(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 623 434**

(51) Int. CI.:

G06F 21/62 (2013.01)
G06F 21/83 (2013.01)
G06F 21/84 (2013.01)

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(86) Fecha de presentación y número de la solicitud internacional: **11.12.2007 PCT/IL2007/001535**

(87) Fecha y número de publicación internacional: **19.06.2008 WO08072234**

(96) Fecha de presentación y número de la solicitud europea: **11.12.2007 E 07849562 (9)**

(97) Fecha y número de publicación de la concesión europea: **08.02.2017 EP 2119075**

(54) Título: **Interfaces habilitadas con cifrado y descifrado**

(30) Prioridad:

12.12.2006 IL 18002006

(45) Fecha de publicación y mención en BOPI de la traducción de la patente:
11.07.2017

(73) Titular/es:

WATERFALL SECURITY SOLUTIONS LTD. (100.0%)
21 Hamelacha Street
48091 Rosh HaAyin, IL

(72) Inventor/es:

FRENKEL, LIOR y
ZILBERSTEIN, AMIR

(74) Agente/Representante:

DE ELZABURU MÁRQUEZ, Alberto

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

DESCRIPCIÓN

Interfaces habilitadas con cifrado y descifrado

Campo de la invención

La presente invención se refiere generalmente a descifrado de datos, y específicamente a métodos y dispositivos para impedir que partes no autorizadas accedan a datos descifrados.

Antecedentes de la invención

El cifrado de datos se usa ampliamente para impedir acceso no autorizado a datos. Se conocen en la técnica diversos métodos de cifrado de datos. En general, estos métodos usan una clave para convertir los datos a una forma que es ininteligible para un lector (humano o máquina), y requieren una clave adecuada con el fin de descifrar los datos. Los métodos de cifrado simétricos usan la misma clave tanto para el cifrado como para el descifrado. Tales métodos simétricos incluyen el DES (Estándar de Cifrado de Datos) bien conocido y los algoritmos AES (Estándar de Cifrado Avanzado). En métodos de cifrado asimétricos, tales como el algoritmo RSA (Rivest Shamir Adelman), un ordenador que va a recibir datos cifrados genera claves públicas y privadas complementarias y transmite la clave pública al remitente. Después de que el remitente ha cifrado los datos usando la clave pública, solamente el poseedor de la clave privada puede descifrarlos.

El documento US-A-5.825.879 describe un procesador de contenido de vídeo seguro (“SVCP”) que recibió información de vídeo digital cifrada y la convierte en información analógica para un monitor mientras que impide acceso no autorizado a los datos digitales no cifrados intermedios. El SVCP usa sobres hardware para impedir acceso no autorizado al flujo digital descifrado.

El documento US-A-5.822.435 describe un método y aparato para garantizar una comunicación segura sobre un medio de comunicaciones no garantizado entre un usuario que trabaja en una estación de trabajo u ordenador no garantizado y un ordenador anfitrión. Se crea una interfaz de usuario segura insertando un subsistema de camino de confianza entre los dispositivos de entrada/salida a la estación de trabajo y la estación de trabajo en sí misma. Los datos transferidos desde los dispositivos de entrada/salida se interceptan, cifran y transmiten en paquetes al ordenador central. Los paquetes de datos de visualización de pantalla desde el ordenador anfitrión se descifran y presentan dentro de una superposición de pantalla definida por el usuario.

El documento US-A-2003/0005295 describe un método para recibir datos de vídeo cifrados en un controlador de gráficos desde un microprocesador. Los datos se descifran en el controlador de gráficos y se representan.

Según un primer aspecto de la presente invención, se proporciona un sistema, que comprende: una interfaz de comunicación; un aparato de descifrado que tiene una memoria de entrada y un procesador de descifrado; una unidad central de procesamiento (CPU), que está acoplada para recibir datos cifrados desde la interfaz de comunicación y para escribir los datos cifrados en la memoria de entrada; y un transductor de salida, para presentar los datos descifrados a un usuario; en donde el procesador de descifrado está acoplado para leer y descifrar los datos cifrados de la memoria de entrada y está acoplado para transportar los datos descifrados al transductor de salida para presentación al usuario; caracterizado por que la CPU es incapaz de acceder a la salida del procesador de descifrado; y por que el procesador de descifrado está configurado físicamente en hardware para no tener salida de escritura a la memoria de entrada.

