando recibido, CRC, que es un código de detección de errores, un símbolo, VC1 y VC2. En el caso de com-2, el símbolo se establece que es la Cadena SECU2. Los datos 2 de detección de integridad, es decir, VC2 se pueden generar usando el método ilustrado en la FIG. 22.

Como se ilustra en la FIG. 22, DATOS2, SW2, CRC2, SECU2 y VC1 están categorizados por 8 bytes, y cada uno de los datos categorizados se calcula de forma secuencial usando una ecuación o un algoritmo de cifrado específico. El relleno se puede usar dependiendo de la longitud de los datos, generando por ello VC2. El VC2 generado se almacena temporalmente en el chip de CRUM 210.

Las FIG. 23 y 24 ilustran un método y una configuración ejemplares para generar datos de detección de integridad que se usan en el cuarto proceso de autenticación.

Por ejemplo, en la FIG. 20, el controlador principal 10 usa datos de detección de integridad cuando se transmite com-7, y el chip de CRUM 210 usa datos de detección de integridad cuando se transmite com-8.

Com-7 incluye CMD que representa com-7, DATOS necesarios para la operación Aut-4, CRC, y cadena de símbolos y VC3 que indica el final de la comunicación que utiliza datos de detección de integridad. En este caso, los DATOS se cifran usando una clave de sesión generada en Aut-1. La cadena de símbolos de com-7 es SECT1.

Como se ilustra en la FIG. 23, VC3 se genera usando CMD3, DATOS3, CRC3, Cadena SECT1 y VC1 y VC2 que son todos los datos de detección de integridad que se han generado hasta el momento. El controlador principal 110 almacena temporalmente el VC3 generado. Cuando se recibe com-7, el chip de CRUM 210 genera datos de detección de integridad de la misma manera que se ilustra en la FIG. 23. Como VC1 y VC2 se almacenan temporalmente en el chip de CRUM 110 durante el proceso Aut-1, se pueden generar datos de detección de integridad que son iguales a VC3. Si hay un problema en la verificación de los datos de integridad, el chip de CRUM no realiza el siguiente proceso de autenticación. En este caso, el dispositivo de formación de imágenes puede

comprobar un error del chip de CRUM y por consiguiente, puede detener o reiniciar una operación.

Si no hay ningún problema en la verificación de los datos de integridad, el chip de CRUM 210 descifra los DATOS en una clave de sesión, realiza las operaciones necesarias para Aut-4, y genera datos com-8 para responder al aparato de formación de imágenes. Com- 8 incluye DATOS, SW, CRC, Cadena SECT2 que son necesarios para Aut-4 y VC4 que son datos de integridad finales. Los DATOS se cifran a una clave de sesión.

La FIG. 24 ilustra un método y una configuración ejemplares para generar VC4. Como se ilustra en la FIG. 24, el chip de CRUM 210 puede generar VC4 calculando DATOS4, SW4, CRC4, Cadena SECT2 y VC!, VC2, VC3 en 8 bytes secuencialmente.

Cuando se recibe com-8, el controlador principal 110 del dispositivo de formación de imágenes genera VC4 usando DATOS4, SW4, CRC4, Cadena SECT2 y VC1, VC2, VC3 que se almacenan temporalmente en el cuerpo principal 100 del dispositivo de formación de imágenes y los comparan para confirmar la integridad. Si no hay ningún problema en la prueba de integridad, los DATOS se descifran en una clave de sesión para realizar una operación de autenticación final. Por consiguiente, cuando el chip de CRUM 210 o la unidad consumible 200 donde está montado el chip de CRUM 210 se confirma que es compatible con el dispositivo de formación de imágenes 100, se determina que una autenticación final tiene éxito y se puede realizar la operación de comunicación posterior.

La unidad consumible 200 puede ser desmontable del cuerpo principal 100 del aparato de formación de imágenes. Cuando se monta la unidad consumible 200, se puede conectar eléctricamente al cuerpo principal 100. Tal conexión se puede realizar en un tipo contacto o un tipo conector, y la comunicación entre la unidad consumible 200 y el cuerpo principal 100 se puede realizar usando un método I2C.

La FIG. 25 ilustra un ejemplo de la configuración externa de la unidad de interfaz 1410 en un tipo contacto. Como se ilustra en la FIG. 25, la unidad consumible 200 incluye una unidad de contacto 2010 para la comunicación. El cuerpo principal 100 del dispositivo de formación de imágenes incluye una unidad de contacto. Cuando la unidad consumible 100 se monta en el cuerpo principal 100, la unidad de interfaz 1410 se pone en contacto con la unidad de contacto 2010 formada en el cuerpo principal 100 del dispositivo de formación de imágenes para ser conectada eléctricamente.

La FIG. 26 ilustra un estado de conexión ejemplar entre la unidad consumible 200 en un tipo contacto y el cuerpo principal 100 del aparato de formación de imágenes. La FIG. 26 ilustra una unidad de contacto 2020, una placa principal 2040 donde se pueden disponer diversas piezas, incluyendo el controlador principal 110, y un cable de conexión 2030 para conectar la placa principal 2040 con la unidad de contacto 2020. Cuando la unidad consumible 200 se monta en el cuerpo principal 100 como se ilustra en la FIG. 26, la unidad de contacto 2010 formada en la unidad consumible 200 hace contacto con el cuerpo principal 100 para ser conectados eléctricamente uno con otro.

Cuando las unidades de contacto son de un tipo contacto como se ilustra en la FIG. 25 y la FIG. 26, no hay nada para fijar los lados de contacto. Por lo tanto, si hay oscilación en el aparato de formación de imágenes, las unidades de contacto 2010, 2020 pueden separarse temporalmente una de otra, causando problemas en la comunicación. Es decir, si los puntos de contacto de las unidades consumibles montadas en el dispositivo de formación de imágenes se separan, se pueden intercambiar datos incorrectos. No obstante, si se usan datos de detección de integridad en la realización de la autenticación y la comunicación de datos como se ha descrito anteriormente, se pueden resolver tales problemas. Es decir, el controlador principal 110 o el chip de CRUM 210 pueden determinar un fallo de autenticación o un error de comunicación comprobando datos de detección de integridad de los datos previos que se han recibido cuando los puntos de contacto se unen normalmente entre sí y los datos que se reciben mientras que los puntos de contacto están unidos de manera inestable entre sí. Por consiguiente, puede no ser realizada la operación de lectura o escritura de datos, evitando que información incorrecta se registre en la unidad consumible 200.

La FIG. 27 ilustra una configuración externa ejemplar de la unidad de interfaz 1410 como tipo conector. Con referencia a la FIG. 27, la unidad consumible 200 incluye un conector 2210 para la comunicación. El conector 2210 está conectado a un puerto 2220 que puede estar en el cuerpo principal 100 del aparato de formación de imágenes. En el tipo conector, pueden ocurrir problemas de contacto, por ejemplo, si una sustancia extraña se interpone entre el conector 2210 y el puerto 2220 o si una unidad de fijación se daña cuando la unidad de interfaz 1410 es de un tipo conector, como se ilustra en la FIG. 27. En este caso, una realización ejemplar de la presente invención puede evitar que se realice una operación incorrecta realizando autenticación o comunicación de datos usando datos de detección de integridad según diversas realizaciones ejemplares.

Se puede usar un método de comunicación en serie para comunicación entre la unidad consumible 200 y el cuerpo principal 100 del aparato de formación de imágenes. Por ejemplo, se puede usar un método de comunicación I2C.

La FIG. 28 ilustra varias formas de onda ejemplares de una señal que se puede transmitir y recibir entre la unidad consumible 200 y el cuerpo principal 100 del dispositivo de formación de imágenes según un método de comunicación I2C. El método de comunicación I2C incluye VCC y GND que suministran alimentación a un esclavo, SCL que proporciona un reloj para la sincronización entre el controlador principal 110 y el chip de CRUM 210, SDA, que es una línea de datos de interfaz I2C, etc. Por tanto, la comunicación I2C tiene una estructura simple y puede

conectar una pluralidad de nodos a un bus.

El método de comunicación I2C se puede preparar para comunicación entre los IC en un circuito de una placa y, de este modo, no hay configuración para comprobar errores durante la comunicación. No obstante, pueden ocurrir diversos errores de comunicación durante un proceso de comunicación entre la unidad consumible y el aparato de formación de imágenes.

Puede ocurrir una resistencia impredecible, por ejemplo, puede ocurrir una interferencia de ruido eléctrico en la superficie de contacto, la comunicación puede verse afectada por polvo, potencia del tóner, etc., o los puntos de contacto de las superficies de contacto pueden separarse debido a la oscilación. Además, los datos de comunicación incorrectos se pueden transmitir en el método de comunicación I2C a medida que los relojes (SCL) llegan a ser incoherentes, y se cambian los datos de transmisión (SDA).

La FIG. 29 ilustra una SDA y un SCL ampliados en la señal I2C de la FIG. 28. Como se ilustra en la FIG. 29, una señal de SCL tiene 8 señales altas/bajas coherentes a la vez y 1 byte de datos se representa a medida que se generan señales altas/bajas con SDA, en consecuencia. Es decir, una señal alta/baja representa 1 bit en SCL o SDA.

Según un método I2C, si ocurre un problema durante la comunicación, es decir, si hay distorsión de señal solamente en 1 bit, no es posible transmitir datos normalmente. Por ejemplo, si hay un problema en la transmisión de datos de 4 bytes, 00000000 00000000 00000000 00000000 (“0” como número decimal), y de este modo solamente se cambia el primer dígito de 1 bit, puede haber una diferencia considerable a medida que llega a ser 10000000 00000000 00000000 00000000 (“2147483648” como número decimal).

No obstante, según una realización ejemplar de la presente invención, incluso si tal error ocurre durante la comunicación, los datos se pueden probar inmediatamente usando los datos de detección de integridad que se han transmitido o recibido previamente, y la integridad de todos los datos también se puede comprobar en la operación final usando los datos de detección de integridad. Por consiguiente, incluso si la unidad de interfaz 1410 está conectada al cuerpo principal en un tipo contacto o tipo conector, o la comunicación entre el cuerpo principal 100 y la unidad consumible 200 se realiza según el método de comunicación I2C, se puede evitar el registro de datos erróneos debidos a una autenticación incorrecta o una comunicación incorrecta.

El método para autenticación y comunicación según una realización ejemplar se puede codificar como software respectivamente, y registrar en un medio registrable no transitorio. El medio registrable no transitorio se puede instalar en un aparato de formación de imágenes, una unidad consumible, o en un chip de CRUM, y/o en varios tipos de aparatos, y por consiguiente, el método de autenticación y comunicación descrito anteriormente se puede realizar en diversos aparatos.

El medio registrable no transitorio se refiere a un medio que puede almacenar datos de manera semipermanente en lugar de almacenar datos durante un tiempo corto, tal como un registro, una memoria caché y una memoria, y puede ser legible por un aparato. Las diversas aplicaciones o programas mencionados anteriormente se pueden almacenar en un medio registrable no temporal, tal como un CD, DVD, disco duro, disco Blu-ray, USB, tarjeta de memoria y ROM y proporcionar en el mismo. Aunque se han mostrado y descrito unas pocas realizaciones de la presente invención, se apreciará por los expertos en la técnica que se pueden hacer cambios en esta realización sin apartarse de los principios y el espíritu de la invención, el alcance de la cual se define en las reivindicaciones y sus equivalentes.

REIVINDICACIONES

1. Un aparato de formación de imágenes, que comprende:

un controlador principal (110) capaz de controlar operaciones del aparato de formación de imágenes; y

un chip de Monitorización de Unidad Sustituible por el Cliente, CRUM, (210) que almacena información con respecto a una unidad consumible (200),

en donde el controlador principal (110) es operable para transmitir al chip de CRUM (210) un primer conjunto de datos y unos primeros datos de detección de integridad con respecto a los primeros datos para autenticación con el chip de CRUM (210), el primer conjunto de datos que comprende primeros datos de comando, primeros datos, primeros datos de Comprobación de Redundancia Cíclica, CRC, y primeros datos de símbolo,

en donde el chip de CRUM (210) es operable:

para generar segundos datos de detección de integridad usando tanto un segundo conjunto de datos a ser transmitido al controlador principal (110) como los primeros datos de detección de integridad en respuesta al primer conjunto de datos y los primeros datos de detección de integridad que se reciben, el segundo conjunto de datos que comprende segundos datos, segundos datos de resultado, segundos datos de CRC y segundos datos de símbolos, y

para transmitir el segundo conjunto de datos y los segundos datos de detección de integridad al controlador principal (110).

