



(51) International Patent Classification:
G06F 21/00 (2006.01) H04N 7/24 (2011.01)

(21) International Application Number:
PCT/EP2011/060651

(22) International Filing Date:
24 June 2011 (24.06.2011)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
61/364,834 16 July 2010 (16.07.2010) US
10185371.1 1 October 2010 (01.10.2010) EP

(71) Applicant (for all designated States except US): **NA-GRAVISION S.A.** [CH/CH]; Route de Geneve 22-24, CH-1033 Cheseaux-sur-Lausanne (CH).

(72) Inventors; and

(75) Inventors/Applicants (for US only): **KUDELSKI, Andre** [CH/CH]; Chemin de Bellingard, CH-1095 Lutry (CH). **NICOLAS, Christophe** [CH/CH]; Chemin de Sous-Aliens 15, CH-1162 Saint-Prex (CH).

(74) Agent: **LEMAN CONSULTING S.A.**; Chemin de Precosy 31, CH-1260 Nyon (CH).

(81) Designated States (unless otherwise indicated, for every kind of national protection available): AE, AG, AL, AM, AO, AT, AU, AZ, BA, BB, BG, BH, BR, BW, BY, BZ, CA, CH, CL, CN, CO, CR, CU, CZ, DE, DK, DM, DO, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, GT, HN, HR, HU, ID, IL, IN, IS, JP, KE, KG, KM, KN, KP, KR, KZ, LA, LC, LK, LR, LS, LT, LU, LY, MA, MD, ME, MG, MK, MN, MW, MX, MY, MZ, NA, NG, NI, NO, NZ, OM, PE, PG, PH, PL, PT, RO, RS, RU, SC, SD, SE, SG, SK, SL, SM, ST, SV, SY, TH, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, ZA, ZM, ZW.

(84) Designated States (unless otherwise indicated, for every kind of regional protection available): ARIPO (BW, GH, GM, KE, LR, LS, MW, MZ, NA, SD, SL, SZ, TZ, UG, ZM, ZW), Eurasian (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European (AL, AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HR, HU, IE, IS, IT, LT, LU, LV, MC, MK, MT, NL, NO, PL, PT, RO, RS, SE, SI, SK, SM, TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG).

Published:

— with international search report (Art. 21(3))

(54) Title: SYSTEM AND METHOD TO PREVENT MANIPULATION OF TRANSMITTED VIDEO DATA

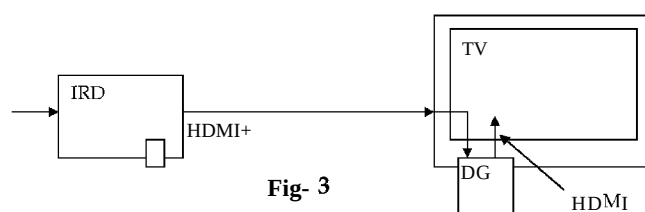


Fig- 3

(57) Abstract: The aim of the invention is to provide a solution to ensure that the content sent by the IRD is the content effectively displayed on the screen. It is then proposed a system to prevent manipulation of transmitted video data comprising an Integrated Receiver Decoder (IRD) receiving audio/video data, a display device (TV), said IRD comprising means to transmit an HDMI compliant audio/video stream toward the display device, characterized in that the system further comprises means to add an over-encryption layer to said HDMI/HDCP stream before reaching the display device and means to remove this added encryption layer so as to recover said HDMI/HDCP stream, before processing said HDMI/HDCP stream by said display device.

System and method to prevent manipulation of transmitted video data

Introduction

The present invention concerns the field of television devices, in particular a set-top-boxes (or IRD Integrated Receiver Decoder) designed to providing additional media
5 experience on the television.

Prior art

The today's situation is described in respect with the figure 1. The IRD is connected to the various sources of data (IP, satellite, cable, antenna) and is in charge of
10 extending the capabilities of the television by providing decryption of the encrypted data as well as handling the access rights. The IRD proposes also storage capabilities, parental control with identification of the user to apply the proper profile and a program guide. The output is connected to a television or a screen to take advantage of the multimedia experience.

15 One of the revenue model of the media content providers is the advertisement introduced during appealing broadcast content. It is therefore important that the advertisements sent by the IRD to the television is not replaced by other information.

The document US 2008/0235140 discloses a dongle for digital rights management protection which includes a digital right management engine and an
20 encryption/ decryption engine. The digital rights management engine is adapted to port digital rights management rules of a source of content to digital rights management rules enforced by the digital rights management engine. The encryption/ decryption engine is adapted to re-encrypting the source of content into a managed copy of the content and the managed copy of the content is locked to the
25 dongle.