Según un segundo aspecto de la presente invención, se proporciona un método para descifrado, implementado en un sistema como se expuso anteriormente, que comprende:

recibir datos cifrados desde la interfaz de comunicación por la unidad central de procesamiento (CPU); almacenar los datos cifrados recibidos en la memoria de entrada; leer y descifrar los datos cifrados de la memoria de entrada usando el procesador de descifrado; y transmitir los datos descifrados desde el procesador de descifrado al transductor de salida para presentación a un usuario.

Compendio de la invención

Los métodos modernos de cifrado hacen muy difícil para una parte maliciosa que intercepta un mensaje cifrado descifrar los contenidos del mensaje. Por otra parte, una vez que un ordenador que recibe el mensaje lo ha descifrado usando la clave y método adecuados, los contenidos del mensaje se mantienen típicamente en forma clara (no cifrada) en el ordenador de recepción, al menos temporalmente. Si una parte maliciosa puede obtener acceso a la memoria (RAM o disco) del ordenador de recepción (usando un “caballo Troyano” u otro programa “espía”, por ejemplo), la parte maliciosa será capaz de leer los contenidos del mensaje. De esta manera, el propio ordenador de recepción resulta el enlace débil en la cadena de seguridad sobre la que se transportan los mensajes cifrados. Un problema similar puede ocurrir con datos que se introducen al ordenador en forma clara desde un dispositivo de entrada, antes de que el ordenador haya cifrado los datos.

Las realizaciones de la presente invención proporcionan métodos y un aparato para cifrado y descifrado que se pueden usar para impedir que partes no autorizadas accedan a datos descifrados en el ordenador de recepción. En algunas realizaciones, un procesador de descifrado lee y descifra datos cifrados desde una memoria de entrada que recibe los datos cifrados, pero el procesador de descifrado es incapaz de escribir en la memoria de entrada. Más bien, el procesador de descifrado está acoplado para transportar los datos descifrados únicamente a un transductor de salida, tal como un visualizador de vídeo, impresora, o altavoz de audio, para presentación al usuario. Por lo tanto, los datos descifrados nunca se mantienen en el ordenador de recepción en una memoria a la que se podría acceder por partes no autorizadas, y no hay ningún enlace disponible sobre el que se podría hacer al procesador de descifrado transmitir los datos descifrados fuera del ordenador distinto de directamente al transductor de salida.

Se proporciona, por lo tanto, según una realización de la presente invención, un aparato de descifrado, que incluye:

una memoria de entrada, que está acoplada para recibir datos cifrados;

un transductor de salida, para presentar datos descifrados a un usuario; y

un procesador de descifrado, que está acoplado para leer y descifrar los datos cifrados desde la memoria de entrada, pero es incapaz de escribir en la memoria de entrada, y que está acoplado para transportar los datos descifrados al transductor de salida para presentación al usuario

en donde el procesador de descifrado tiene una salida que está acoplada al transductor de salida, y el aparato incluye una unidad central de procesamiento (CPU) y una interfaz de comunicación, en donde la CPU se acopla para recibir los datos cifrados desde la interfaz de comunicación y para escribir los datos cifrados en la memoria de entrada, y en donde la CPU es incapaz de acceder a la salida del procesador de descifrado.

En una realización, el aparato incluye una memoria de salida, que está acoplada para recibir los datos descifrados desde el procesador de descifrado y para emitir los datos descifrados al transductor de salida, en donde la memoria de entrada está acoplada para recibir los datos cifrados desde una unidad central de procesamiento (CPU) de un ordenador, y en donde la memoria de salida es inaccesible para la CPU.

En una realización, el transductor de salida incluye un visualizador de vídeo, y la CPU está dispuesta para definir una ventana en el visualizador de vídeo para presentación de los datos descifrados, y en donde el procesador de descifrado está dispuesto para escribir los datos descifrados en la ventana. Adicional o alternativamente, el procesador de descifrado está dispuesto para descifrar los datos cifrados usando una clave predeterminada, y la CPU es incapaz de acceder a la clave predeterminada.

El transductor de salida puede incluir un visualizador de vídeo, un altavoz de audio, o una impresora.

También se proporciona, según una realización de la presente invención, un método para descifrado, que incluye:

recibir datos cifrados en una memoria de entrada;

leer y descifrar los datos cifrados desde la memoria de entrada usando un procesador de descifrado, que es incapaz de escribir en la memoria de entrada; y

transportar los datos descifrados desde el procesador de descifrado a un transductor de salida para presentación a un usuario caracterizado por que los datos cifrados se reciben desde una interfaz de comunicación por una unidad central de procesamiento (CPU), que escribe los datos cifrados en la memoria de entrada, pero es incapaz de acceder a la salida del procesador de descifrado.

