(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 555 262**

(51) Int. CI.:

H04N 5/913 (2006.01)
G11B 20/00 (2006.01)
H04N 7/16 (2011.01)
H04N 7/173 (2011.01)
H04N 7/24 (2011.01)
H04L 9/32 (2006.01)

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(96) Fecha de presentación y número de la solicitud europea: **24.06.2011 E 11727198 (1)**

(97) Fecha y número de publicación de la concesión europea: **30.09.2015 EP 2594064**

(54) Título: **Sistema y método para evitar la manipulación de datos de vídeo transmitidos**

(30) Prioridad:

07.10.2010 EP 10186869
16.07.2010 US 364834 P

(45) Fecha de publicación y mención en BOPI de la traducción de la patente:
30.12.2015

(73) Titular/es:

NAGRAVISION S.A. (100.0%)
Route de Genève 22-24
1033 Cheseaux-sur-Lausanne, CH

(72) Inventor/es:

KUDELSKI, ANDRÉ y
NICOLAS, CHRISTOPHE

(74) Agente/Representante:

TOMAS GIL, Tesifonte Enrique

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

Sistema y método para evitar la manipulación de datos de vídeo transmitidos

Introducción

[0001] La presente invención se refiere al campo de los dispositivos de televisión, en particular descodificadores (o Receptores Decodificadores Integrados, IRD) diseñados para proporcionar experiencias de medios adicionales en la televisión.

Estado de la técnica

[0002] La situación de hoy se describe con respecto a la figura 1.
El IRD se conecta a varias fuentes de datos (IP, satélite, cable, antena) y está encargado de extender las capacidades de la televisión al proporcionar una desencriptación de los datos encriptados así como al gestionar los derechos de acceso.
El IRD propone también capacidades de almacenamiento, control parental con identificación del usuario para aplicar el perfil apropiado y una guía de programación.
La salida se conecta a una televisión o a una pantalla para aprovechar la experiencia multimedia.

[0003] Un modelo de ingresos de los proveedores de contenido multimedia es la publicidad introducida durante la emisión de contenido atractivo.
Es por lo tanto importante que los anuncion enviados por el IRD a la televisión no se sustituyan por otras informaciones.

[0004] El documento DE 10 2008 003364 divulga un método para detectar manipulaciones en datos multimedia, tales como vídeo.
Este método pretende determinar si una imagen ha sido manipulada, por comparación de su huella digital con la de la imagen original.
Con este fin, una imagen entera que se ha de controlar se divide en varios bloques cada uno del mismo tamaño, para formar una matriz.
Para cada bloque, se determina un valor de color (o valor de nivel gris).
Un valor medio se determina teniendo en cuenta todos los valores de los bloques de la imagen.
Una huella digital de esta imagen se determina por comparación sucesiva del valor de cada bloque con el valor medio.
Como resultado, la huella digital finalmente corresponde a una sucesión de n bits (0 o 1 dependiendo del resultado de la comparación), donde n es el número de bloques de la imagen.
Además, este método está configurado para distinguir modificaciones menores de manipulaciones intencionales.

[0005] El documento US 2007/277041 divulga un dispositivo y un método para detectar manipulaciones dentro de la señal de información.
Esta señal de información comprende dos componentes, que son información secundaria e información principal que están entrelazadas.
El dispositivo sugerido en este documento comprende un extractor para extraer información secundaria, y un medio de encriptación para el encriptado del componente extraído para obtener una señal encriptada.
El dispositivo comprende además un comparador para la comparación de la señal encriptada con una señal de referencia.
Esta señal de referencia es una representación encriptada de un componente de señal de referencia no manipulado, usado para detectar cualquier manipulación.

[0006] El documento US 6,370,209 divulga un proceso para detectar manipulaciones de información digital tales como la secuencia de imágenes de vídeo transmitidas de una cámara de supervisión a un centro de supervisión.
Para prevenir una clasificación errónea, como "información manipulada", cuando los trastornos ocurren durante el procesamiento, se sugiere dividir la información en subunidades de información de cada una de las cuales se deriva una identificación individual.
Estas identificaciones individuales se corresponden con firmas, y estas firmas se suplementan con una consignación de hora y una consignación de ubicación.
Cada subunidad se clasifica bien como válida o bien como potencialmente manipulada.
La información digital se clasifica como manipulada si se ha determinado que al menos dos subunidades que están correlacionadas respecto al tiempo o ubicación han sido potencialmente manipuladas.

