



(43) International Publication Date
6 September 2013 (06.09.2013)

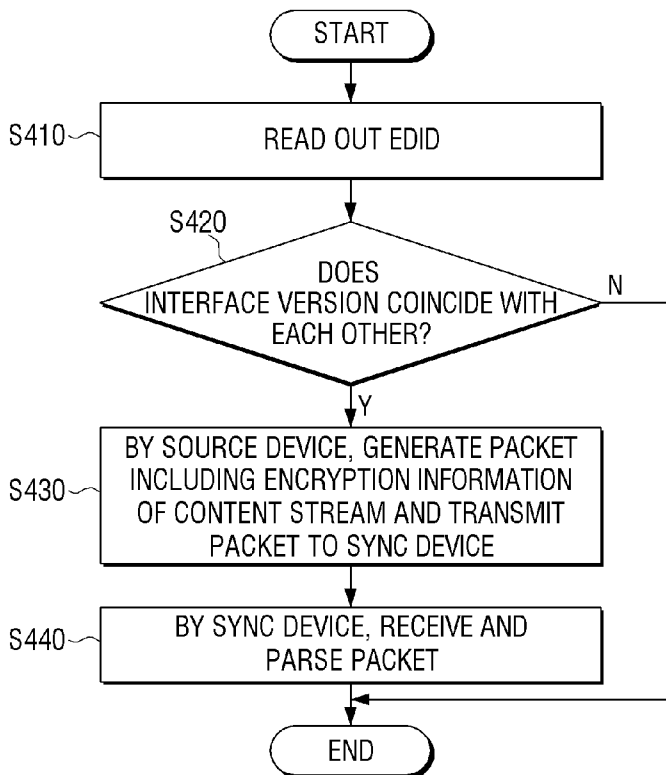
- (51) International Patent Classification:
H04L 12/70 (2013.01) H04L 9/12 (2006.01)
- (21) International Application Number:
PCT/KR2013/001052
- (22) International Filing Date:
8 February 2013 (08.02.2013)
- (25) Filing Language: English
- (26) Publication Language: English
- (30) Priority Data:
61/604,831 29 February 2012 (29.02.2012) US
10-2012-0134843
26 November 2012 (26.11.2012) KR
- (71) Applicant: SAMSUNG ELECTRONICS CO., LTD.
[KR/KR]; 129, Samsung-ro, Yeongtong-gu, Suwon-si,
Gyeonggi-do 443-742 (KR).
- (72) Inventors: Yun, Suk-jin; 2-204, Jinheung Apt., Seocho
4(sa)-dong, Seocho-gu, Gyeonggi-do 137-776 (KR). KIM,
Soo-young; No. 204, Yeji Villat, 1250-4, Maetan 3(sam)-
dong, Yeongtong-gu, Suwon-si, Gyeonggi-do 443-848
(KR). KIM, Jong-hwa; 172-13, Godeung-dong, Paldal-gu,

Suwon-si, Gyeonggi-do 442-882 (KR). NA, Il-ju; 101-306, Jukjeon Xi 2-cha Apt., Bojeong-dong, Giheung-gu, Yongin-si, Gyeonggi-do 446-913 (KR). LEE, Jae-min; 113-1701, Raemian Nobleclass Apt., Ingye-dong, Paldal-gu, Suwon-si, Gyeonggi-do 442-703 (KR).

- (74) Agent: JEONG, Hong-sik; 8th Floor, Daelim Bldg., 1600-3, Seocho-dong, Seocho-gu, Seoul 137-877 (KR).
- (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, BN, 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, 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, PA, PE, PG, PH, PL, PT, QA, RO, RS, RU, RW, 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, RW, SD, SL, SZ, TZ, UG, ZM, ZW), Eurasian (AM, AZ, BY, KG, KZ, RU, TJ,

[Continued on next page]

(54) Title: DATA TRANSMITTER, DATA RECEIVER, DATA TRANSCIEVING SYSTEM, DATA TRANSMITTING METHOD, DATA RECEIVING METHOD, AND DATA TRANSCIEVING METHOD



(57) Abstract: A data transmitter is provided. The data transmitter includes a packet generating unit which generates a packet including encryption information of a content stream, and a transmitting unit which transmits the generated packet to a data receiver, wherein the generated packet comprises a first field for indicating identification information of the content stream, and a second field for indicating an encryption parameter value of the content stream.