La presente invención se entenderá más completamente a partir de la siguiente descripción de las realizaciones de la misma, tomadas junto con los dibujos en los que:

Breve descripción de los dibujos

La Fig. 1 es una ilustración esquemática, gráfica de un sistema de transmisión, recepción y procesamiento de datos cifrados, según una realización de la presente invención;

La Fig. 2 es un diagrama de bloques que muestra esquemáticamente elementos de un terminal para cifrar y descifrar datos, según una realización de la presente invención; y

La Fig. 3 es un diagrama de flujo que ilustra esquemáticamente un método para descifrar y mostrar datos cifrados, según una realización de la presente invención.

Descripción detallada de realizaciones

La Fig. 1 es una ilustración esquemática, gráfica de un sistema para transmisión, recepción y descifrado de datos cifrados, según con una realización de la presente invención. Un ordenador 24 de origen transmite datos cifrados sobre una red 22 a un terminal 20 de recepción. Los datos se pueden cifrar según cualquier método adecuado de

cifrado que sea conocido en la técnica, incluyendo métodos tanto simétricos como asimétricos. La red 22 puede comprender Internet o sustancialmente cualquier otra red informática pública o privada.

El terminal 20 comprende una consola 26 de ordenador, que está acoplada a uno o más transductores de salida para convertir los datos en la consola a una forma en la que un usuario humano pueda recibir y comprender el contenido de los datos. Ejemplos de transductores de salida que se muestran en la Fig. 1 incluyen una pantalla 28 de visualización de video, altavoces 30 de audio y una impresora 32. En la descripción que sigue, se usa la pantalla 28 de visualización como el transductor de destino con propósitos de descifrado seguro de datos cifrados recibidos por el terminal 20. Alternativamente, los altavoces de audio o la impresora se pueden usar para este propósito, en la medida en que lo pueden ser transductores de salida de otros tipos (no mostrados en las figuras).

Típicamente, el terminal 20 también comprende uno o más dispositivos de entrada de usuario, que pueden comprender transductores de entrada de texto, de captura de imágenes y/o entrada de audio. Típicamente, el transductor de entrada de texto comprende un teclado 34. Alternativa o adicionalmente, los dispositivos de entrada de usuario pueden comprender una cámara 36, o un micrófono 38, o una pantalla táctil, un escáner u otros tipos de dispositivos de entrada conocidos en la técnica (no mostrados en las figuras). En la descripción que sigue, se describen, a modo de ejemplo, ciertas técnicas para la entrada segura de datos cifrados a la consola 26, con referencia al teclado 34. Estas técnicas se pueden aplicar de manera similar, cambiando lo que se deba de cambiar, a dispositivos de entrada de otros tipos.

La Fig. 2 es un diagrama de bloques que muestra esquemáticamente detalles de la consola 26, según una realización de la presente invención. La consola 26 puede ser un ordenador de propósito general con un adaptador 46 de visualizador especializado, que realiza funciones seguras de descifrado de datos. Alternativamente, las funciones de descifrado del adaptador 46 se pueden realizar por un circuito de descifrado que está integrado en la electrónica de la pantalla 28 (o integrado de manera similar en la electrónica de otro tipo de transductor de salida), en lugar de dentro de la consola del ordenador. Adicional o alternativamente, el teclado 34 está adaptado, como se describe a continuación, para realizar cifrado de datos seguro. Alternativamente, además, el terminal 20 puede comprender uno o más dispositivos dedicados, de propósito especial, que implementan los principios de descifrado y/o cifrado seguro que se describen en la presente memoria. Aunque por el bien de la integridad, las funciones tanto de descifrado seguro como de cifrado seguro se ilustran en la Fig. 2, el terminal 20 se puede configurar alternativamente con capacidades solamente de descifrado seguro o solamente de cifrado seguro.