[0007] El documento WO 2006/059053 se refiere a un método para toma de huella digital de un vídeo que implica la identificación de movimiento en el vídeo y utiliza una medida del movimiento identificado como huella digital.

Una vez que se ha tomado la huella digital de los vídeos, estas huellas digitales se pueden usar en un método para la identificación de vídeos.
Esto implica la creación de una huella digital de movimiento para vídeos desconocidos; la comparación de las huellas digitales de los vídeos conocidos y desconocidos, y la identificación de si el vídeo desconocido es una copia del vídeo conocido basado en el paso de comparación.

Breve descripción de la invención

[0008] El objetivo de la invención es proporcionar una solución para asegurar que el contenido enviado por el IRD es el contenido visualizado efectivamente en la la pantalla.

[0009] Se propone luego un sistema para prevenir la manipulación de datos de vídeo transmitidos que comprende un receptor descodificador integrado (IRD) que recibe datos de audio/vídeo, un dispositivo de pantalla (TV), donde dicho IRD comprende medios para transmitir un flujo de datos audio/video que cumplen con HDMI al dispositivo de pantalla.
Las características que caracterizan el sistema inventivo se establecen en la reivindicación independiente 1.

Breve descripción de las figuras

[0010] La presente invención será mejor entendida gracias a las figuras adjuntas, donde:

La figura 1 ilustra el sistema conocido estándar.
La figura 2 muestra el ataque denominado "man-in-the-middle"
La figura 3 ilustra la invención que utiliza una llave para determinar la imagen visualizada real
La figura 4 es similar a la figura 3 con la diferencia de que los datos de retroinformación se envían de forma inalámbrica
La figura 5 ilustra la misma forma de realización que la figura 4 con una llave externa inalámbrica recibida en el lado del IRD.
La figura 6 ilustra la caja con un segundo canal de retroinformación HDMI
La figura 7 ilustra una caja cuando la firma se calcula por el dispositivo de pantalla
La figura 8 ilustra una caja cuando el canal posterior se utiliza para controlar el acceso al contenido

Descripción de las varias formas de realización

[0011] La figura 1 ilustra el sistema conocido estándar.
El IRD (receptor decodificador integrado) está por un lado conectado a los canales de emisión, por ejemplo a través de una antena, cable, o IP, y por otro lado conectado a un dispositivo de pantallade TV.
El propósito del IRD es recibir la señal, convertirla en varios canales y, si es necesario, desencriptar el canal seleccionado con la cooperación de un módulo de seguridad.
El canal seleccionado se transmite después a la TV a través de un cable HDMI.
Otras funciones son también propuestas por el IRD tales como grabar un evento, bien directamente mientras se emite, o de acuerdo con un tiempo/fecha programado/a.

[0012] El IRD es también encargado de la recepción, preparación y pantalla de la guía electrónica de programas (EPG) que ayuda al usuario a acceder rápidamente al canal deseado.

[0013] La comuniación HDMI está protegida por protocolo HDCP que define el marco del intercambio de datos.
HDCP se basa en la verificación de certificados y la encriptación de datos.
Antes de que los datos sean emitidos por un dispositivo fuente, se inicia un protocolo de enlace durante el que el certificado de la fuente y el sumidero se intercambian.
El certificado recibido (por ejemplo X509) es luego verificado y usado para establecer una clave de encriptación común.
La verificación puede usar listas blancas o negras.

[0014] La figura 2 muestra el ataque denominado "man-in-the-middle" en el que un dispositivo adicional MM se coloca en la salida del IRD e intercepta el flujo de datos de audio/video.
El riesgo en tal caso es de desviar las reglas de seguridad que estaban asociadas al contenido, tales como, "sólo ver, “ver una vez", "sin registro".
El hecho de que el contenido está en un dispositivo externo abre la posibilidad de que una tercera parte use el contenido de una forma no autorizada por el proveedor de contenido.
El objetivo de esta solicitud de patente es detectar la presencia de tal dispositivo externo e intermedio por el IRD y tomar las medidas apropiadas.