2. El aparato de formación de imágenes según la reivindicación 1, en donde el controlador principal (110) es operable:

para generar terceros datos de detección de integridad usando un tercer conjunto de datos, los primeros datos de detección de integridad y los segundos datos de detección de integridad, el tercer conjunto de datos que comprende terceros datos de comando, terceros datos, terceros datos de CRC y terceros datos de símbolos, y

para transmitir los terceros datos y los terceros datos de detección de integridad al chip de CRUM (210),

en donde el chip de CRUM (210) es operable:

para probar el tercer conjunto de datos usando los terceros datos de detección de integridad, en respuesta a la recepción del tercer conjunto de datos,

para generar cuartos datos de detección de integridad usando un cuarto conjunto de datos y los primeros a terceros datos de detección de integridad, en respuesta a la integridad del tercer conjunto de datos que se verifica, el cuarto conjunto de datos comprende cuartos datos, cuartos datos de resultado, cuarto datos de CRC y cuarto datos de símbolo, y

para transmitir el cuarto conjunto de datos y los cuartos datos de detección de integridad al controlador principal (110),

en donde el controlador principal (110) es operable para probar el cuarto conjunto de datos usando los cuartos datos de detección de integridad en respuesta a la cuarta señal que se recibe.

3. El aparato de formación de imágenes según la reivindicación 1,

en donde el controlador principal (110) y el chip de CRUM (210) están adaptados para realizar una autenticación a través de una pluralidad de procesos de autenticación,

en donde el controlador principal (110) es operable:

para generar terceros datos de detección de integridad usando un tercer conjunto de datos, los primeros datos de detección de integridad y los segundos datos de detección de integridad en un proceso de autenticación final de entre la pluralidad de procesos de autenticación,

el tercer conjunto de datos que comprende terceros datos de comando, terceros datos, terceros datos de CRC y terceros datos de símbolo y para transmitir el tercer conjunto de datos y los terceros datos de detección de integridad al chip de CRUM,

en donde el chip de CRUM (210) es operable para generar cuartos datos de detección de integridad usando un cuarto conjunto de datos y los primeros a terceros datos de detección de integridad, en respuesta a la recepción del tercer conjunto de datos y los terceros datos de integridad, y para transmitir el cuarto conjunto de datos y los cuartos datos de detección de integridad al controlador principal, el cuarto conjunto de datos que comprende cuartos datos, cuartos datos de resultado, cuartos datos de CRC y cuartos datos de símbolo.

4. El aparato de formación de imágenes según la reivindicación 3, en donde la pluralidad de procesos de autenticación incluye un primer proceso de autenticación en el que el controlador principal (110) y el chip de CRUM (210) son operables para transmitir y recibir los primeros datos y los segundos datos y para generar una clave de sesión respectivamente, un segundo proceso autenticación para sincronizar una primera tabla almacenada en cada uno del controlador principal (110) y el chip de CRUM (210), un tercer proceso de autenticación para sincronizar una segunda tabla almacenada en cada uno del controlador principal (110) y el chip de CRUM (210), y un cuarto proceso de autenticación en el que el controlador principal (110) y el chip de CRUM (210) son operables para transmitir y recibir los terceros datos y los cuartos datos y determinar la compatibilidad entre el controlador principal (110) y el chip de CRUM (210).

5. Un chip de Monitorización de Unidad Sustituible por el Cliente, CRUM, (1400) operable para comunicarse con un aparato de formación de imágenes, el chip de CRUM que comprende:

una unidad de interfaz (1410) que es operable para recibir un primer conjunto de datos y primeros datos de detección de integridad con respecto al primer conjunto de datos desde un controlador principal (110) del aparato de formación de imágenes, el primer conjunto de datos que comprende primeros datos de comando, primeros datos, primeros datos de Comprobación de Redundancia Cíclica, CRC, y primeros datos de símbolo;

una unidad de generación (1430) que es operable para generar segundos datos de detección de integridad usando tanto un segundo conjunto de datos a ser transmitido al controlador principal (110) del aparato de formación de imágenes como los primeros datos de detección de integridad, el segundo conjunto de datos que comprende segundos datos, segundos datos de resultado, segundos datos de CRC y segundos datos de símbolos, y

un controlador (1440) que es operable para transmitir el segundo conjunto de datos y los segundos datos de detección de integridad al controlador principal (110) del aparato de formación de imágenes.

6. El chip de CRUM según la reivindicación 5, en donde el controlador (1440) es operable para transmitir el segundo conjunto de datos y los segundos datos de detección de integridad al controlador principal (110) del aparato de formación de imágenes en respuesta a la integridad del primer conjunto de datos que se verifica.

7. El chip de CRUM según la reivindicación 5, que comprende además:

un almacenamiento para almacenar los primeros datos de detección de integridad y los segundos datos de detección de integridad.

8. El chip de CRUM según la reivindicación 5, en donde la unidad de generación (1430) es operable para generar cuartos datos de detección de integridad usando los primeros datos de detección de integridad, los segundos datos de detección de integridad y unos terceros datos de detección de integridad y

un cuarto conjunto de datos a ser transmitido a un controlador principal (110) del aparato de formación de imágenes, en respuesta al tercer conjunto de datos y los terceros datos de integridad con respecto al tercer conjunto de datos que se recibe desde el controlador principal (110) del aparato de formación de imágenes,

en donde el controlador (1440) es operable para controlar la unidad de interfaz para transmitir el cuarto conjunto de datos y los cuartos datos de detección de integridad a un controlador principal (110) del aparato de formación de imágenes,

en donde el tercer conjunto de datos comprende terceros datos de comando, terceros datos, terceros datos de CRC y terceros datos de símbolos, y el cuarto conjunto de datos comprende cuartos datos, cuartos datos de resultado, cuartos datos de CRC y cuartos datos de símbolos.

9. El chip de CRUM según la reivindicación 8, en donde el chip de CRUM (1400) comprende una unidad de prueba (1420) que es operable para detectar la integridad del tercer conjunto de datos usando terceros datos de detección de integridad y los primeros a segundos datos de detección de integridad almacenados.

10. El chip de CRUM según la reivindicación 5, en donde el controlador (1440) es operable para generar una clave de sesión usando el primer conjunto de datos y el segundo conjunto de datos, y para realizar un proceso de autenticación para sincronizar una primera tabla almacenada en cada uno del controlador principal (110) del aparato de formación de imágenes y el chip de CRUM (1400), un proceso de autenticación para sincronizar una segunda tabla almacenada en cada uno del controlador principal (110) del aparato de formación de imágenes y el chip de CRUM (1400), y un proceso de autenticación para determinar la compatibilidad entre el aparato de formación de imágenes y el chip de CRUM (1400) en base a al menos una de la primera tabla y la segunda tabla.

11. El chip de CRUM según una cualquiera de las reivindicaciones 5 a 10, en donde los segundos datos comprenden cualquiera de datos aleatorios, un número de serie del chip, información con respecto a una clave usada para un algoritmo de clave asimétrica, información interna del chip de CRUM e información de resultado sobre el resultado de un trabajo realizado en el chip de CRUM (1400).

12. El chip de CRUM según una cualquiera de las reivindicaciones 5 a 10, en donde los primeros datos comprenden

un primer valor arbitrario, y los segundos datos comprenden un segundo valor arbitrario y un Código de Autenticación de Mensaje generado usando los primeros datos y los segundos datos.

13. El chip de CRUM según una cualquiera de las reivindicaciones 5 a 10, en donde:

los primeros datos de CRC y los segundos datos de CRC son cada uno códigos de detección de errores, y

los primeros datos de símbolo y los segundos datos de símbolo se usan cada uno como un símbolo que identifica datos de detección de integridad a partir de otros datos.

14. Un método de autenticación de un aparato de formación de imágenes, que comprende:

generar primeros datos de detección de integridad con respecto a un primer conjunto de datos por un controlador principal (110), para la autenticación con un chip de Monitorización de Unidad Sustituible por el Cliente, CRUM, (210), el primer conjunto de datos que comprende primeros datos de comando, primeros datos, primeros datos de Comprobación de Redundancia Cíclica, CRC, y primeros datos de símbolo;

transmitir por el controlador principal (110) el primer conjunto de datos y los primeros datos de detección de integridad al chip de CRUM (210);

probar la integridad de la primera señal por el chip de CRUM (210) usando los primeros datos de detección de integridad;

generar por el chip de CRUM (210) segundos datos de detección de integridad usando tanto un segundo conjunto de datos a ser transmitido al controlador principal (110) como los primeros datos de detección de integridad, en respuesta a la integridad del primer conjunto de datos que se verifica; y

transmitir por el chip de CRUM (210) el segundo conjunto de datos y los segundos datos de detección de integridad al controlador principal.

15. Un método de autenticación de un chip de Monitorización de Unidad Sustituible por el Cliente, CRUM, (210) operable para comunicarse con un aparato de formación de imágenes, que comprende:

recibir desde un controlador principal (110) del primer conjunto de datos del aparato de formación de imágenes y los primeros datos de detección de integridad con respecto al primer conjunto de datos, el primer conjunto de datos que comprende primeros datos de comando, primeros datos, primeros datos de Comprobación de Redundancia Cíclica, CRC, y primeros datos de símbolo;

generar segundos datos de detección de integridad usando tanto el segundo conjunto de datos a ser transmitido al controlador principal (110) del aparato de formación de imágenes como los primeros datos de detección de integridad, el segundo conjunto de datos que comprende segundos datos, segundos datos de resultado, segundos datos de CRC y segundos datos de símbolos; y

transmitir el segundo conjunto de datos y los segundos datos de detección de integridad al controlador principal (110) del aparato de formación de imágenes.

FIG. 1

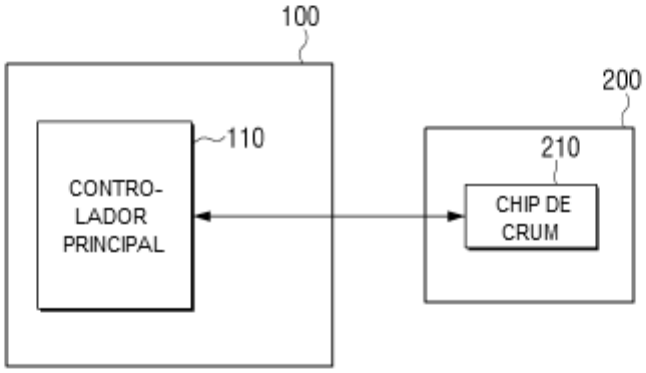

FIG. 2

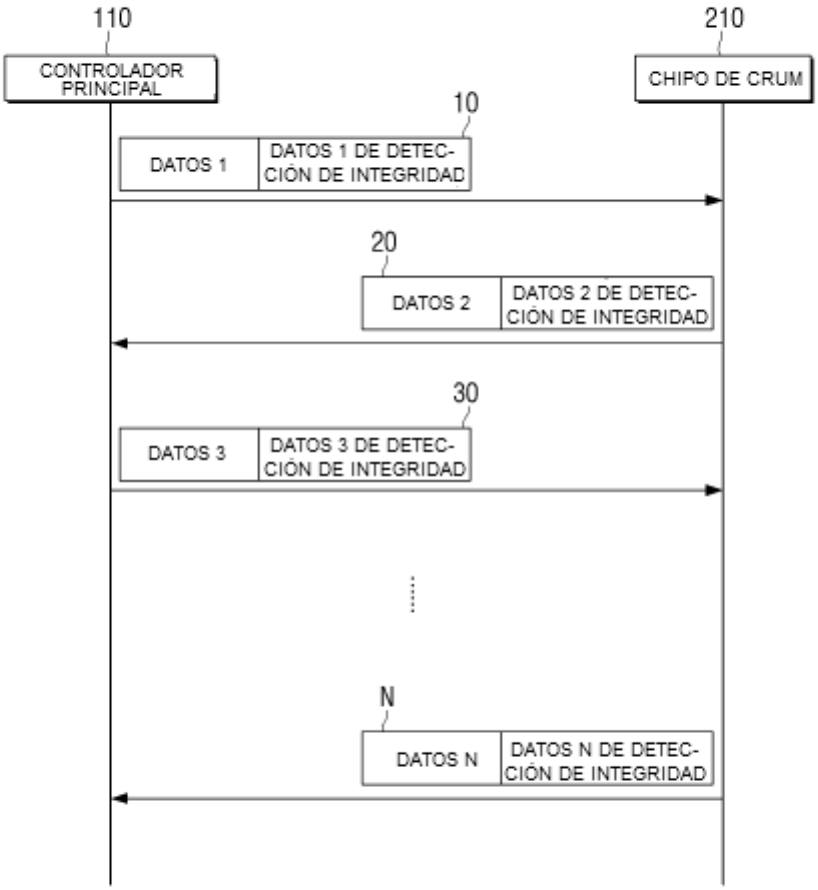
110
CONTROLADOR PRINCIPAL
210
CHIPO DE CRUM
10
DATOS 1
DATOS 1 DE DETEC-CIÓN DE INTEGRIDAD
20
DATOS 2
DATOS 2 DE DETEC-CIÓN DE INTEGRIDAD
30
DATOS 3
DATOS 3 DE DETEC-CIÓN DE INTEGRIDAD
N
DATOS N
DATOS N DE DETEC-CIÓN DE INTEGRIDAD