La consola 26 comprende una unidad central de procesamiento (CPU) 40, que realiza funciones informáticas generales. La CPU 40 se acopla a través de una interfaz 42 de comunicación para transmitir y recibir datos hacia y desde la red 22. La consola comprende una memoria 44 (que típicamente puede comprender tanto RAM como memoria de disco), a la que se accede por la CPU de una manera convencional. Típicamente, al recibir una transmisión de datos cifrados, la CPU 40 escribe los datos cifrados en la memoria 44. En escenarios convencionales, la clave requerida para descifrar los datos también se puede mantener en la memoria. La CPU descifraría entonces los datos usando esta clave, y luego emitiría los datos descifrados al usuario automáticamente o bajo petición. En el transcurso de un proceso tal, la CPU típicamente escribe los datos descifrados en la memoria 44. Como resultado, si una parte maliciosa es capaz de obtener acceso a la memoria a través de una violación de seguridad de software, por ejemplo, esa parte puede ser capaz de leer los datos descifrados (generalmente haciendo que la CPU 40 u otro componente del terminal 20 transmita los datos descifrados sobre la red 22), a pesar de la resistencia del cifrado que se usó en la transmisión de los datos sobre la red.

Para evitar este tipo de escenario en la presente realización, la CPU 40 no descifra los datos cifrados transmitidos por el ordenador 24 de origen. En su lugar, la CPU escribe los datos cifrados en una memoria 48 de adaptador del adaptador 46 de visualizador. La memoria 48 sirve como la memoria de entrada con propósitos de descifrado. Un procesador 50 de descifrado en el adaptador de visualizador entonces decodifica los datos cifrados usando la clave adecuada y las instrucciones de programa almacenadas en una memoria 52 de programa. El procesador de descifrado puede comprender un dispositivo de procesamiento programable, tal como un microprocesador o una agrupación de puertas programables en campo (FPGA), o puede comprender alternativamente un dispositivo lógico codificado de forma permanente. (En este último caso, la memoria 52 puede ser innecesaria, o esta memoria se puede usar solamente para contener la clave de descifrado y/u otros datos de operación básicos).

El procesador 50 escribe los datos descifrados en una memoria 54 de pantalla, típicamente en forma o bien de un mapa de bits o bien de caracteres y/o vectores para representación en la pantalla 28. La memoria de pantalla sirve de esta manera como la memoria de salida para el proceso de descifrado. Un circuito 56 de controlador de pantalla activa la pantalla 28 para mostrar los contenidos de la memoria 54. Alternativamente, el procesador 50 de descifrado puede alimentar el circuito de controlador de pantalla directamente, o las funciones del procesador de descifrado y el controlador de pantalla se pueden integrar en un único circuito integrado.

Como se ilustra por las direcciones de las flechas en el adaptador 46, el procesador 50 de descifrado está acoplado a la memoria 48 de adaptador en una configuración de sólo lectura, es decir, el procesador es capaz de leer desde el adaptador, pero no de volver a escribir en el adaptador. Esta configuración se puede implementar físicamente en hardware conectando la salida de escritura del procesador 50 a la memoria 54 de pantalla, pero no a la memoria 48 de adaptador. De manera similar, la memoria de pantalla se puede configurar de manera que el procesador 50

pueda sobrescribir los contenidos de memoria, pero los contenidos de la memoria solamente se puedan leer por el circuito 56 de controlador de pantalla. Como resultado, incluso si una parte no autorizada tiene éxito en obtener acceso, a través de una violación de software, a la CPU 40 y a las memorias 44 y 48, será físicamente imposible para esta parte acceder a los datos descifrados generados por el procesador 50. Alternativamente, el procesador de descifrado 50 se puede configurar en software para deshabilitar el acceso de escritura a la memoria 48 (y a otros elementos fuera del adaptador 46), pero si es así, es deseable que el software sea almacenado de una forma que impida que partes no autorizadas accedan a él y lo cambien.

El adaptador 46 se puede configurar como una tarjeta conectable, que ocupa el lugar de un adaptador de visualizador convencional en la consola 26. En este caso, el terminal 20 puede ser un ordenador personal estándar, que es mejorado para descifrado de datos seguro mediante la instalación del adaptador 46. Alternativamente, algunas o todas las funciones del adaptador 46 se pueden integrar en la placa madre de la consola 26. Alternativamente, además, como se señaló anteriormente, las funciones de descifrado seguro del adaptador 46 se pueden integrar en la electrónica de la pantalla 28 de visualización, en forma de componentes de hardware y/o software embebido adecuados. En esta última realización, la consola 26 emite datos cifrados a la pantalla 28, y la circuitería en la pantalla descifra y muestra los datos. Aunque los elementos del adaptador 46 se muestran en la Fig. 2, por el bien de la claridad, como bloques funcionales separados, en la práctica algunos o todos estos bloques funcionales se pueden combinar en o más chips de circuitos integrados.