[0015] Para prevenir la manipulación de datos de vídeo transmitidos por tal dispositivo adicional MM, el sistema de la presente invención sugiere definir un área variable en el dispositivo de pantalla, y después memorizar datos de referencia que corresponden con estos datos de vídeo que se envían al dispositivo de pantalla.
Al otro lado del sistema, comprende medios para extraer los datos de vídeo visualizados contenidos en la misma área y medios para reenviar al IRD datos de prueba en referencia a los datos de vídeo extraídos.
Finalmente, el sistema comprende medios para comparar datos de prueba con datos de referencia y medios para tomar las medidas apropiadas en caso de diferencias resultantes de esta comparación.

[0016] El área variable definida en el dispositivo de pantalla corresponde a una parte de la pantalla que cambia cada vez que el sistema verifica si se han hecho manipulaciones en los datos de vídeo de referencia.
Al limitar el área que va a ser procesada por el sistema de la presente invención a una parte del dispositivo de pantalla, por ejemplo a un área de tamaño relativamente pequeño, los datos de referencia y los datos de prueba también son de tamaño pequeño y de manera ventajosa pueden ser transferidos rápidamente entre los dispositivos localizados en los dos extremos del sistema.
La receptividad del sistema también se mejora.

[0017] El área variable se puede definir por coordenadas dentro de un sistema de dos dimensiones.
Estas coordenadas se pueden enviar desde el IRD a medios encargados de extraer el área predefinida de los datos de vídeo visualizados reales de un mensaje encriptado.
Este mensaje se puede parametrizar mediante una clave de encriptación de propietario conocida sólo por los dos dispositivos de la comunicación, es decir el IRD y los medios de extracción.
Estos últimos son internos o externos al dispositivo de pantalla.

[0018] Para proceder con la comparación de los datos, el sistema también comprende medios para almacenar temporalmente datos de referencia que corresponden con datos de vídeo del área enviados al dispositivo de pantalla.
Estos datos se almacenan hasta que se lleva a cabo la comparación de datos de prueba con datos de referencia.

[0019] Según la forma de realización preferida de la invención, la ubicación del área variable definida en el dispositivo de pantalla se determina según un pseudo proceso aleatorio para que sea imprevisible.
Además, tal proceso puede ser un proceso de muestreo que verifica progresivamente las áreas posibles completas del dispositivo de pantalla, teniendo en cuenta las áreas que ya han sido controladas.

[0020] La figura 3 ilustra la invención que utiliza una llave como medio para determinar la imagen visualizada real.
Una llave dongle DG-SN se conecta al dispositivo de pantalla con el objetivo de recopilar información acerca de qué se está visualizando actualmente en el dispositivo.
Esto puede hacerse redirigiendo en salida la señal HDMI que entra en el dispositivo de pantalla hasta la llave.
Para tal fin, la llave se puede conectar a la salida HDMI del dispositivo de pantalla o a otra interfaz tal como CI+, por ejemplo en el caso de que la llave tenga la forma de una tarjeta CI+ y esté alimentada por una interfaz CI+ del dispositivo de pantalla.

[0021] Según un aspecto de la invención, el sistema comprende medios para calcular una firma de referencia en los datos de vídeo, limitados al área variable, que se envían al dispositivo de pantalla y una firma de prueba en los datos de vídeo extraídos en la misma área.
Preferiblemente, los datos de referencia, usados durante la comparación de datos, corresponden a esta firma de referencia y los datos de prueba, enviados de nuevo al IRD, corresponden a esta firma de prueba.

[0022] Típicamente, la llave puede comprender medios para extraer los datos de vídeo visualizados en el área variable y/o medios para calcular la firma en estos datos de vídeo extraídos; esta firma es comparada con una firma de referencia calculada por el IRD según la forma de realización preferida.
La comparación de ambas firmas se puede llevar a cabo en la llave dongle DG o por el IRD.
En el primer caso, la llave recibe la firma de referencia del IRD a través de otra conexión, tal como una conexión USB, y simplemente reenvía una señal para la comparación positiva o negativa al IRD.
En el segundo ejemplo, la llave transmite la firma de prueba de la imagen visualizada al IRD y este último lleva a cabo la comparación.