Brief description of the invention

The aim of the invention is to provide a solution to ensure that the content sent by the IRD is the content effectively displayed on the screen.

It is therefore proposed a system to prevent manipulation of transmitted video data comprising an Integrated Receiver Decoder (IRD) receiving audio / video data, a display device (TV), said IRD comprising means to transmit an HDMI compliant audio / video stream toward the display device, characterized in that this system
5 further comprises means to add an over-encryption layer to this HDMI/HDCP stream before reaching the display device and means to remove this added encryption layer so as to recover this HDMI/HDCP stream, before processing this HDMI/HDCP stream by said display device.

Brief description of the figures

10 The present invention will be better understood thanks to the attached figures in which :

The **figure 1** illustrates the standard known system.

The **figure 2** shows the so-called "man-in-the-middle" attack

The **figure 3** illustrates a first solution to address this problem

15 The **figure 4** is similar to the figure 3 with the difference that the HDMI+ stream is directly connected to the dongle DG

The **figure 5** illustrates another embodiment of the invention

The **figure 6** illustrates a modification of the embodiment of the figure 5, in which the display device receives the HDMI+ stream and reroute it to the dongle

20 The **figure 7** is similar to the other designs with a wireless connection

The **figure 8** illustrates an embodiment in which the IRD comprises no wireless capabilities.

Description of the various embodiments

The **figure 1** illustrates the standard known system. The IRD (Integrated Receiver
25 Decoder) is on one side connected to the broadcast channels, such as via an antenna, cable, or IP, and on the other side is connected to a display device TV. The purpose of the IRD is to receive the signal, convert it into a plurality of channels, and if necessary, decrypt the selected channel with the cooperation of a security module.

The selected channel is then transmitted to the TV via an HDMI cable. Other functions are also proposed by the IRD such as recording an event, either directly while it is broadcasted, or according to a programmed time / date.

The IRD is also in charge of the reception, preparation and display of the Electronic Program Guide (EPG) that helps the user to quickly access the desired channel.

The HDMI communication is protected by HDCP which defines the frame of data exchange. HDCP is based on certificates verification and data encryption. Before the data are outputted by a source device, a handshake is initiated during which the certificate of the source and the sink are exchanged. The received certificate (e.g. X509) is then verified and used to establish a common encryption key. The verification can use white or black lists. The known HDMI communication protected by HDCP adds an encryption layer to an unprotected HDMI stream. However, HDCP being a well known standard, an additional device can embed genuine HDCP certificates and can therefore receive the content sent by the IRD in view of manipulating said content.

Contrary to the prior art, it should be noted that the present invention does not attempt to decrypt the HDMI/HDCP stream in order to get the basic HDMI stream, namely an HDMI stream which is unprotected by the HDCP protocol.

The **figure 2** shows the so-called "man-in-the-middle" attack in which an additional device MM is placed at the output of the IRD and intercepts the audio/ video stream. The risk in such a case is to bypass the security rules that were associated with the content such as "view only", "view once", "no record". The fact that the content is in an external device opens the possibility for a third party to use the content in a way not authorized by the content provider. Another aim of this patent application is to detect the presence of such external and in-between device by the IRD and take appropriate action.

The **figure 3** illustrates a first solution to address this problem. The IRD outputs a modified HDMI/HDCP signal, called HDMI+ in which all or part of the payload (audio/ video data) is protected by an encryption layer. The format is the same as the original HDMI/HDCP but the audio/video data are further encrypted (i.e. over-

encrypted). Contrarily to the HDMI/HDCP which has also a standard encryption layer by means of HDCP protocol, designed to exchange data with any device having the correct certificate, the HDMI+ layer is a proprietary encryption layer, namely a layer which cannot be decrypted without knowing the encryption mode used to generate this layer. The HDMI+ stream is then sent to the display device TV through the HDMI input. The header of the packets sent according to this standard contains an indicator allowing the display device TV to redirect the stream to a dongle DG connected with the display device. According to one embodiment, the connector is a CI+ connector but the present invention is not limited to this solution.

10 We can also have a HDMI like dongle having an input and an output. The purpose of this dongle DG (connected to the CI+ port of another port) is to receive the HDMI+ stream and remove the proprietary encryption layer.

For that purpose, the dongle should contain the same key (or keys) as in the IRD.