Como se señaló anteriormente, aunque las funciones de descifrado seguro de esta realización se implementan en conjunto con la pantalla 28 de visualización, tales funciones se pueden integrar de manera similar con otros tipos de transductores de salida. Por ejemplo, una tarjeta de sonido con capacidades de descifrado se puede acoplar para activar los altavoces 30 para reproducir mensajes descifrados, o una interfaz de impresora con capacidades de descifrado puede activar la impresora 32 para imprimir texto y/o gráficos descifrados. Como en el caso de la pantalla 28, las capacidades de descifrado seguro en estos ejemplos se pueden incorporar en la consola 26 o en los altavoces o la impresora.

La Fig. 3 es un diagrama de flujo que ilustra esquemáticamente un método para descifrar y mostrar datos cifrados, según una realización de la presente invención. El método se describe, por el bien de la claridad, con referencia a la configuración de hardware mostrada en la Fig. 2, pero también se puede llevar a cabo de manera similar, cambiando lo que se deba de cambiar, en otras configuraciones, tales como las mencionadas anteriormente. En la realización de la Fig. 3, se supone que el terminal 20 funciona como un ordenador personal, que ejecuta un sistema operativo basado en ventanas y lleva a cabo otros tipos de aplicaciones de ordenador, además de la función de descifrado seguro del adaptador 46 de visualizador. Por lo tanto, el adaptador de visualizador es capaz de mostrar tanto los datos descifrados como otros datos de aplicación no seguros en la misma pantalla simultáneamente. (El procesador 50 de descifrado se puede puentear u operar en un modo de paso para mostrar los datos no seguros). Alternativamente, el método se puede simplificar, como será evidente para los expertos en la técnica, si el adaptador 46 se limita a mostrar los datos descifrados en modo de pantalla completa.

Para iniciar el descifrado, la CPU 40 abre una ventana en la pantalla 28 en la que van a ser mostrados los datos descifrados, en un paso 60 de definición de ventana. Típicamente, la CPU abre la ventana de descifrado en respuesta a una orden del usuario del terminal 20 cuando el usuario desea leer un mensaje cifrado u otros datos cifrados. Alternativamente, la CPU puede abrir la ventana automáticamente al recibir los datos cifrados desde el ordenador 24 de origen.

La CPU entonces escribe los datos cifrados que van a ser descifrados y mostrados en la ventana en la memoria 48 de adaptador, en un paso 62 de entrada de datos. Junto con los datos, la CPU envía una cabecera u otras instrucciones al procesador 50 indicando que los datos deberían ser descifrados (y posiblemente incluyendo parámetros de descifrado, tales como un identificador de clave), y definiendo la ventana en la que deberían ser mostrados los datos descifrados. El procesador 50 de descifrado lee las instrucciones, descifra los datos, y escribe los datos descifrados en el intervalo de direcciones adecuado en la memoria 54 de pantalla, en un paso 64 de descifrado. Como se señaló anteriormente, los datos descifrados pueden tener la forma de caracteres alfanuméricos, un mapa de bits, o vectores gráficos, dependiendo del tipo de datos implicados y de las capacidades de representación del controlador 56 de pantalla. El controlador de pantalla lee los datos descifrados desde la memoria 54, y muestra el contenido descifrado en la ventana adecuada en la pantalla 28, en un paso 66 de visualización.

El método descrito anteriormente es adecuado para mostrar un único bloque de datos (caracteres y/o gráficos) de un tamaño predeterminado. Después de ver un bloque, el usuario puede sugerir a la CPU 40 que vuelva al paso 62 y alimentar el siguiente bloque de datos cifrados al adaptador 46. Alternativamente, para aplicaciones interactivas, la CPU 40 puede cargar un archivo de datos en la memoria 48 del adaptador, y el decodificador 50 se puede configurar para recibir varias entradas de usuario de modo que el usuario pueda navegar a través del archivo y cambiar los parámetros de visualización mientras que ve los contenidos del archivo en la pantalla 28. Por ejemplo, el procesador de descifrado se puede programar para soportar una interfaz de tipo navegador en Web en la ventana asignada para la visualización de datos descifrados. En este caso, la CPU 40 puede pasar objetos gráficos y de texto cifrados, junto con instrucciones de lenguaje de marcas (que pueden o no estar cifradas) al adaptador 46, que entonces muestra

los gráficos descifrados y el texto en la interfaz del navegador. El procesador de descifrado se puede programar de manera similar para soportar interfaces de aplicaciones de otros tipos.