FIG. 3

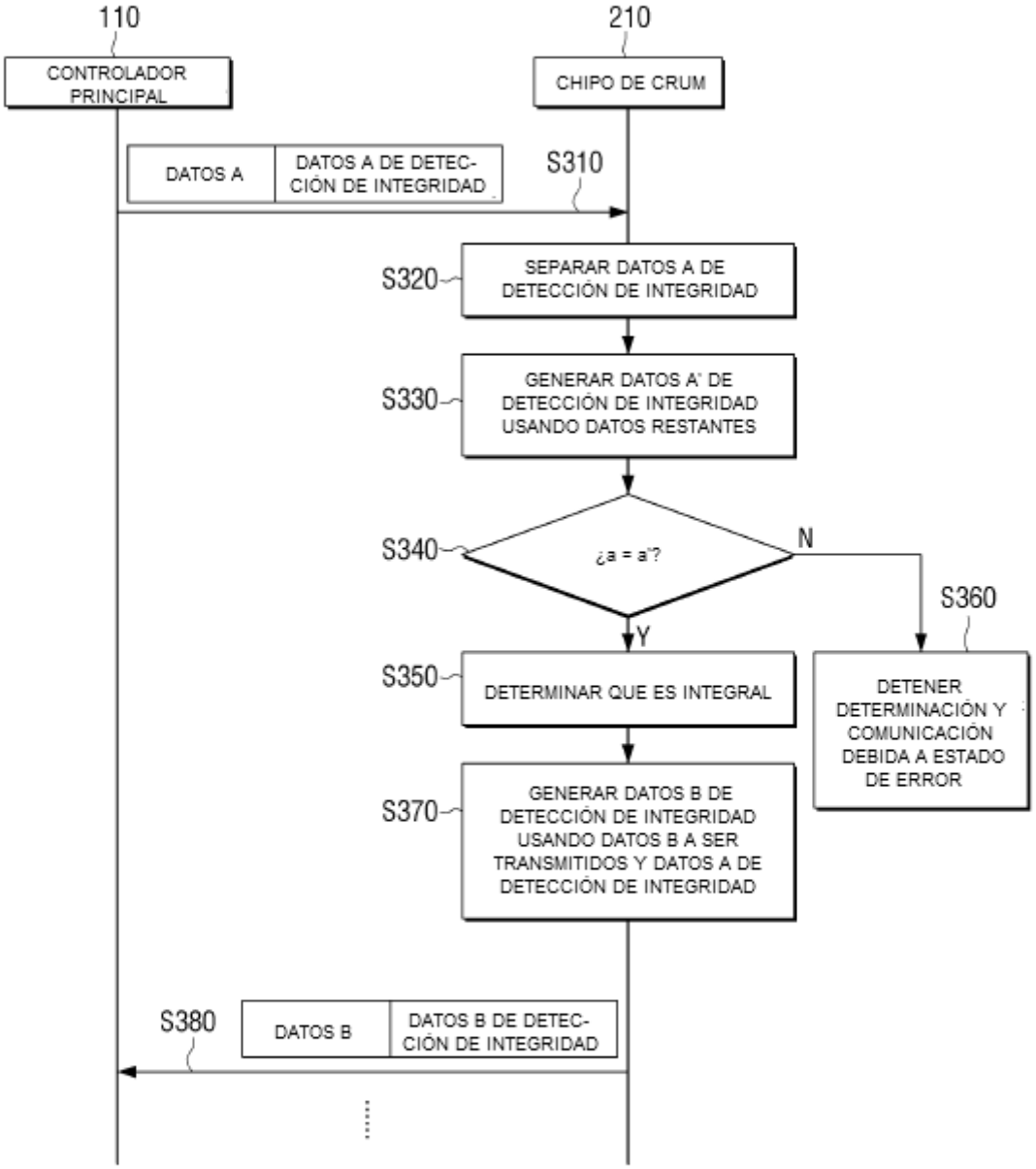
110
CONTROLADOR PRINCIPAL
210
CHIPO DE CRUM
DATOS A
DATOS A DE DETEC-CIÓN DE INTEGRIDAD
S310
S320
SEPARAR DATOS A DE DETECCIÓN DE INTEGRIDAD
S330
GENERAR DATOS A' DE DETECCIÓN DE INTEGRIDAD USANDO DATOS RESTANTES
S340
¿a = a'?
N
S360
Y
S350
DETERMINAR QUE ES INTEGRAL
DETENER DETERMINACIÓN Y COMUNICACIÓN DEBIDA A ESTADO DE ERROR
S370
GENERAR DATOS B DE DETECCIÓN DE INTEGRIDAD USANDO DATOS B A SER TRANSMITIDOS Y DATOS A DE DETECCIÓN DE INTEGRIDAD
S380
DATOS B
DATOS B DE DETEC-CIÓN DE INTEGRIDAD

FIG. 4

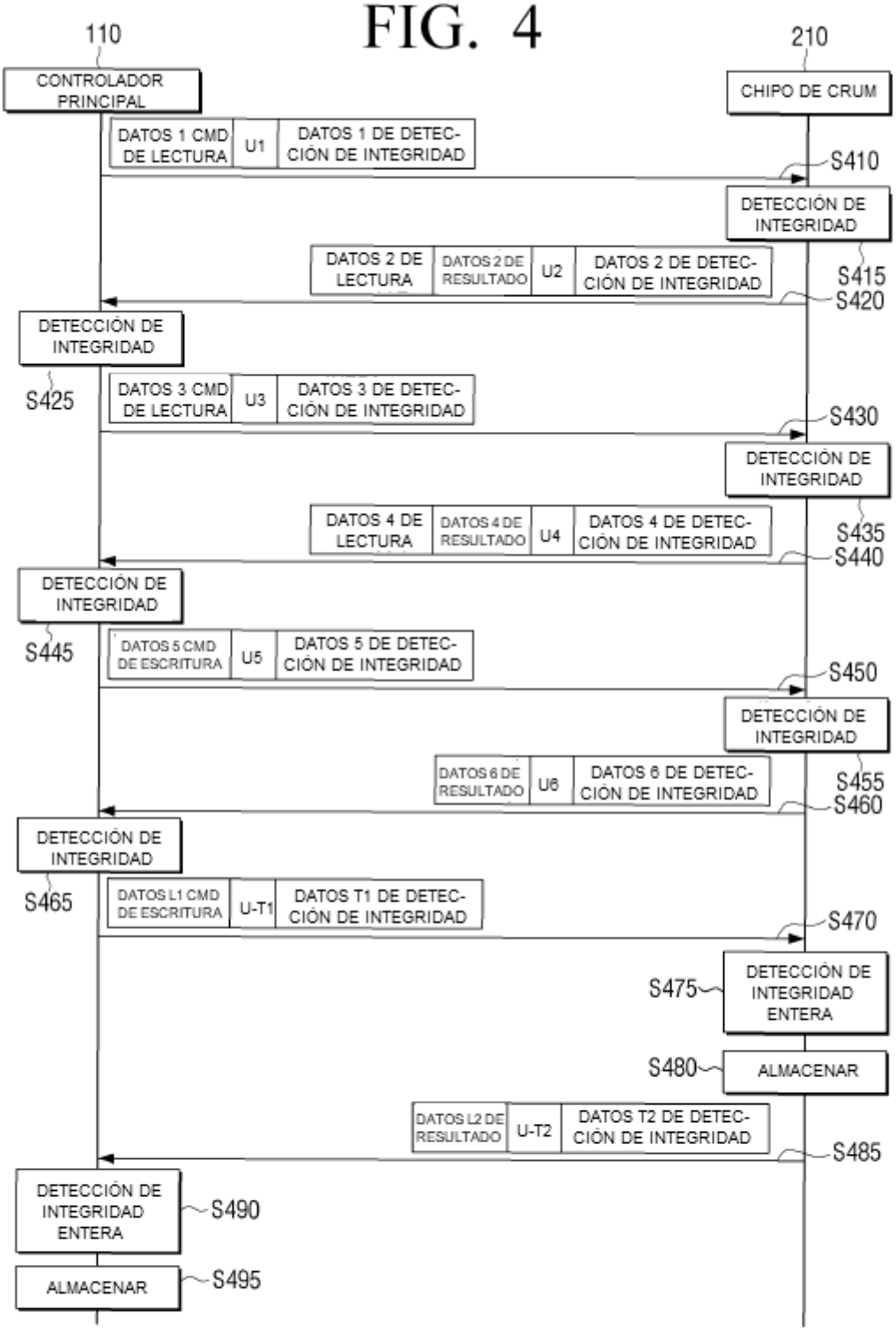
110
CONTROLADOR PRINCIPAL
210
CHIPO DE CRUM
DATOS 1 CMD DE LECTURA
U1
DATOS 1 DE DETECCIÓN DE INTEGRIDAD
S410
DETECCIÓN DE INTEGRIDAD
DATOS 2 DE LECTURA
DATOS 2 DE RESULTADO
U2
DATOS 2 DE DETECCIÓN DE INTEGRIDAD
S415
S420
DETECCIÓN DE INTEGRIDAD
S425
DATOS 3 CMD DE LECTURA
U3
DATOS 3 DE DETECCIÓN DE INTEGRIDAD
S430
DETECCIÓN DE INTEGRIDAD
DATOS 4 DE LECTURA
DATOS 4 DE RESULTADO
U4
DATOS 4 DE DETECCIÓN DE INTEGRIDAD
S435
S440
DETECCIÓN DE INTEGRIDAD
S445
DATOS 5 CMD DE ESCRITURA
U5
DATOS 5 DE DETECCIÓN DE INTEGRIDAD
S450
DETECCIÓN DE INTEGRIDAD
DATOS 6 DE RESULTADO
U6
DATOS 6 DE DETECCIÓN DE INTEGRIDAD
S455
S460
DETECCIÓN DE INTEGRIDAD
S465
DATOS L1 CMD DE ESCRITURA
U-T1
DATOS T1 DE DETECCIÓN DE INTEGRIDAD
S470
S475
DETECCIÓN DE INTEGRIDAD ENTERA
S480
ALMACENAR
DATOS L2 DE RESULTADO
U-T2
DATOS T2 DE DETECCIÓN DE INTEGRIDAD
S485
DETECCIÓN DE INTEGRIDAD ENTERA
S490
ALMACENAR
S495

FIG. 5

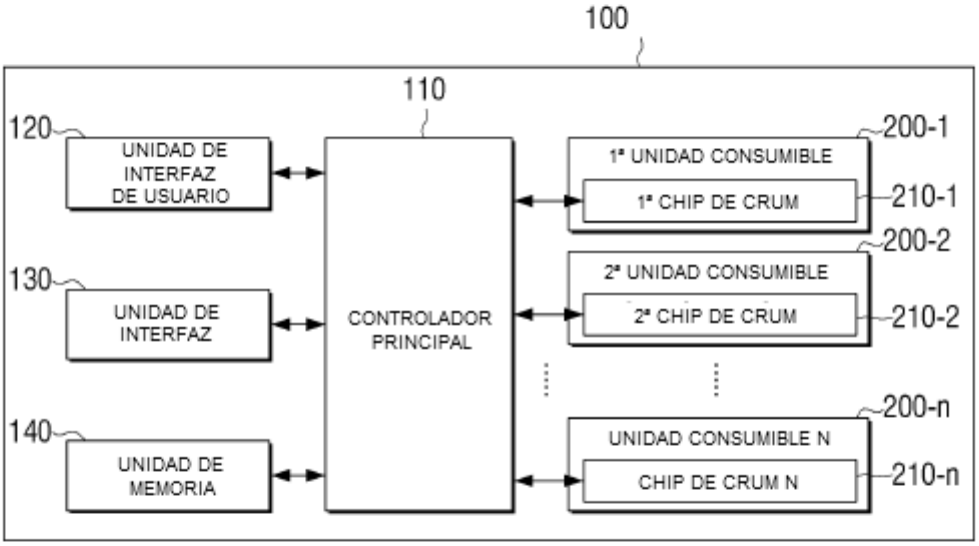
100
110
120
UNIDAD DE INTERFAZ DE USUARIO
130
UNIDAD DE INTERFAZ
140
UNIDAD DE MEMORIA
CONTROLADOR PRINCIPAL
200-1
1ª UNIDAD CONSUMIBLE
1ª CHIP DE CRUM
210-1
200-2
2ª UNIDAD CONSUMIBLE
2ª CHIP DE CRUM
210-2
200-n
UNIDAD CONSUMIBLE N
CHIP DE CRUM N
210-n