Different solutions exist to achieve this aim. The first method is based on a pre-initialization of the dongle with encryption key. This dongle has a unique number identifying it and thus allowing the management center to trace the use of the dongle. When the dongle is delivered to the client, a suitable message can be send to the client's IRD to transmit, in a secure way, the corresponding key (or keys) that were previously loaded into the dongle. The dongle and the IRD are then paired and can only work together.

Another way to share the same key between the dongle and the IRD is to connect the dongle directly with the IRD. For that purpose, the IRD can use its HDMI connection already present in the dongle, or alternatively, use another connection such as USB, wifi or other. The dongle will then contain in addition to the HDMI input and output, a USB connection. During an initialization step, the IRD will read the unique number of the dongle, and start the generation of the communication key.

Generation method such as Diffie-Hellman can be used.

At the end of the initialization, the IRD and the dongle are paired, i.e. contain the same key.

The dongle acts as a bridge, receiving the encrypted HDMI+, remove the over-encryption layer thanks to the key previously loaded, and return the HDMI/HDCP stream to the display device.

The **figure 4** is similar to the figure 3 with the difference that the HDMI+ stream is directly connected to the dongle DG. The function of the dongle is the same as before. The display device does not need to be modified to reroute the HDMI+ stream to the dongle. In this solution, the form factor plays an interesting role. The preferred solution is using another input than the standard HDMI input. The CI+ connection, as an example, gives a better protection against tampering the output of the dongle. The dongle DG, in case in the form of a CI+ card, can comprise an HDMI input and a HDMI output. The HDMI output is then connected to the standard HDMI input of the display device. The connector of the CI+ is essentially used to power the dongle. To this end, the dongle has the shape of a CI+ card and is powered by the CI+ Interface of the display device.

The way to load the decryption key into the dongle has been described and is also valid for this case.

The **figure 5** illustrates another embodiment of the invention. In this case, the IRD is not HDMI+ compliant. This is why a converter box CC is added at the output of the IRD to convert the HDMI/HDCP to HDMI+. It is not necessary, for the converter box, to have a HDMI certificate since no decryption will be carried out in this module. The processing device simply detects the beginning of a packet (packet header) and over-encrypts the payload with the key common to the converter box and the dongle DG. The dongle executes the reverse function, i.e. removing this extra encryption layer thanks to the decryption key.

The difference between the **figure 5 and 6** is the same as the figure 3 and 4. In a first example, the display device receives the HDMI+ stream and reroute it to the dongle. In the other example, the dongle receives directly the stream and, once decrypted, pass it to the display device.

The feedback connection between the converter box CC with the IRD can be used to check whether the HDMI link between these two devices was not modified. The

converter box CC can extract randomly or on request of the IRD, a packet entering into the converter box, this packet being sent back to the IRD for verification. Instead of the packet, the converter box can send a signature (e.g. an Hash value) of it for comparison by the IDR. The IRD execute the same function to calculate the signature of the packet sent and compare the received signature with the one calculated. The IRD can then determine if the packet sent to the converter box is the same as the one received by the converter box and sent back. In case if discrepancy, the IRD can take suitable actions.