Aunque la descripción anterior se refiere a usos de realizaciones de la presente invención para impedir acceso no autorizado a datos descifrados, la arquitectura y los métodos asociados con estas realizaciones también pueden ser útiles en la mejora de la eficiencia y fiabilidad de diversos procesos de cifrado y descifrado, como será evidente para los expertos en la técnica. Se apreciará, de esta manera, que las realizaciones descritas anteriormente se citan a modo de ejemplo, y que la presente invención no está limitada a lo que se ha mostrado y descrito particularmente en lo que antecede.

REIVINDICACIONES

1. Un sistema que comprende:

una interfaz (42) de comunicación;

un aparato (46) de descifrado que tiene una memoria (48) de entrada y un procesador (50) de descifrado;

una unidad central de procesamiento (CPU) (40), que está acoplada para recibir datos cifrados desde la interfaz (42) de comunicación y para escribir los datos cifrados en la memoria (48) de entrada; y

un transductor (28) de salida, para presentar datos descifrados a un usuario;

en donde el procesador (50) de descifrado está acoplado para leer y descifrar los datos cifrados desde la memoria (48) de entrada y está acoplado para transmitir los datos descifrados al transductor (28) de salida para presentación al usuario;

caracterizado por que la CPU (40) es incapaz de acceder a la salida del procesador (50) de descifrado; y

por que el procesador (50) de descifrado está configurado físicamente en hardware para no tener salida de escritura a la memoria (48) de entrada.

2. El aparato según la reivindicación 1, y que comprende una memoria (54) de salida, que está acoplada para recibir los datos descifrados desde el procesador de descifrado y para emitir los datos descifrados al transductor de salida.

3. El aparato según la reivindicación 2, en donde la memoria de salida es inaccesible para la CPU.

4. El aparato según la reivindicación 1, en donde el transductor de salida comprende un visualizador de vídeo, y en donde la CPU está dispuesta para definir una ventana en el visualizador de vídeo para presentación de los datos descifrados, y en donde el procesador de descifrado está dispuesto para escribir los datos descifrados en la ventana.

5. El aparato según la reivindicación 1, en donde el procesador de descifrado está dispuesto para descifrar los datos cifrados usando una clave predeterminada, y en donde la CPU es incapaz de acceder a la clave predeterminada.

6. El aparato según cualquiera de las reivindicaciones 1-5, en donde el transductor de salida se selecciona de un grupo de dispositivos que consiste en un visualizador de vídeo, un altavoz de audio, y una impresora.

7. Un método para descifrado, implementado en un sistema según cualquiera de las reivindicaciones 1 a 6, que comprende:

recibir datos cifrados desde la interfaz (42) de comunicación por la unidad central de procesamiento (CPU) (40);

almacenar los datos cifrados recibidos en la memoria (48) de entrada;

leer y descifrar los datos cifrados de la memoria (48) de entrada usando el procesador (50) de descifrado; y

transmitir los datos descifrados desde el procesador (50) de descifrado al transductor (28) de salida para presentación a un usuario.