[0023] Cada firma se calcula en primer lugar usando una función hash aplicada a los datos de vídeo que deben ser firmados.
Un compendio se obtiene como resultado de esta función hash.
En segundo lugar, este compendio es luego encriptado por una función de encriptación.
El hash o compendio asegura la integridad de los datos de vídeo y su encriptación asegura la autentificación.
Así, los datos enviados al IRD son encriptados por la llave o por cualquier medio usado para calcular la firma en los

datos extraídos.
En el caso de que los datos de vídeo sean directamente enviados al IRD para el cálculo de la firma, estos datos de vídeo son en primer lugar encriptados por la llave o por cualquiera de los otros medios antes de ser enviados.

[0024] Alternativamente, los datos de vídeo comprendidos dentro del área variable y que se envían al dispositivo de pantalla pueden ser directamente usados como datos de referencia sin calcular una firma en estos datos.
De la misma manera, los datos de vídeo extraídos que se envían al IRD pueden ser directamente usados como datos de prueba.
No obstante, es más acertado utilizar la firma de los datos de vídeo enviados al dispositivo de pantalla como datos de referencia y usar la firma de los datos extraídos como datos de prueba.

[0025] La figura 4 ilustra una forma de realización similar a la de la figura 3.
La única diferencia es la conexión entre la llave dongle DG y el IRD, que es inalámbrica.
En este caso, el IRD no comprende ningún medio inalámbrico y por eso el IRD se conecta a un transmisor RC.
El transmisor RC se conecta por ejemplo con el IRD gracias a una conexión USB.

[0026] La figura 5 es similar a la figura 4 con una llave externa al dispositivo de pantalla e inalámbrica recibida en el lado IRD.

[0027] La figura 6 se basa en el mismo principio pero la llave anteriormente descrita se incluye en el IRD.
El dispositivo de pantalla de TV comprende una salida que da los datos actualmente visualizados, por ejemplo salida HDMI.
El IRD luego calcula la firma basadándose en los datos recibidos y la compara con la calculado en los datos de vídeo enviados por la salida HDMI del IRD.

[0028] La figura 7 sigue estando basada en la comparación de firma, donde el dispositivo de pantalla tiene un módulo de procesamiento que puede calcular la firma en la imagen visualizada.
Esta firma es luego enviada al IRD a través de varios medios, tales como USB, Bluetooth, wifi, corriente.
El IRD calcula la firma de referencia en la imagen enviada al dispositivo de pantalla y compara la firma recibida, es decir la firma de prueba, con la firma de referencia.

[0029] El sistema de la invención comprende medios para la conmutación del modo operativo del sistema de un modo estándar o normal a un modo interrumpido en caso de diferencia entre estas firmas.
Según la forma de realización preferida, el IRD comprende medios para interrumpir la transmisión de señal de vídeo en caso de diferencia.
No obstante, se debe entender que se podrían tomar otras medidas en caso de diferencias entre el par de firmas.

[0030] Otro aspecto que es común al precedente acerca de los datos de vídeo que se van a usar para la comparación, es la sincronización entre el módulo que procesa la imagen visualizada (por ejemplo por cálculo de la firma de prueba) y el módulo que procesa la imagen de referencia (por ejemplo por cálculo de la firma de referencia).
Esta sincronización tiene por objetivo determinar qué imagen, es decir qué dato de referencia y qué datos de prueba, servirá/n como base para el cálculo de las firmas, por ejemplo.
Para asegurar la comprensión, el módulo en el dispositivo de pantalla (o fijado al dispositivo de pantalla) será denominado "módulo de firma receptor" y el módulo equivalente en el IRD se denomina "módulod e firma receptor".
El IRD puede enviar un comando al módulo de firma receptor que acciona el cálculo de la firma.
Este comando puede comprender la indicación (por ejemplo, coordenadas) acerca del área sobre la que el cálculo debería ser realizado.
El comando enviado por el IRD al módulo de firma receptor puede también indicar un índice de imagen.
El dispositivo de pantalla muestra una sucesión de imágenes, cada una con un índice.
Cuando el índice apropiado se detecta, el módulo de firma receptor calcula la firma de prueba y manda ésta al IRD (o la compara localmente con la firma de referencia recibida del IRD).