FIG. 6

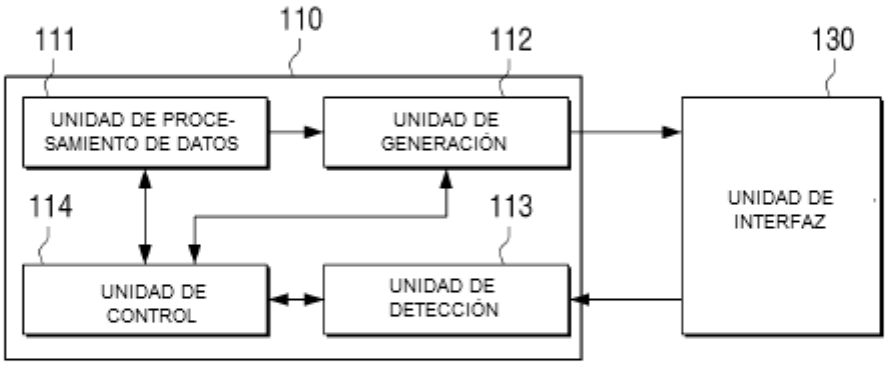
111
110
112
130
UNIDAD DE PROCE-SAMIENTO DE DATOS
UNIDAD DE GENERACIÓN
UNIDAD DE INTERFAZ
114
113
UNIDAD DE CONTROL
UNIDAD DE DETECCIÓN

FIG. 7

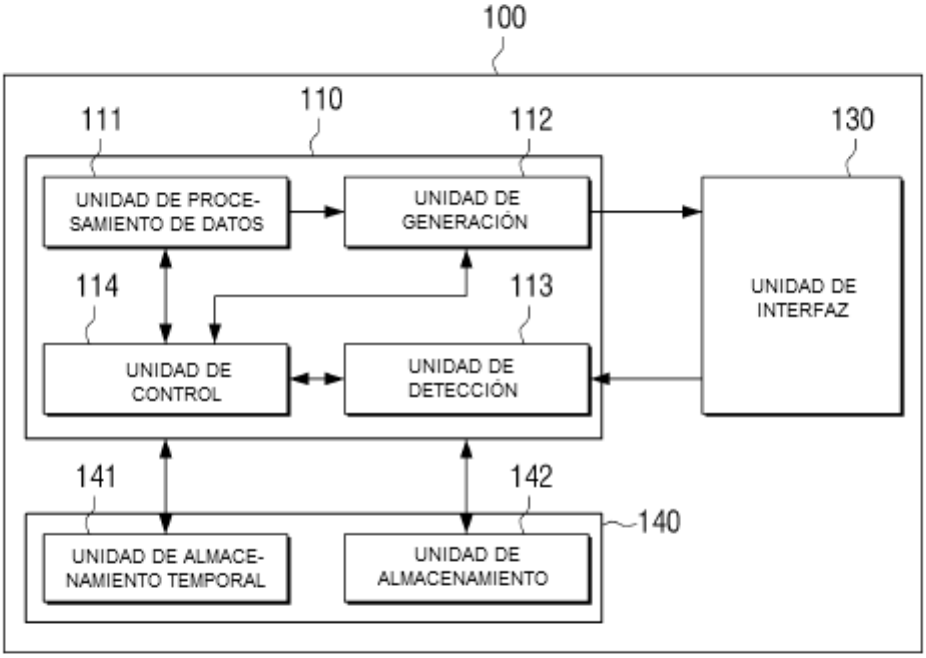
100
110
111
112
130
UNIDAD DE PROCE-SAMIENTO DE DATOS
UNIDAD DE GENERACIÓN
UNIDAD DE INTERFAZ
114
113
UNIDAD DE CONTROL
UNIDAD DE DETECCIÓN
141
142
140
UNIDAD DE ALMACE-NAMIENTO TEMPORAL
UNIDAD DE ALMACENAMIENTO

FIG. 8

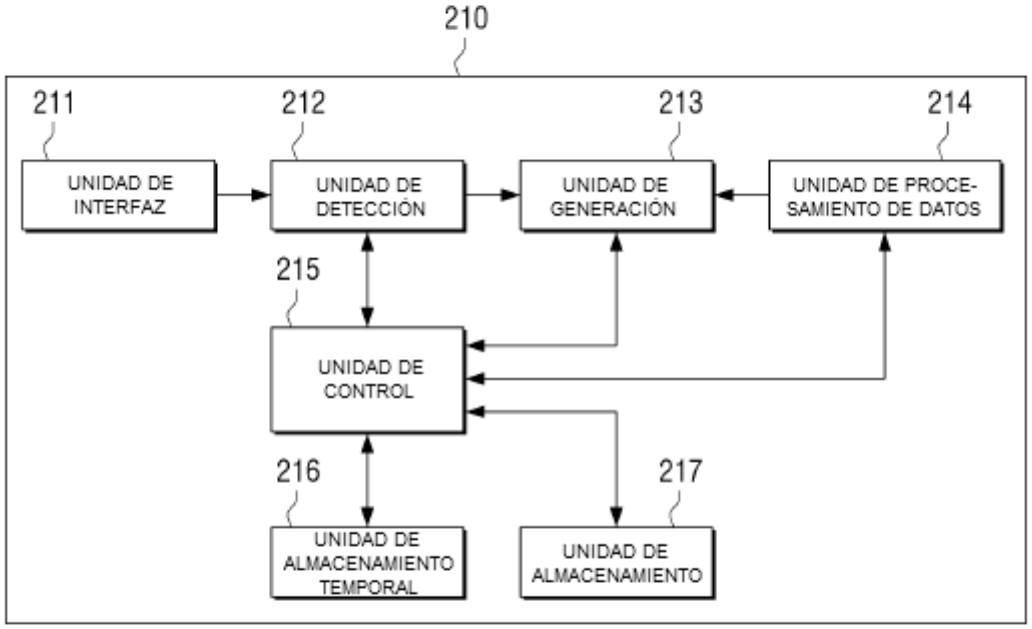
210
211
UNIDAD DE INTERFAZ
212
UNIDAD DE DETECCIÓN
213
UNIDAD DE GENERACIÓN
214
UNIDAD DE PROCE-SAMIENTO DE DATOS
215
UNIDAD DE CONTROL
216
UNIDAD DE ALMACENAMIENTO TEMPORAL
217
UNIDAD DE ALMACENAMIENTO

FIG. 9

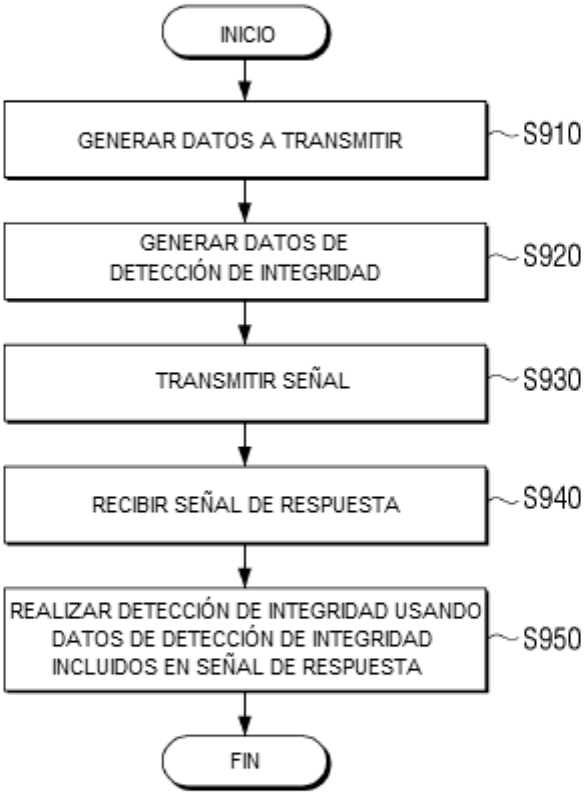
INICIO
GENERAR DATOS A TRANSMITIR
S910
GENERAR DATOS DE DETECCIÓN DE INTEGRIDAD
S920
TRANSMITIR SEÑAL
S930
RECIBIR SEÑAL DE RESPUESTA
S940
REALIZAR DETECCIÓN DE INTEGRIDAD USANDO DATOS DE DETECCIÓN DE INTEGRIDAD INCLUIDOS EN SEÑAL DE RESPUESTA
S950
FIN

FIG. 10

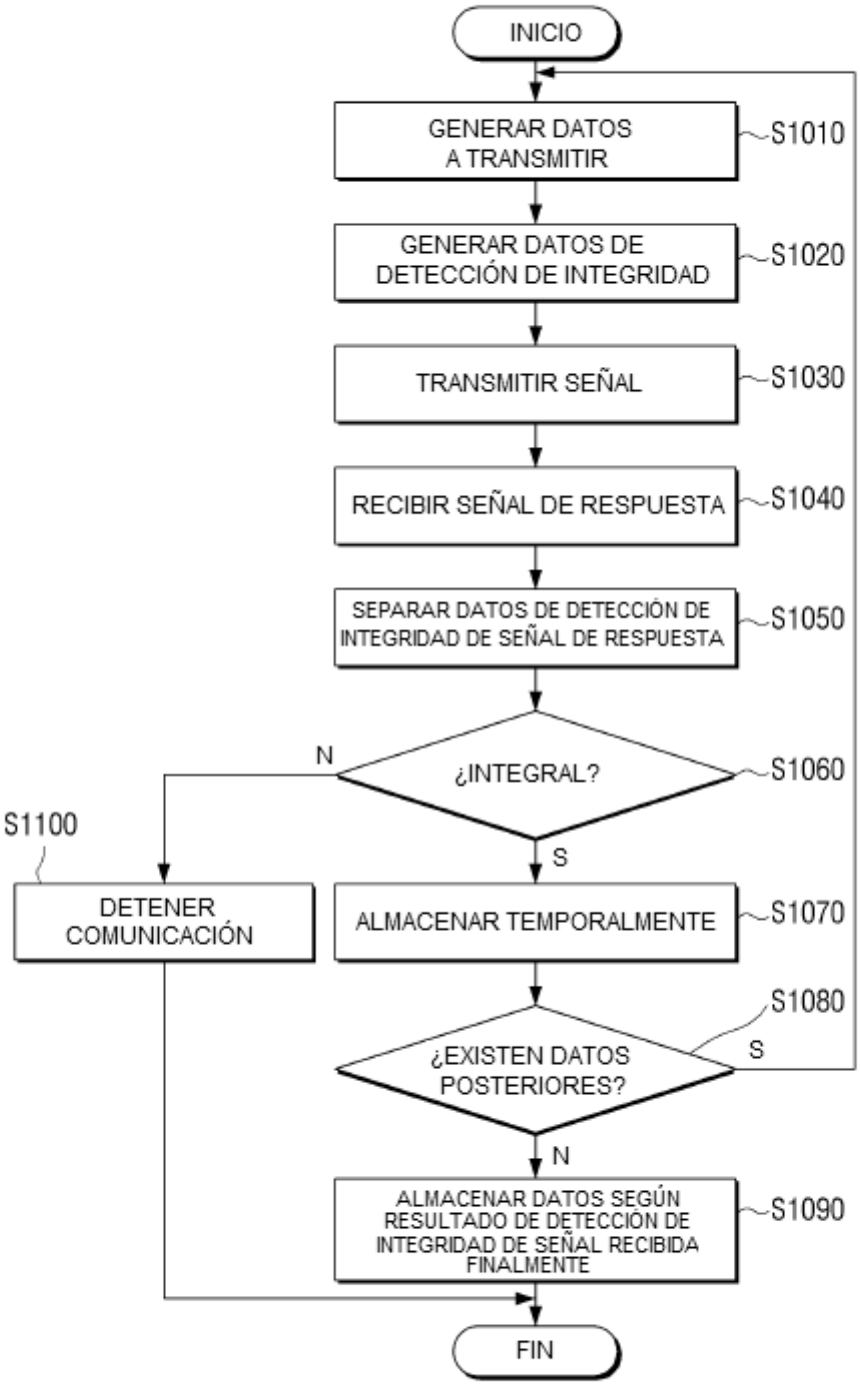
INICIO
GENERAR DATOS A TRANSMITIR
S1010
GENERAR DATOS DE DETECCIÓN DE INTEGRIDAD
S1020
TRANSMITIR SEÑAL
S1030
RECIBIR SEÑAL DE RESPUESTA
S1040
SEPARAR DATOS DE DETECCIÓN DE INTEGRIDAD DE SEÑAL DE RESPUESTA
S1050
¿INTEGRAL?
S1060
N
S
S1100
DETENER COMUNICACIÓN
ALMACENAR TEMPORALMENTE
S1070
S1080
¿EXISTEN DATOS POSTERIORES?
S
N
ALMACENAR DATOS SEGÚN RESULTADO DE DETECCIÓN DE INTEGRIDAD DE SEÑAL RECIBIDA FINALMENTE
S1090
FIN