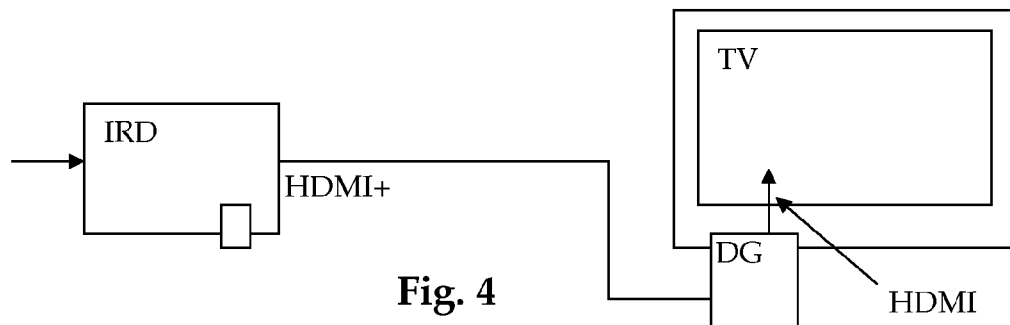
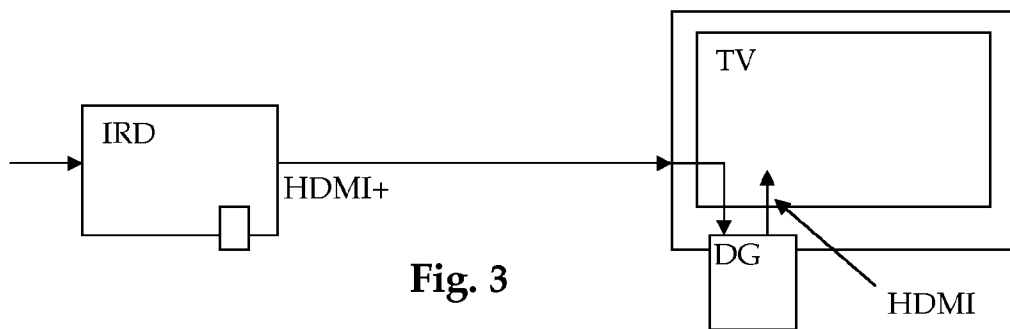
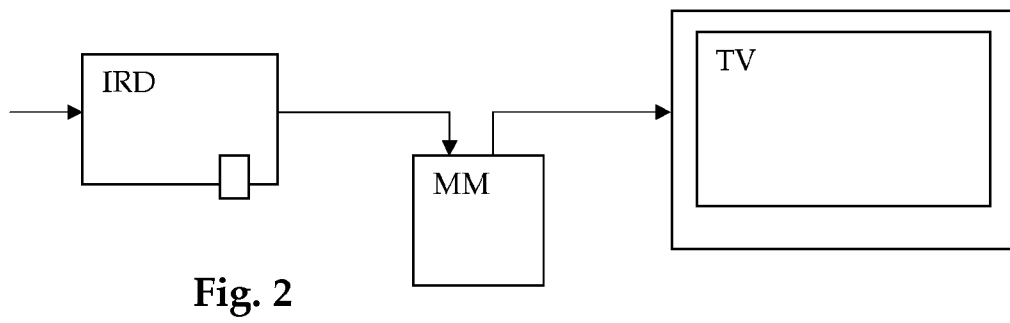
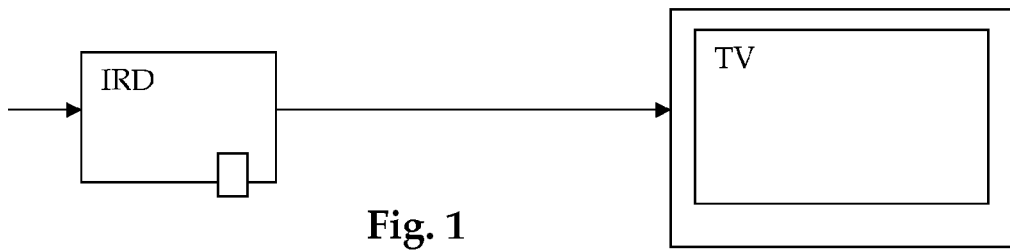
The **figure 7** is similar to the other designs, the wire connection between the IRD and the display device being replaced by a wireless connection. The figure 7 illustrates an example in which the IRD contains wireless capabilities. The HDMI+ signal is sent and the dongle can receive this signal. Once decrypted, the dongle DG can pass it to the display device.