[0031] Otro aspecto para asegurar la sincronización de las imágenes resultantes de datos de referencia y las imágenes resultantes de datos de prueba es el de calcular el retraso de transmisión necesitado por el sistema entre el momento en que los datos de vídeo que van a ser visualizados son enviados por el IRD y el momento en que estos datos son eficazmente visualizados en el dispositivo de pantalla.
Este retraso de transmisión puede ser diferente de un sistema a otro suponiendo que cada sistema no comprende necesariamente los mismos componentes/dispositivos.
Una solución para determinar este retraso de transmisión es enviar una señal emitida por el IRD, por ejemplo generando un marcador durante un periodo de tiempo breve, como marcador claro que puede ser detectado de una forma fiable por el módulo receptor o por un medio que está encargado de extraer los datos de vídeo, y calcular el tiempo transcurrido

entre la emisión y la recepción de esta señal.
Una vez determinado, el retraso de transmisión de los datos de vídeo del emisor al módulo receptor del sistema puede utilizarse para configurar el proceso de extracción y para asegurar que los datos de referencia se comparan con los datos de prueba apropiados.
Como el tiempo requerido hasta que una imagen es visualizada puede variar ligeramente, se puede asignar una tolerancia al retraso de transmisión.
Típicamente, tal tolerancia puede ser de alrededor de algunos milisegundos.
Si es necesario, el retraso de transmisión y/o la tolerancia se pueden enviar a los medios de extracción y/o al módulo receptor a través de un comando o un mensaje específico.
Todos estas operaciones podrían ser, por ejemplo, contenidas dentro de un proceso de calibración que podría ser implementado mediante un medio de calibración.
Según la forma de realización preferida, el medio para extraer los datos del vídeo visualizado real comprende medios para accionar la extracción de modo que los datos de vídeo extraídos se refieran a los datos de vídeo correspondientes enviados al dispositivo de pantalla.
Con este fin, los medios de accionamiento están configurados para tener en cuenta el retraso de transmisión anteriormente mencionado.

[0032] La figura 8 ilustra otro aspecto basado en la tecnología descrita en el documento WO 2004/073292.
Los datos de audio/vídeo que entran en el IRD son atraídos, es decir parte de los datos son extraídos y sustituidos por datos simulados.
El IRD crea así dos flujos, un flujo modificado y un objeto de control.
El flujo se envía de forma convencional al dispositivo de pantalla, por ejemplo mediante HDMI.
El objeto de control CO creado por el IRD contiene los datos extraídos durante esta fase de engaño.
El objeto de control CO se puede enviar a un módulo equivalente unido (o dentro de) el dispositivo de pantalla para la reconstrucción del flujo de audio/vídeo original.
Otra función del módulo de reconstrucción es controlar la consistencia del flujo reconstruido.
Este módulo, una vez que los datos originales se restablecen en la ubicación apropiada en el flujo modificado, pueden calcular una suma de control en el flujo original previsto (o información de verificación equivalente).
Esta verificación puede tomar varias formas, tal como la verificación del valor simulado que fue insertado en lugar del valor original en el flujo modificado.
Puede ser la verificación de otro valor en una ubicación indicada en el segundo flujo o un valor hash de un paquete de datos.
El resultado de la verificación es luego enviado al IRD que puede tomar las medidas necesarias en caso de diferencia.