FIG. 11

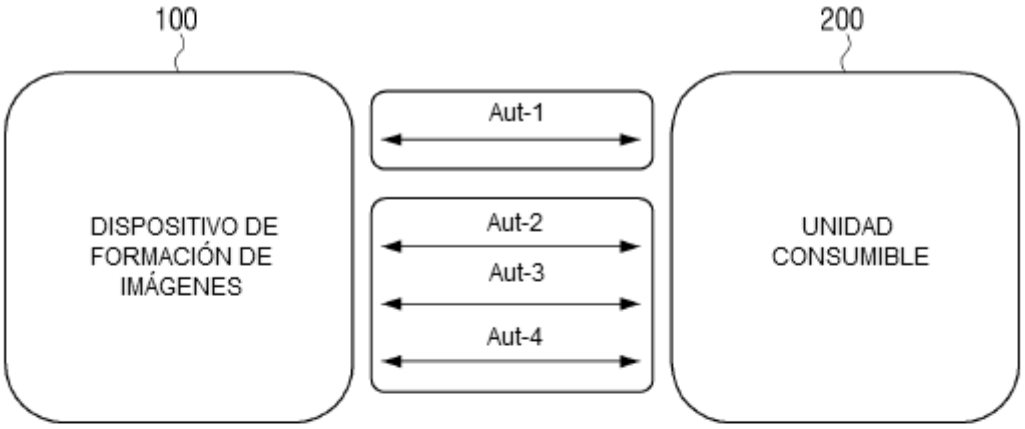
100
200
DISPOSITIVO DE FORMACIÓN DE IMÁGENES
Aut-1
Aut-2
Aut-3
Aut-4
UNIDAD CONSUMIBLE

FIG. 12

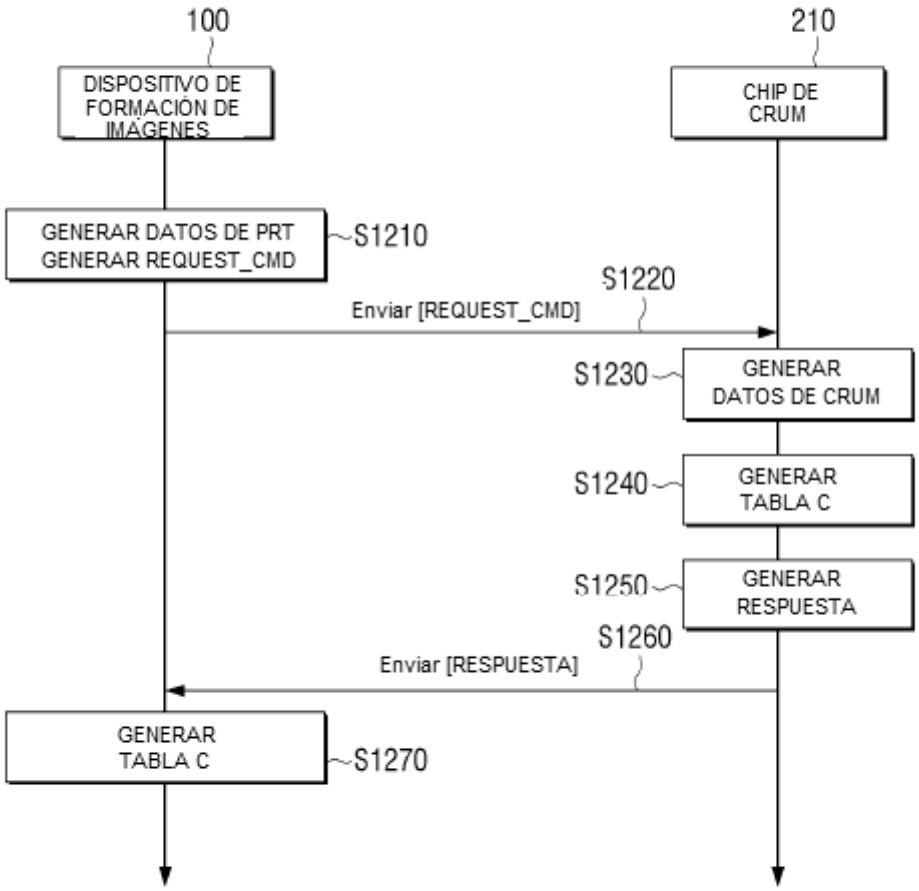
100
210
DISPOSITIVO DE FORMACIÓN DE IMÁGENES
CHIP DE CRUM
GENERAR DATOS DE PRT
GENERAR REQUEST_CMD
S1210
S1220
Enviar [REQUEST_CMD]
S1230
GENERAR DATOS DE CRUM
S1240
GENERAR TABLA C
S1250
GENERAR RESPUESTA
S1260
Enviar [RESPUESTA]
GENERAR TABLA C
S1270

FIG. 13

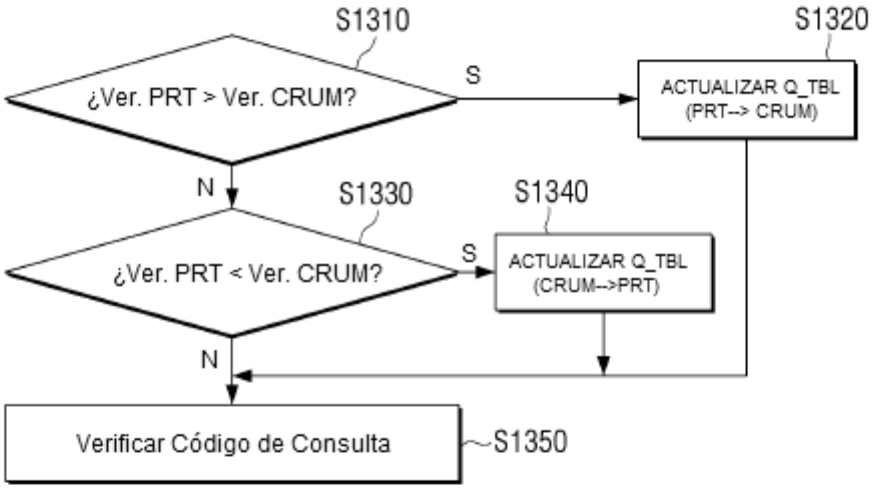
S1310
¿Ver. PRT > Ver. CRUM?
S
S1320
ACTUALIZAR Q_TBL
(PRT--> CRUM)
N
S1330
¿Ver. PRT < Ver. CRUM?
S
S1340
ACTUALIZAR Q_TBL
(CRUM-->PRT)
N
Verificar Código de Consulta
S1350

FIG. 14

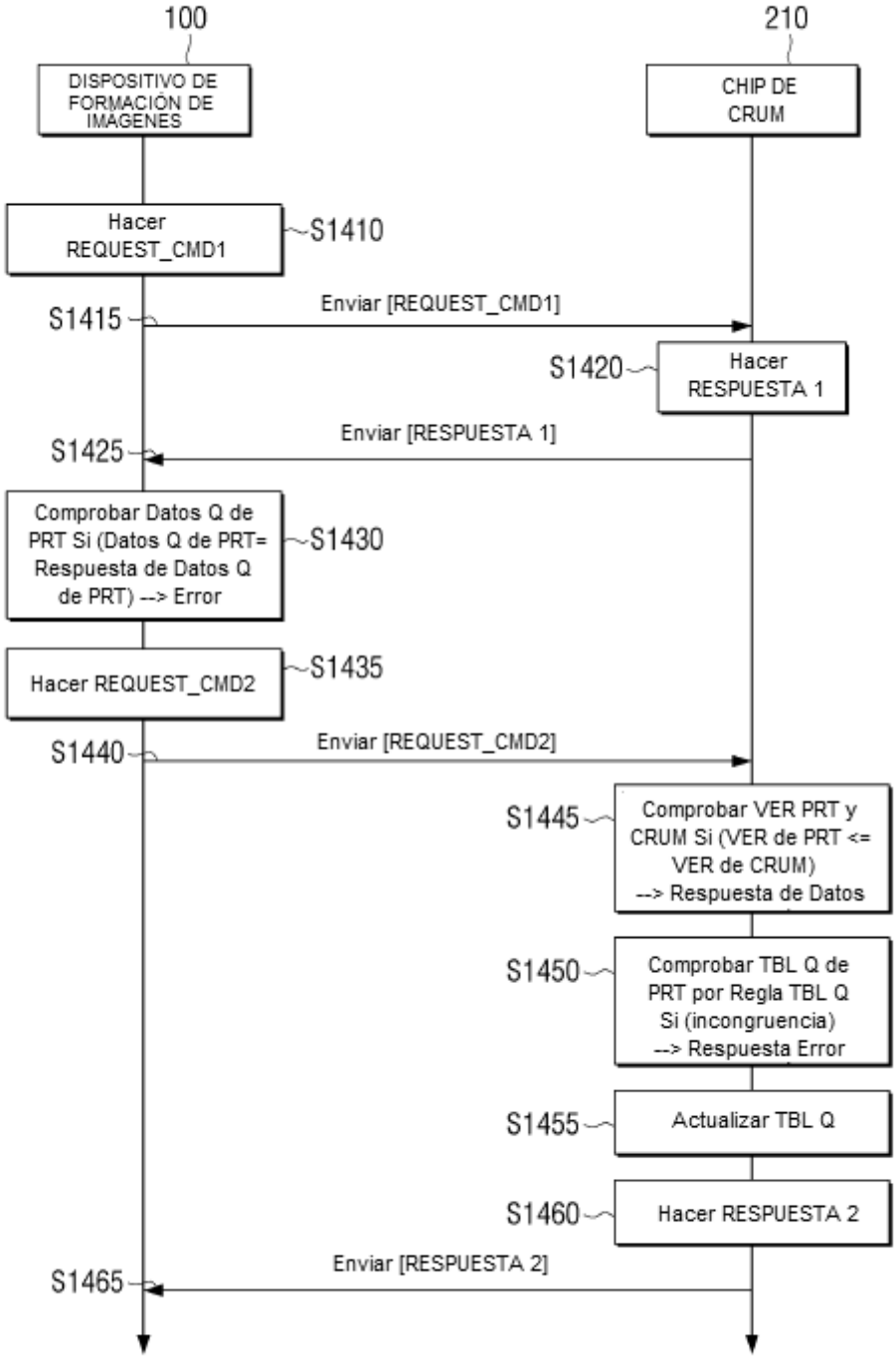
100
210
DISPOSITIVO DE FORMACIÓN DE IMÁGENES
CHIP DE CRUM
Hacer REQUEST_CMD1
S1410
S1415
Enviar [REQUEST_CMD1]
S1420
Hacer RESPUESTA 1
Enviar [RESPUESTA 1]
S1425
Comprobar Datos Q de PRT Si (Datos Q de PRT= Respuesta de Datos Q de PRT) --> Error
S1430
Hacer REQUEST_CMD2
S1435
S1440
Enviar [REQUEST_CMD2]
S1445
Comprobar VER PRT y CRUM Si (VER de PRT <= VER de CRUM) --> Respuesta de Datos
S1450
Comprobar TBL Q de PRT por Regla TBL Q Si (incongruencia) --> Respuesta Error
S1455
Actualizar TBL Q
S1460
Hacer RESPUESTA 2
Enviar [RESPUESTA 2]
S1465