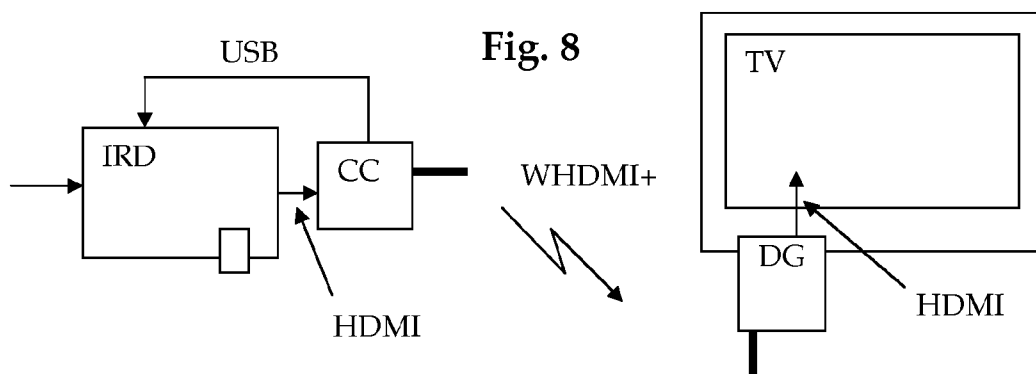
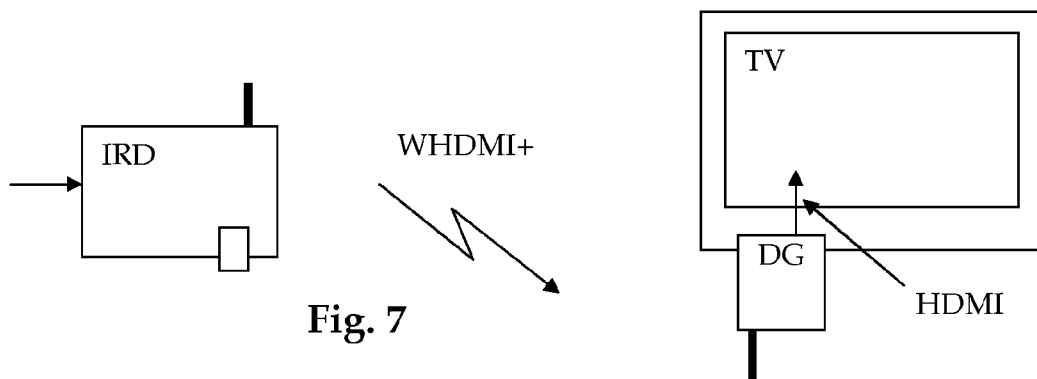
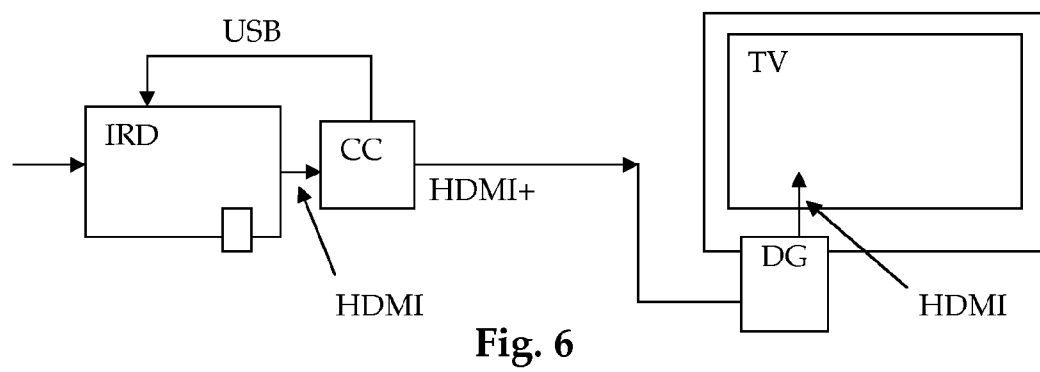
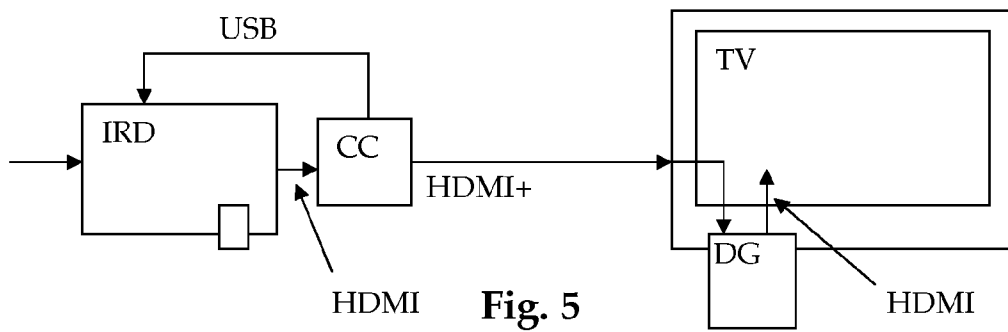
The **figure 8** illustrates an embodiment in which the IRD comprises no wireless capabilities. In this case, the converter box already described above contains a wireless emitter to transmit the signal HDMI+.