REIVINDICACIONES

1. Sistema para prevenir la manipulación de datos de vídeo transmitidos que comprende un receptor decodificador integrado (IRD) que recibe datos de audio/vídeo, un dispositivo de pantalla (TV), donde dicho IRD comprende medios para transmitir un flujo de datos audio/video según HDMI hacia el dispositivo de pantalla, donde dicho sistema comprende además:

- medios para definir un área en una ubicación de la imagen visualizada en el dispositivo de pantalla,
- medios para memorizar datos de referencia que corresponden con datos de vídeo de dicha área que se envían al dispositivo de pantalla.
- medios internos o externos al dispositivo de pantalla para extraer los datos de vídeo visualizados reales de dicha área,
- medios para enviar, a dicho IRD, datos de prueba determinados a partir de dichos datos de vídeo extraídos,
- medios para comparar dichos datos de prueba con dichos datos de referencia,

caracterizado por el hecho de que comprende además medios para la conmutación de un modo operativo del sistema de un modo estándar a un modo interrumpido en caso de diferencia resultante de esta comparación, y por el hecho de que dicha área es un área variable y la ubicación de dicha área se determina según un pseudo proceso aleatorio, donde dicha ubicación se comunicada al dispositivo de pantalla.

2. Sistema según la reivindicación 1, donde éste comprende medios de accionamiento para accionar la extracción de los datos visualizados reales de modo que estos últimos se refieren a los datos de vídeo correspondientes transmitidos al dispositivo de pantalla, donde dichos medios de accionamiento tienen en cuenta un retraso de transmisión que corresponde al intervalo de tiempo entre el momento en que los datos de vídeo que deben ser visualizados son enviados por el IRD y el momento en que estos datos son visualizados a través del dispositivo de pantalla.

3. Sistema según la reivindicación 2, donde dicho retraso de transmisión lo determina un medio de calibración que es capaz de medir el intervalo de tiempo requerido por una señal de señalización entre un primer momento en que ésta es emitida por el IRD y un segundo momento en que ésta es recibida por el dispositivo de pantalla.

4. Sistema según cualquiera de las reivindicaciones 1 a 3, donde dicha ubicación se determina según un proceso de muestreo que verifica progresivamente las áreas posibles completas del dispositivo de pantalla.

5. Sistema según cualquiera de las reivindicaciones 1 a 4, donde comprende además medios para calcular:
una firma de referencia en los datos de vídeo de dicha área enviados al dispositivo de pantalla y
una firma de prueba de los datos de prueba y;
donde el paso de comparación se realiza con la firma de referencia y la firma de prueba.

6. Sistema según cualquiera de las reivindicaciones 1 a 3, donde dicho medio para extraer dichos datos de vídeo y/o dicho medio para enviar dichos datos de prueba son partes de una llave que comprende medios de conexión con el IRD para el envío de dichos datos de prueba.

7. Sistema según la reivindicación 6, donde el medio de conexión con el IRD es inalámbrico.

8. Sistema según la reivindicación 6 o 7, donde la llave se conecta a una salida HDMI del dispositivo de pantalla.

9. Sistema según cualquiera de las reivindicaciones 6 a 8, donde la llave comprende dicho medio para calcular dicha firma de prueba.

10. Sistema según cualquiera de las reivindicaciones 6 a 9, donde el IRD comprende dicho medio para comparar la firma de prueba con la firma de referencia.

11. Sistema según la reivindicación 1, donde dicho medio para la conmutación del modo operativo del sistema permite interrumpir la transmisión de señal de vIdeo en caso de diferencias en dicha comparación.

12. Sistema según cualquiera de las reivindicaciones 1 a 11, donde los datos de vídeo visualizados son una sucesión de imágenes, y el medio para extraer la información visualizada recibe una señal de activación del IRD, donde dicha señal indica qué imagen debe ser extraída para el cálculo de la firma de prueba.