FIG. 15

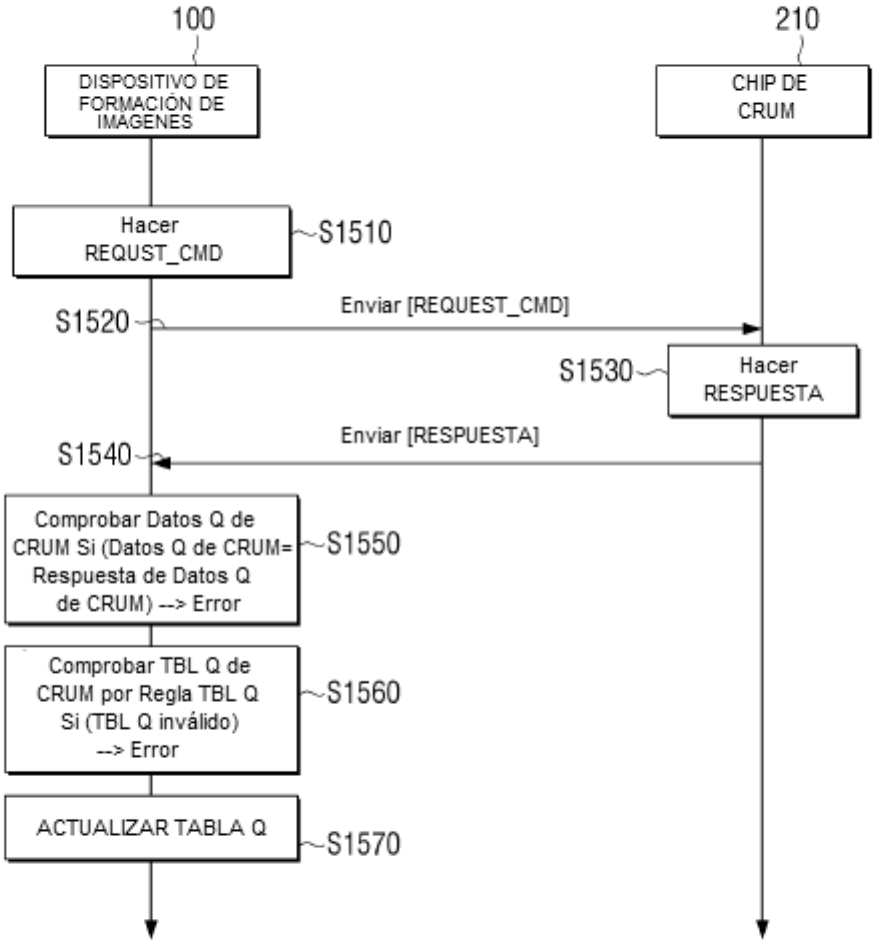
100
210
DISPOSITIVO DE FORMACIÓN DE IMÁGENES
CHIP DE CRUM
Hacer REQUST_CMD
S1510
S1520
Enviar [REQUEST_CMD]
S1530
Hacer RESPUESTA
Enviar [RESPUESTA]
S1540
Comprobar Datos Q de CRUM Si (Datos Q de CRUM= Respuesta de Datos Q de CRUM) --> Error
S1550
Comprobar TBL Q de CRUM por Regla TBL Q Si (TBL Q inválido) --> Error
S1560
ACTUALIZAR TABLA Q
S1570

FIG. 16

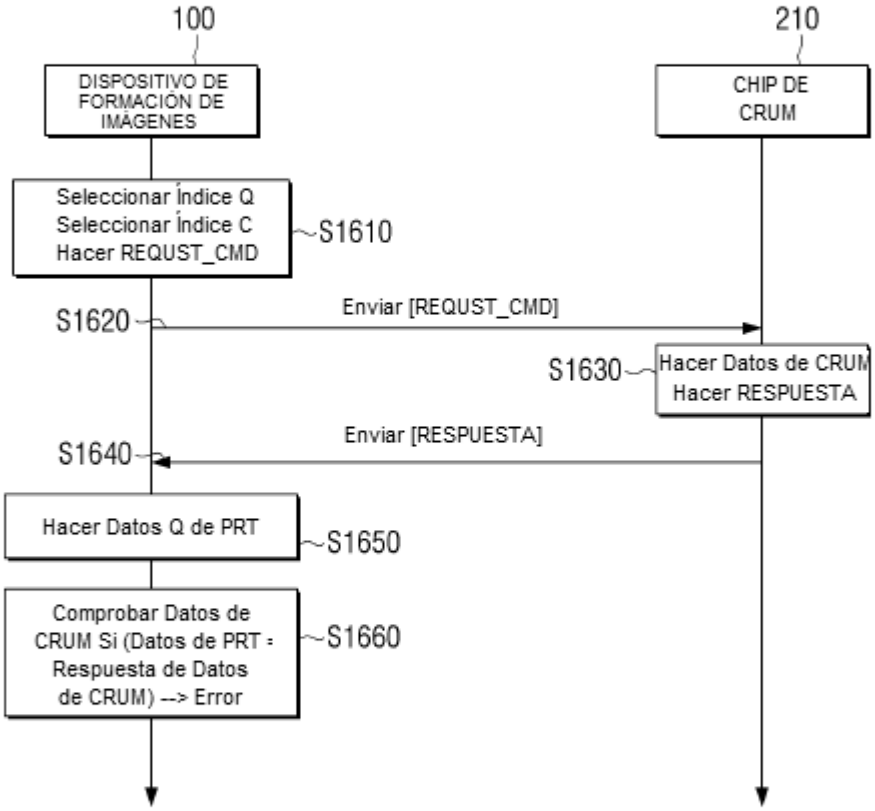
100
210
DISPOSITIVO DE FORMACIÓN DE IMÁGENES
CHIP DE CRUM
Seleccionar Índice Q
Seleccionar Índice C
Hacer REQUST_CMD
S1610
S1620
Enviar [REQUST_CMD]
S1630
Hacer Datos de CRUM
Hacer RESPUESTA
Enviar [RESPUESTA]
S1640
Hacer Datos Q de PRT
S1650
Comprobar Datos de CRUM Si (Datos de PRT = Respuesta de Datos de CRUM) --> Error
S1660

FIG. 17

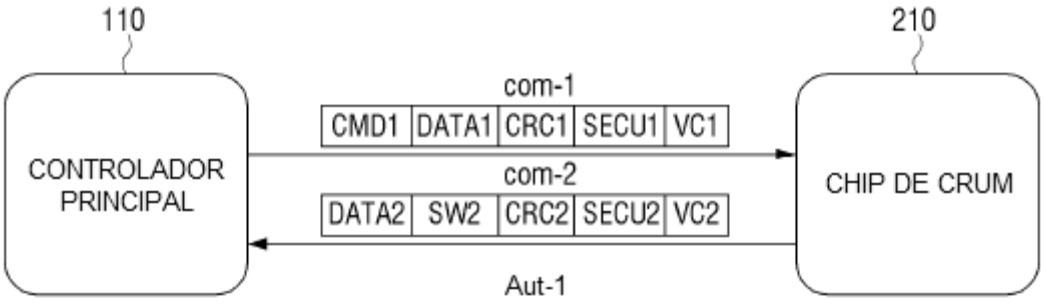
110
210
com-1
CMD1 DATA1 CRC1 SECU1 VC1
CONTROLADOR PRINCIPAL
com-2
DATA2 SW2 CRC2 SECU2 VC2
CHIP DE CRUM
Aut-1

FIG. 18

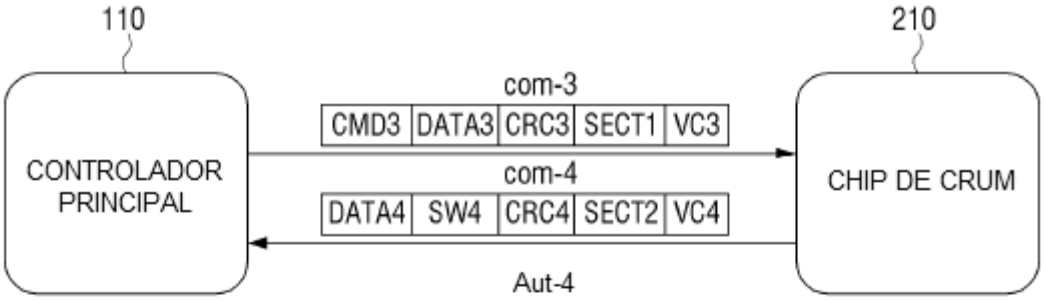
110
210
com-3
CMD3
DATA3
CRC3
SECT1
VC3
CONTROLADOR PRINCIPAL
com-4
CHIP DE CRUM
DATA4
SW4
CRC4
SECT2
VC4
Aut-4

FIG. 19

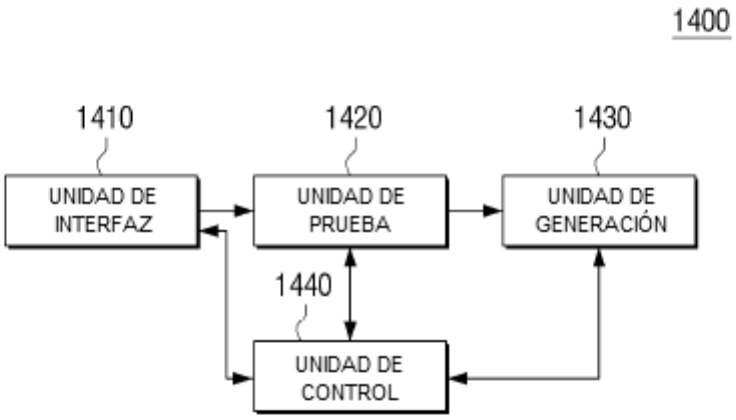
1400
1410
1420
1430
UNIDAD DE INTERFAZ
UNIDAD DE PRUEBA
UNIDAD DE GENERACIÓN
1440
UNIDAD DE CONTROL

FIG. 20

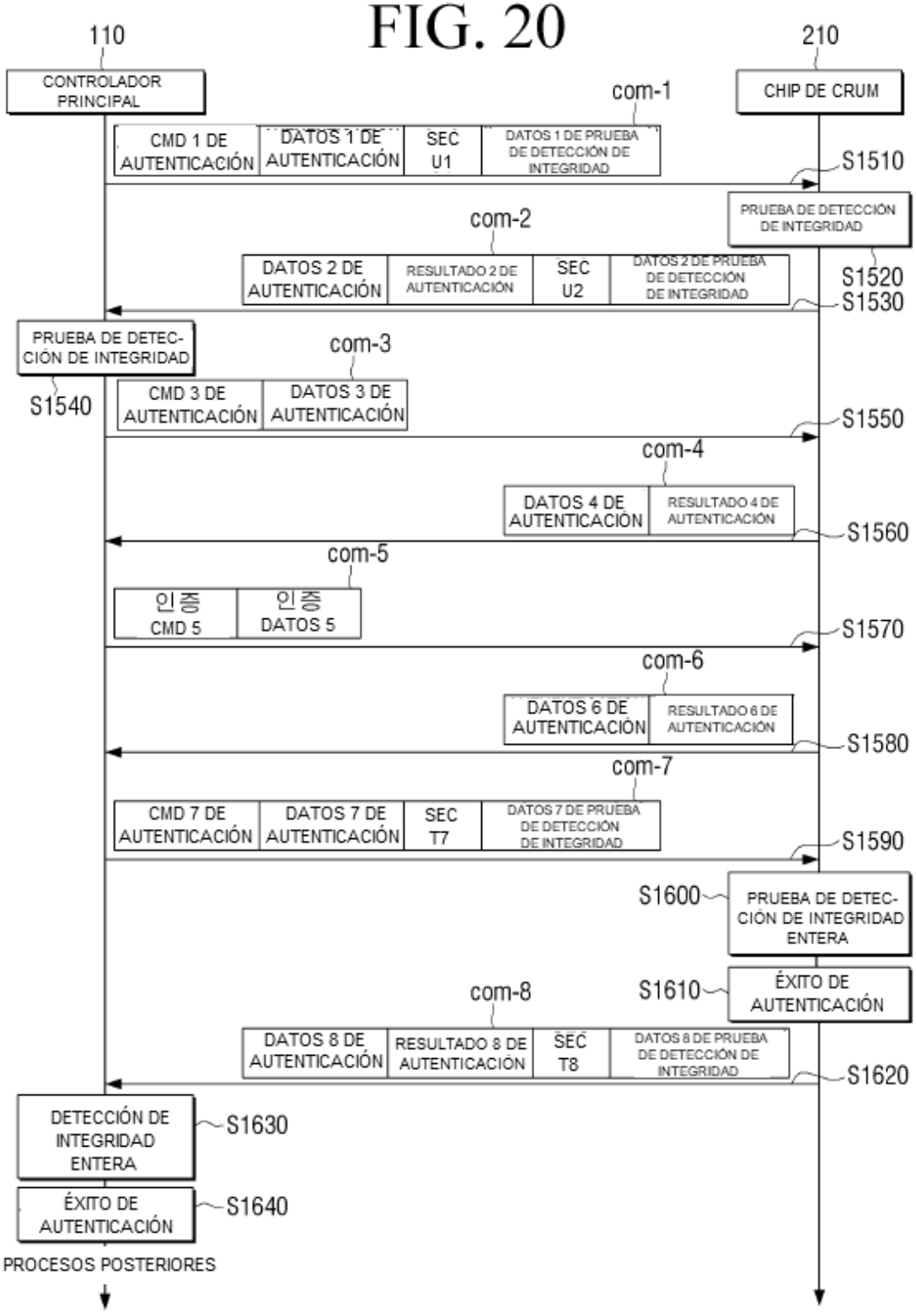
110
CONTROLADOR PRINCIPAL
210
CHIP DE CRUM
com-1
CMD 1 DE AUTENTICACIÓN
DATOS 1 DE AUTENTICACIÓN
SEC U1
DATOS 1 DE PRUEBA DE DETECCIÓN DE INTEGRIDAD
S1510
PRUEBA DE DETECCIÓN DE INTEGRIDAD
S1520
com-2
DATOS 2 DE AUTENTICACIÓN
RESULTADO 2 DE AUTENTICACIÓN
SEC U2
DATOS 2 DE PRUEBA DE DETECCIÓN DE INTEGRIDAD
S1530
PRUEBA DE DETEC-CIÓN DE INTEGRIDAD
S1540
com-3
CMD 3 DE AUTENTICACIÓN
DATOS 3 DE AUTENTICACIÓN
S1550
com-4
DATOS 4 DE AUTENTICACIÓN
RESULTADO 4 DE AUTENTICACIÓN
S1560
com-5
인증 CMD 5
인증 DATOS 5
S1570
com-6
DATOS 6 DE AUTENTICACIÓN
RESULTADO 6 DE AUTENTICACIÓN
S1580
com-7
CMD 7 DE AUTENTICACIÓN
DATOS 7 DE AUTENTICACIÓN
SEC T7
DATOS 7 DE PRUEBA DE DETECCIÓN DE INTEGRIDAD
S1590
S1600
PRUEBA DE DETEC-CIÓN DE INTEGRIDAD ENTERA
S1610
ÉXITO DE AUTENTICACIÓN
com-8
DATOS 8 DE AUTENTICACIÓN
RESULTADO 8 DE AUTENTICACIÓN
SEC T8
DATOS 8 DE PRUEBA DE DETECCIÓN DE INTEGRIDAD
S1620
DETECCIÓN DE INTEGRIDAD ENTERA
S1630
ÉXITO DE AUTENTICACIÓN
S1640
PROCESOS POSTERIORES