Claims

1. System to prevent manipulation of transmitted video data comprising an Integrated Receiver Decoder (IRD) receiving audio/ video data, a display device (TV), said IRD comprising means to transmit an HDMI compliant audio / video stream protected by an HDCP protocol toward the display device, characterized in that it further comprises means to add an over-encryption layer to said HDMI/HDCP stream before reaching the display device and means to remove this added encryption layer so as to recover said HDMI/HDCP stream, before processing said HDMI/HDCP stream by said display device.
2. System of claim 1, wherein said over-encryption layer is a proprietary encryption layer which cannot be decrypted without knowing an encryption mode used to generate this over-encryption layer.
3. System of claim 1, wherein said means to remove the over-encryption layer is external to said display device.
4. System of claim 1 or 3, wherein said means to remove the over-encryption layer is a dongle which comprises means to receive the over-encrypted HDMI/HDCP stream and means to return it to the display device after removing the over-encryption.
5. System of claim 4, wherein the dongle has the shape of a CI+ card and is powered by a CI+ Interface of the display device.
6. System of any of the claims 1 to 5, wherein the IRD comprises an external converter box which is in charge of receiving the HDMI/HDCP stream and to add an over-encryption layer to said HDMI/HDCP stream.
7. System of claim 6, wherein the converter box comprises feedback means to communicate with the IRD and means to extract a packet entering into the converter box and means to send it via the feedback means.
8. System of claim 6, wherein the converter box comprises feedback means to communicate with the IRD and means to extract a packet entering into the converter box and means to send a signature of the packet via the feedback means.

9. System of any of the claims 1 to 8, wherein the connection between the IRD or the converter box and the display device or the dongle, is wireless.





INTERNATIONAL SEARCH REPORT

International application No
PCT/EP2011/060651

A. CLASSIFICATION OF SUBJECT MATTER
INV. G06F21/00 H04N7/24
ADD..

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
G09G H04N H04L G06F

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practical, search terms used)

EPO-Internal

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
Y	US 2008/235140 A1 (READ CHRISTOPHER JENSEN [US]) 25 September 2008 (2008-09-25)	1-6, 8, 9
A	abstract paragraph [0015]; figure 1 paragraph [0016]; figure 2 paragraphs [0019] , [0021] paragraphs [0027] - [0028]; figures 3,6 paragraph [0029] paragraph [0030] ----- -/- .	7



Further documents are listed in the continuation of Box C.



See patent family annex.

* Special categories of cited documents :

"A" document defining the general state of the art which is not considered to be of particular relevance

"E" earlier document but published on or after the international filing date

"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)

"O" document referring to an oral disclosure, use, exhibition or other means

"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art.

"&" document member of the same patent family

Date of the actual completion of the international search

20 September 2011

Date of mailing of the international search report

28/09/2011

Name and mailing address of the ISA/

European Patent Office, P.B. 5818 Patentlaan 2
NL - 2280 HV Rijswijk
Tel. (+31-70) 340-2040,
Fax: (+31-70) 340-3016

Authorized officer

Berne, Jean-Frangois

INTERNATIONAL SEARCH REPORT

International application No

PCT/EP2011/060651

C(Continuation). DOCUMENTS CONSIDERED TO BE RELEVANT		
Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
Y	HITACHI ET AL: "High-Definition Multimedia Interface Specification Version 1.1", INTERNET CITATION, 20 May 2004 (2004-05-20) , page COMPLETE, XP007909795 , Retrieved from the Internet: URL: http://www.hdmi.org/download/HDMI_Specification_1.1.pdf [retrieved on 2009-09-16]	1-6,8,9
A	page 96	7
Y	Oogabada: "HDFury: la scorciatoia per l'accesso alla next-gen PS3", console-tri.be.com , 14 September 2007 (2007-09-14) , XP002623712 , Retrieved from the Internet: URL: http://ps3.console-tri.be.com/articoli/5/hdfury-la-scorciatoia-per-l-accesso-alla-next-gen-ps3.html [retrieved on 2011-02-18]	3,4
A	page 4; figure 1 page 5; figure 3 page 8; figure 1	1,2,5-9
Y	US 2007/028260 A1 (WILLIAMS GEORGE [US] ET AL WILLIAMS GEORGE [US] ET AL) 1 February 2007 (2007-02-01)	5
A	abstract figure 2 paragraphs [0038] - [0040] ; figure 5 paragraphs [0041] - [0042] paragraph [0065]	1-4,6-9
Y	US 2008/134237 A1 (TU EDGAR [US] ET AL) 5 June 2008 (2008-06-05)	8
A	abstract figure 5 paragraphs [0072] - [0074] ; figure 9 paragraphs [0126] - [0128] paragraph [0163]	1-7 ,9

INTERNATIONAL SEARCH REPORT

Information on patent family members

International application No

PCT/EP2011/060651

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
US 2008235140	A1	25-09-2008	NONE
US 2007028260	A1	01-02-2007	US 2010083337 A1 01-04-2010
US 2008134237	A1	05-06-2008	EP 2052542 A2 29-04-2009 JP 2010502115 A 21-01-2010 WO 2008022301 A2 21-02-2008