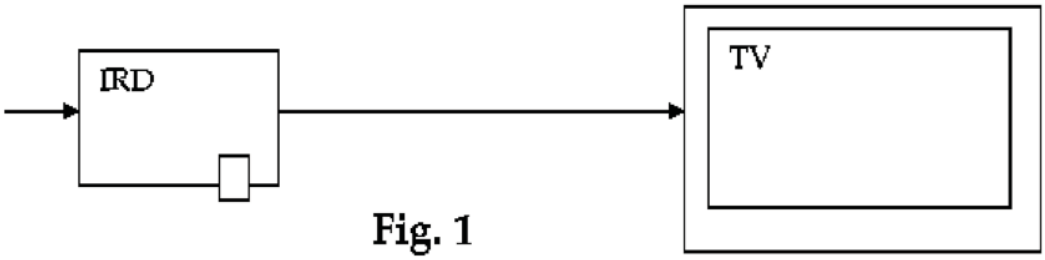

Fig. 1

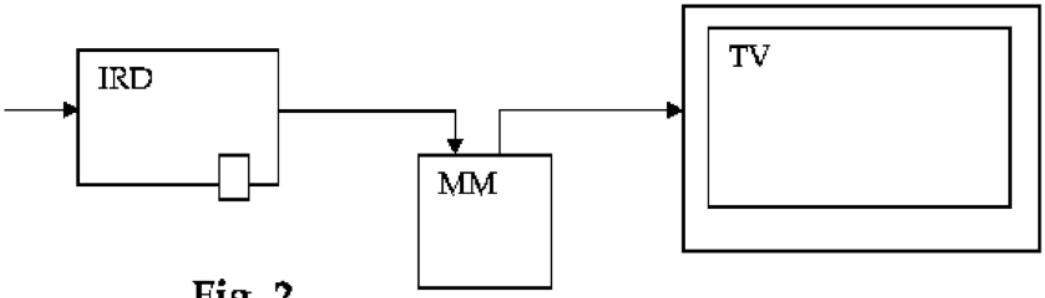

Fig. 2

Fig. 3

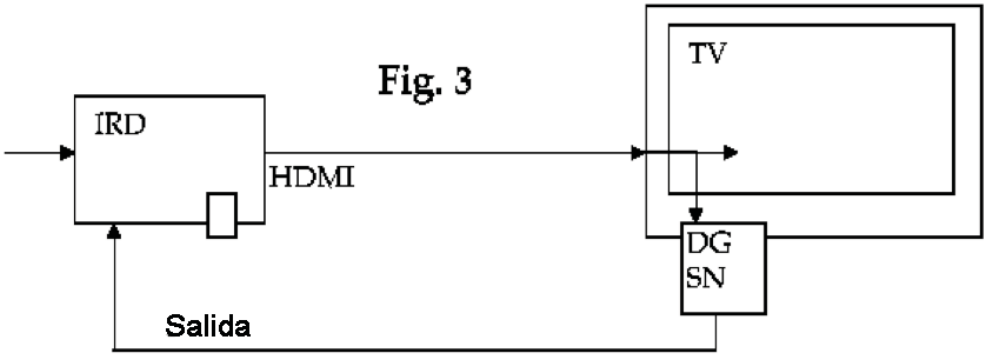

Fig. 4