FIG. 1

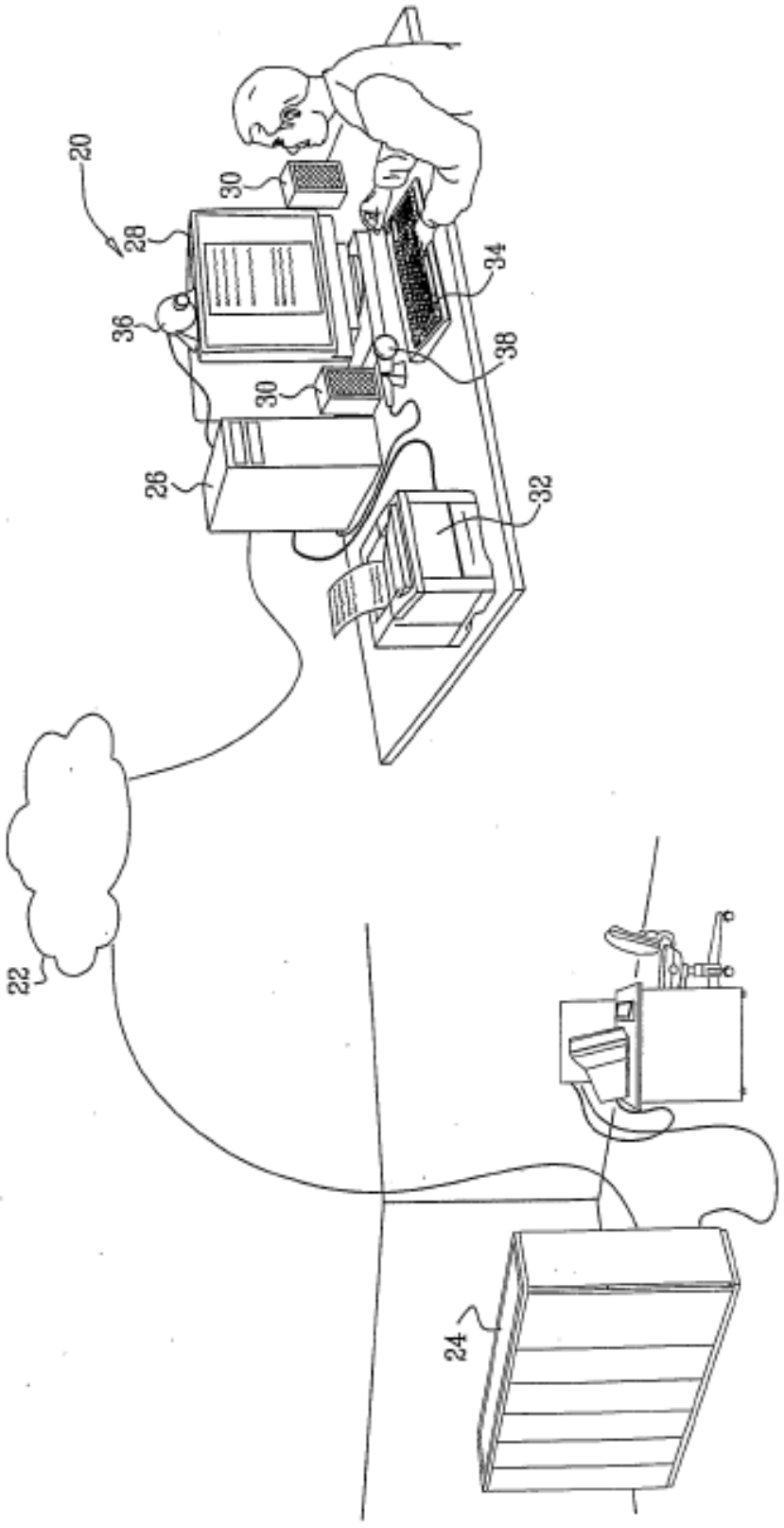


FIG. 2

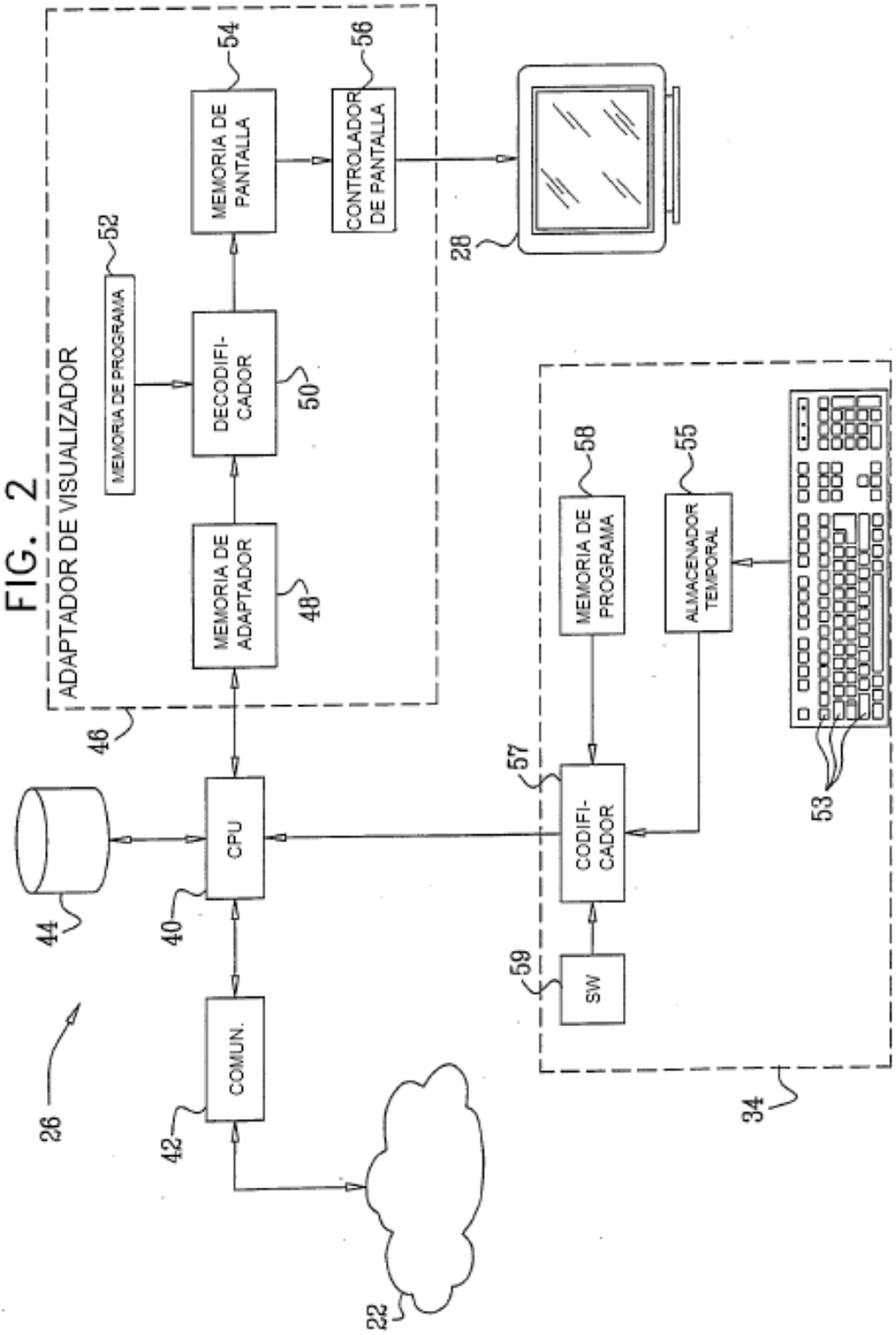
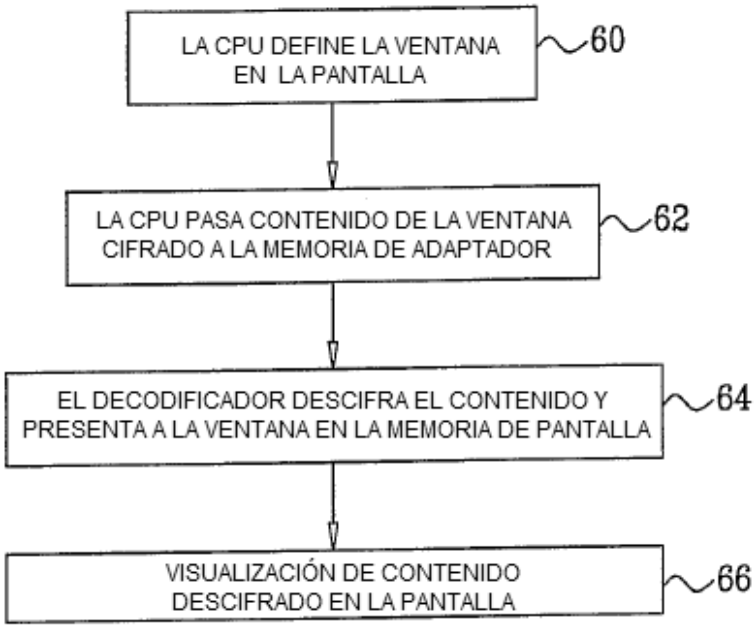

ADAPTADOR DE VISUALIZADOR
MEMORIA DE PROGRAMA
52
DECODIFI-CADOR
50
MEMORIA DE ADAPTADOR
48
MEMORIA DE PANTALLA
54
CONTROLADOR DE PANTALLA
56
28
46
CPU
40
44
COMUN.
42
26
22
MEMORIA DE PROGRAMA
58
ALMACENADOR TEMPORAL
55
CODIFI-CADOR
57
SW
59
53
34

FIG. 3


LA CPU DEFINE LA VENTANA EN LA PANTALLA
60
LA CPU PASA CONTENIDO DE LA VENTANA CIFRADO A LA MEMORIA DE ADAPTADOR
62
EL DECODIFICADOR DESCIFRA EL CONTENIDO Y PRESENTA A LA VENTANA EN LA MEMORIA DE PANTALLA
64
VISUALIZACIÓN DE CONTENIDO DESCIFRADO EN LA PANTALLA
66