FIG. 21

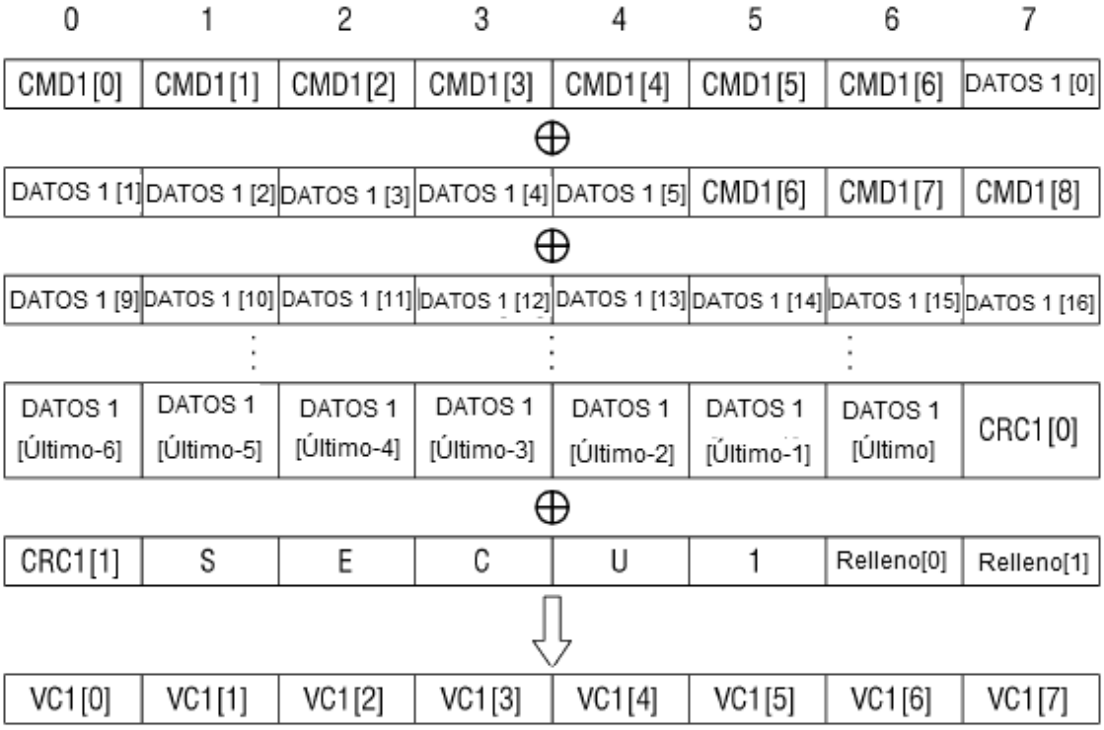
0 1 2 3 4 5 6 7
CMD1[0] CMD1[1] CMD1[2] CMD1[3] CMD1[4] CMD1[5] CMD1[6] DATOS 1 [0]
⊕
DATOS 1 [1] DATOS 1 [2] DATOS 1 [3] DATOS 1 [4] DATOS 1 [5] CMD1[6] CMD1[7] CMD1[8]
⊕
DATOS 1 [9] DATOS 1 [10] DATOS 1 [11] DATOS 1 [12] DATOS 1 [13] DATOS 1 [14] DATOS 1 [15] DATOS 1 [16]
DATOS 1 [Último-6] DATOS 1 [Último-5] DATOS 1 [Último-4] DATOS 1 [Último-3] DATOS 1 [Último-2] DATOS 1 [Último-1] DATOS 1 [Último] CRC1[0]
⊕
CRC1[1] S E C U 1 Relleno[0] Relleno[1]
VC1[0] VC1[1] VC1[2] VC1[3] VC1[4] VC1[5] VC1[6] VC1[7]

FIG. 22

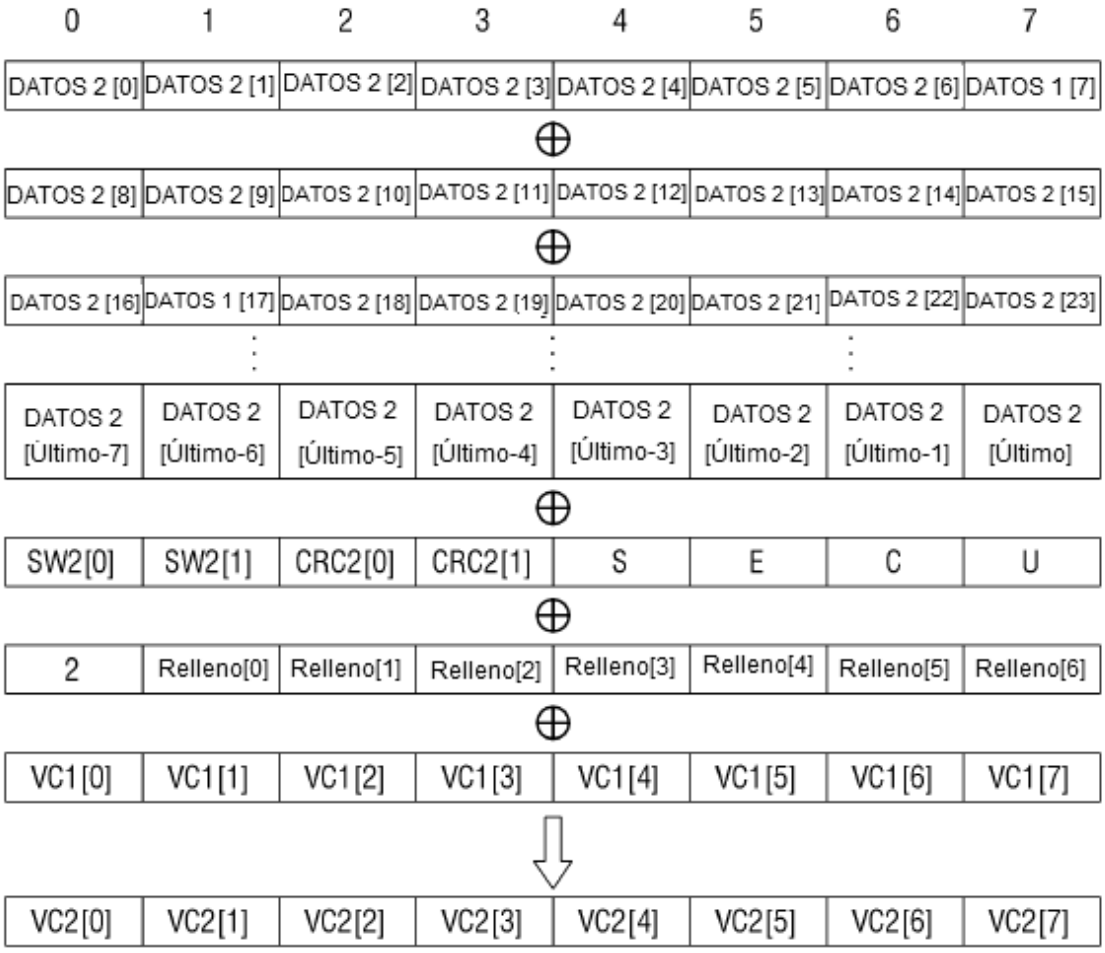
0 1 2 3 4 5 6 7
DATOS 2 [0] DATOS 2 [1] DATOS 2 [2] DATOS 2 [3] DATOS 2 [4] DATOS 2 [5] DATOS 2 [6] DATOS 1 [7]
DATOS 2 [8] DATOS 2 [9] DATOS 2 [10] DATOS 2 [11] DATOS 2 [12] DATOS 2 [13] DATOS 2 [14] DATOS 2 [15]
DATOS 2 [16] DATOS 1 [17] DATOS 2 [18] DATOS 2 [19] DATOS 2 [20] DATOS 2 [21] DATOS 2 [22] DATOS 2 [23]
DATOS 2 [Último-7] DATOS 2 [Último-6] DATOS 2 [Último-5] DATOS 2 [Último-4] DATOS 2 [Último-3] DATOS 2 [Último-2] DATOS 2 [Último-1] DATOS 2 [Último]
SW2[0] SW2[1] CRC2[0] CRC2[1] S E C U
2 Relleno[0] Relleno[1] Relleno[2] Relleno[3] Relleno[4] Relleno[5] Relleno[6]
VC1[0] VC1[1] VC1[2] VC1[3] VC1[4] VC1[5] VC1[6] VC1[7]
VC2[0] VC2[1] VC2[2] VC2[3] VC2[4] VC2[5] VC2[6] VC2[7]