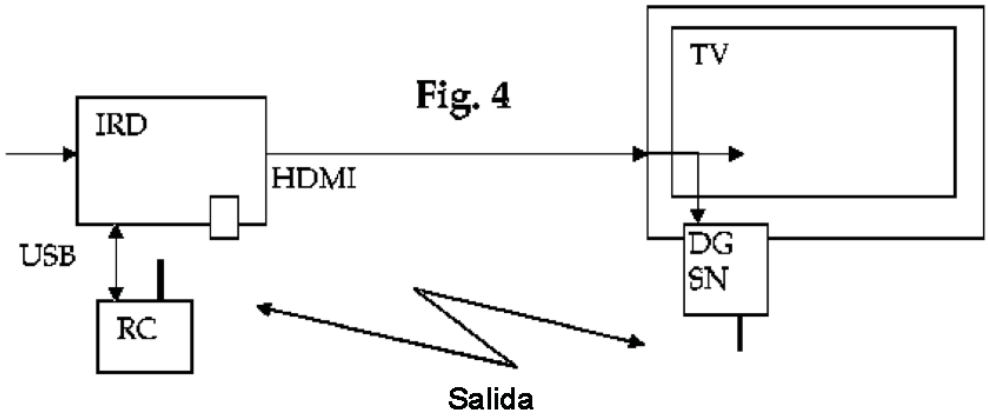

Fig. 5

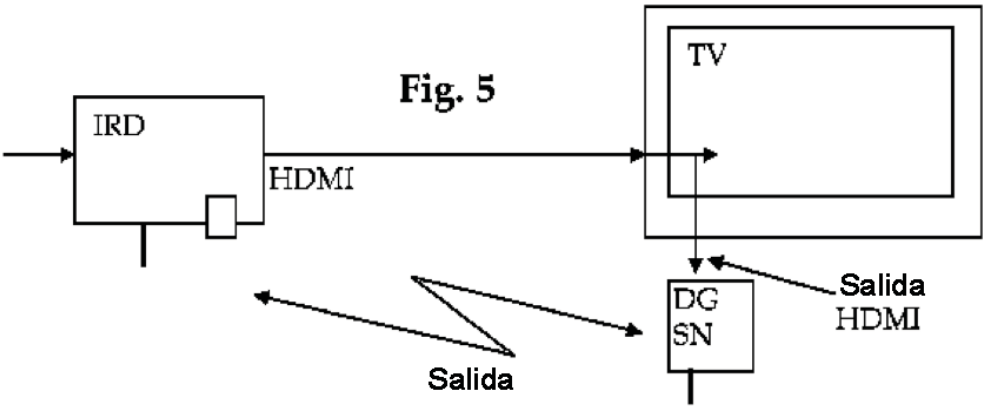

Fig. 6

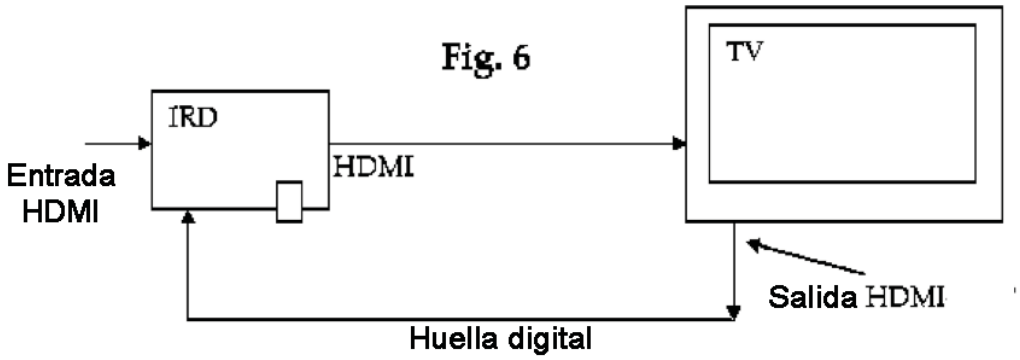

Fig. 7

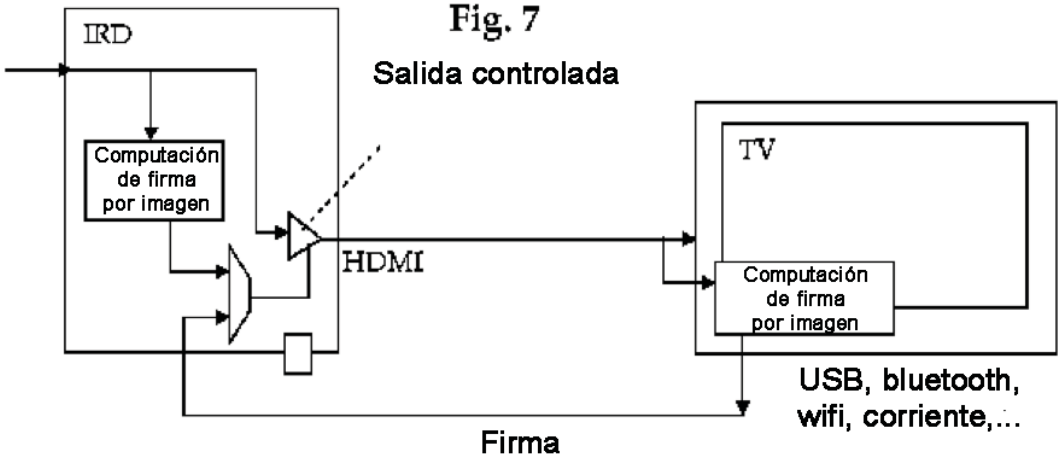

Fig. 8