FIG. 23

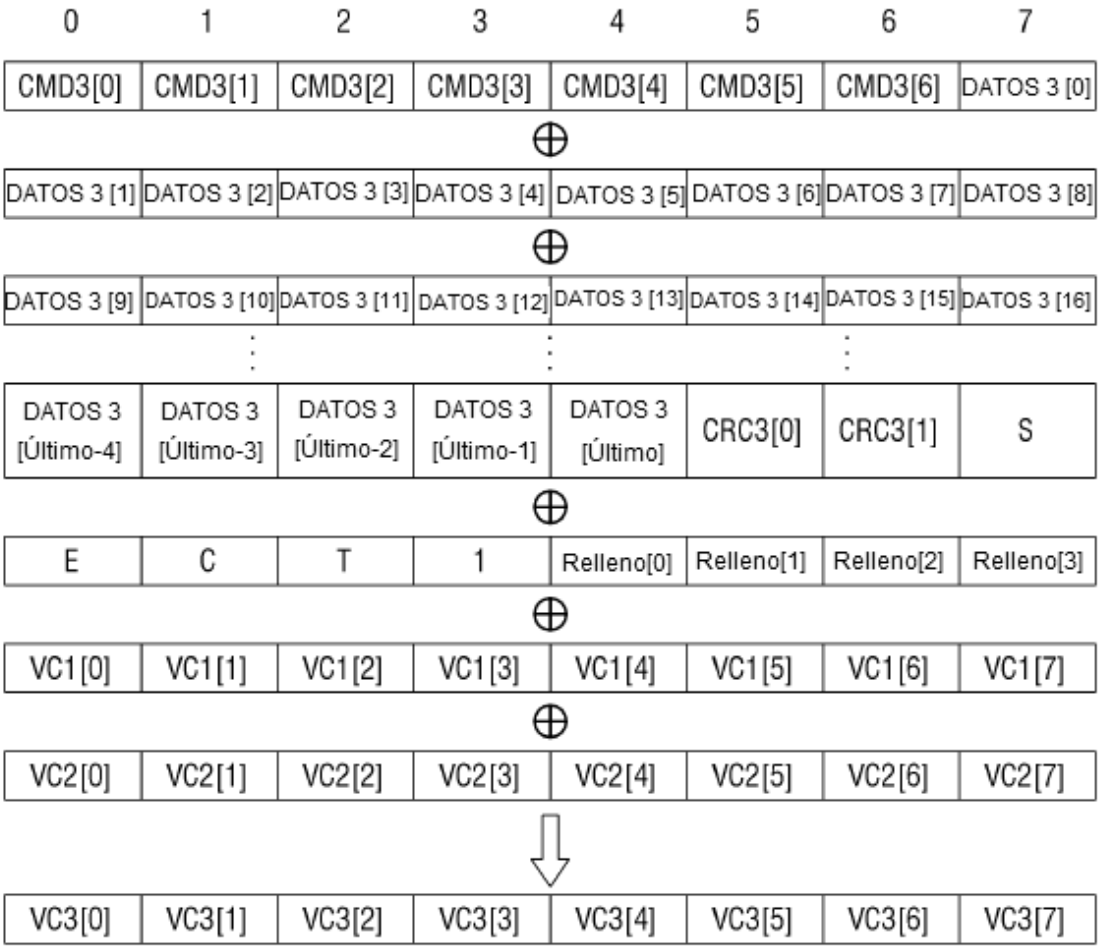
0 1 2 3 4 5 6 7
CMD3[0] CMD3[1] CMD3[2] CMD3[3] CMD3[4] CMD3[5] CMD3[6] DATOS 3 [0]
DATOS 3 [1] DATOS 3 [2] DATOS 3 [3] DATOS 3 [4] DATOS 3 [5] DATOS 3 [6] DATOS 3 [7] DATOS 3 [8]
DATOS 3 [9] DATOS 3 [10] DATOS 3 [11] DATOS 3 [12] DATOS 3 [13] DATOS 3 [14] DATOS 3 [15] DATOS 3 [16]
DATOS 3 [Último-4] DATOS 3 [Último-3] DATOS 3 [Último-2] DATOS 3 [Último-1] DATOS 3 [Último] CRC3[0] CRC3[1] S
E C T 1 Relleno[0] Relleno[1] Relleno[2] Relleno[3]
VC1[0] VC1[1] VC1[2] VC1[3] VC1[4] VC1[5] VC1[6] VC1[7]
VC2[0] VC2[1] VC2[2] VC2[3] VC2[4] VC2[5] VC2[6] VC2[7]
VC3[0] VC3[1] VC3[2] VC3[3] VC3[4] VC3[5] VC3[6] VC3[7]

FIG. 24

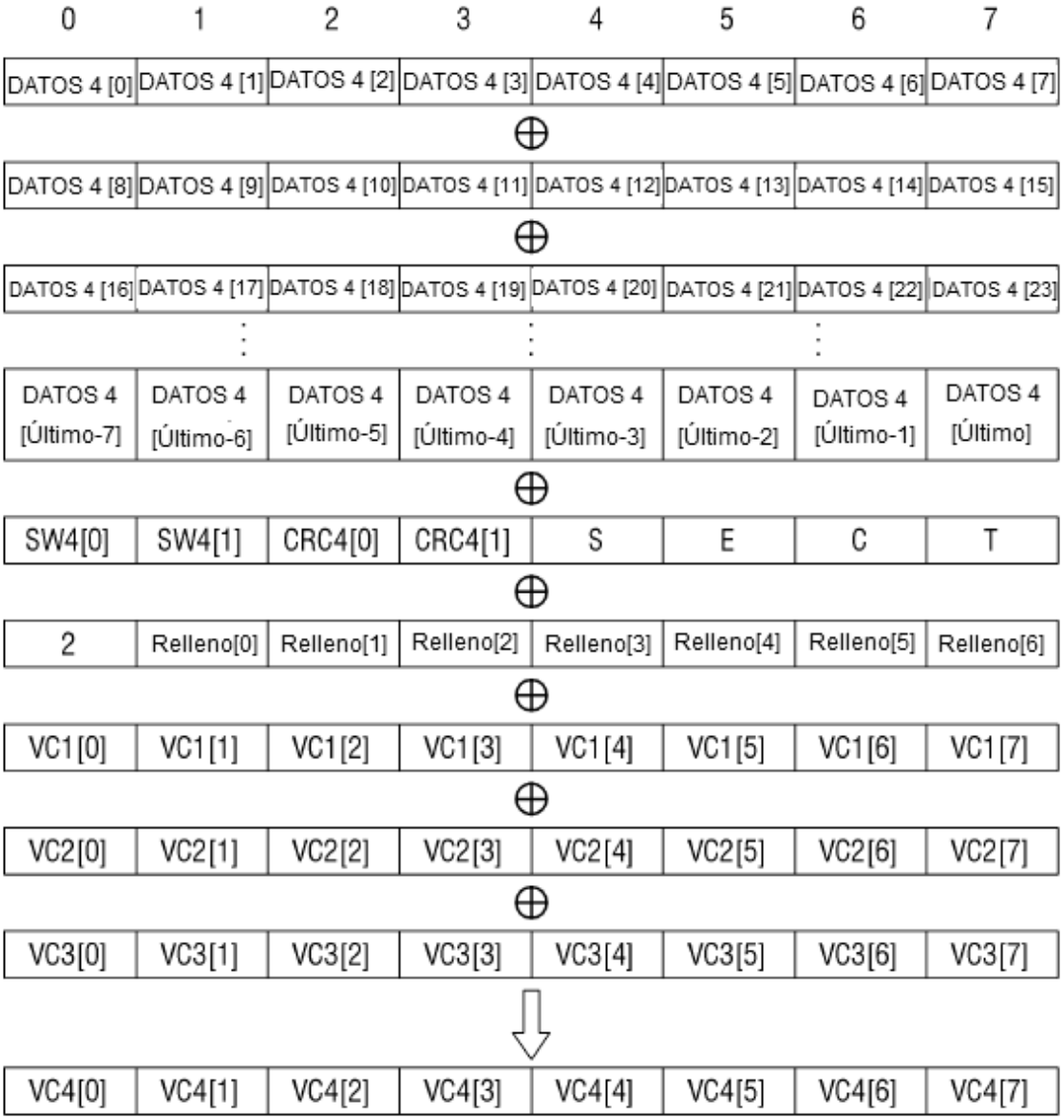
0 1 2 3 4 5 6 7
DATOS 4 [0] DATOS 4 [1] DATOS 4 [2] DATOS 4 [3] DATOS 4 [4] DATOS 4 [5] DATOS 4 [6] DATOS 4 [7]
DATOS 4 [8] DATOS 4 [9] DATOS 4 [10] DATOS 4 [11] DATOS 4 [12] DATOS 4 [13] DATOS 4 [14] DATOS 4 [15]
DATOS 4 [16] DATOS 4 [17] DATOS 4 [18] DATOS 4 [19] DATOS 4 [20] DATOS 4 [21] DATOS 4 [22] DATOS 4 [23]
DATOS 4 [Último-7] DATOS 4 [Último-6] DATOS 4 [Último-5] DATOS 4 [Último-4] DATOS 4 [Último-3] DATOS 4 [Último-2] DATOS 4 [Último-1] DATOS 4 [Último]
SW4[0] SW4[1] CRC4[0] CRC4[1] S E C T
2 Relleno[0] Relleno[1] Relleno[2] Relleno[3] Relleno[4] Relleno[5] Relleno[6]
VC1[0] VC1[1] VC1[2] VC1[3] VC1[4] VC1[5] VC1[6] VC1[7]
VC2[0] VC2[1] VC2[2] VC2[3] VC2[4] VC2[5] VC2[6] VC2[7]
VC3[0] VC3[1] VC3[2] VC3[3] VC3[4] VC3[5] VC3[6] VC3[7]
VC4[0] VC4[1] VC4[2] VC4[3] VC4[4] VC4[5] VC4[6] VC4[7]

FIG. 25

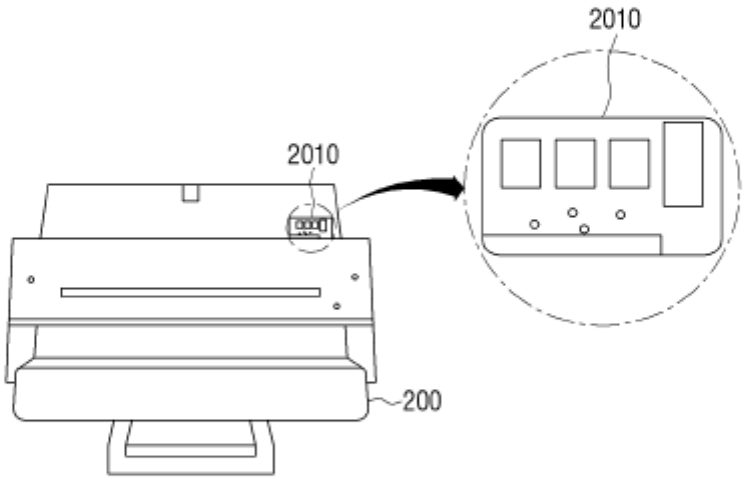

FIG. 26

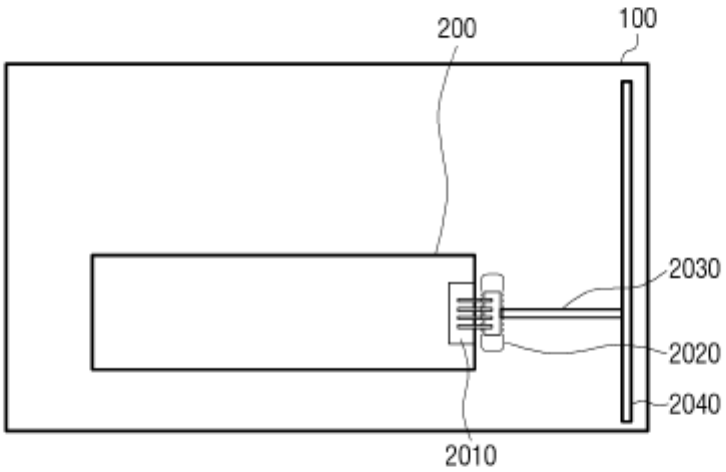

FIG. 27

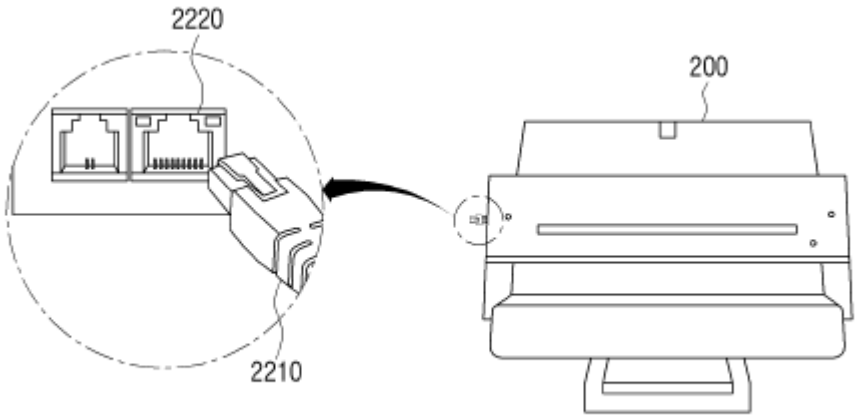

FIG. 28

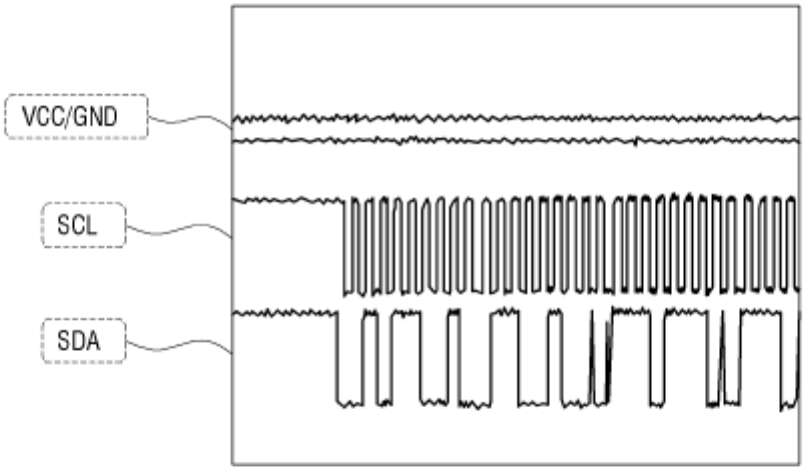

FIG. 29