WO 2013/129785 A1

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))*

Description

Title of Invention: DATA TRANSMITTER, DATA RECEIVER, DATA TRANSCIVING SYSTEM, DATA TRANSMITTING METHOD, DATA RECEIVING METHOD, AND DATA TRANSCIVING METHOD

Technical Field

- [1] Apparatuses and methods consistent with exemplary embodiments relate to a data transmitter, a data receiver, and a data transceiving method, and more particularly, to a data transmitter and a data receiver which transmit and receive an encryption parameter for a content stream, a data transceiving system, a data transmitting method, a data receiving method, and a data transceiving method.

Background Art

- [2] Recently, as multimedia environments have developed, wired interface environments for high-quality content transmission have been introduced. For example, High-Definition Multimedia Interface (HDMI) and Mobile High-Definition Link (MHL) provide transmission standards for high quality of diverse formats of video data, audio data and control signals. In such a wired interface environment for high-quality content transmission, a technology for protecting illegal copy of contents. High-bandwidth Digital Content Protection (HDCP) is a kind of video copyright protection technology which was introduced for the above purpose.
- [3] HDCP has a feature of inter-operability which is used as copyright protection technology for contents. Inter-operability indicates that in order to use original content to which HDCP is applied in high-definition, a display apparatus which meets HDCP standard requirements is needed. In other words, in order to use HDCP content, all component connectors which may access a display apparatus must meet the HDCP standard requirements.
- [4] If a receiver which is connected to a source providing HDCP content does not meet the HDCP standard requirements, image quality may deteriorate. For example, video resolution may be as compulsorily down-converted as image quality of a general digital versatile disk (DVD) is output. Similarly, DVD audio content which does not meet the HDCP standard requirements may deteriorate to digital audiotape (DAT) quality or at worst may not be output.
- [5] Down-conversion of image quality of content is compelled by a particular digital flag, an Image Constraint Token (ICT). A content provider uses a flag so as to limit output by a display apparatus or output by image component of a set top box. The

content provider may put an ICT into each disk or content. In order to use high-definition content of the highest resolution, a device supporting HDCP is needed. However, in an environment having no device supporting HDCP, when an HDCP source is connected, it is not always that nothing is output. This may be decided by the content provider.

[6] HDCP has developed from 1.0 version supporting Digital Visual Interface (DVI) to 1.3 version supporting DVI, HDMI, UDI, gigabit video interface (GVIF), DisplayPort (DP) and the like. Recently, 2.x version has been discussed.

[7] FIG. 1 illustrates a problem of compatibility between a source device and a sink device in HDMI 2.0.

[8] In HDMI 2.0 version, a new content protection (CP) scheme may be adopted. If a source device encrypts audio/video content using new CP, there may be a problem of compatibility with a sink device which can recognize only existing CP as illustrated in FIG. 1. In this case, the source device must be able to identify a sink device any time before transmitting audio/video content. This concept is applied to other wired interface environments which are similar to HDMI in the same manner.

[9] As stated above, adoption of new CP schemes in diverse wired interfaces is under discussion. This is because in an environment of transmitting mass storage ultra-high definition (UHD) 4K content, it is difficult to guarantee the security of content distribution by simply expanding only bandwidth. Accordingly, received UHD 4K content needs to be protected using a stronger content protection scheme.

[10] In order to protect content more strongly by the introduction of new CP, a means for safely transmitting a parameter used for encryption is needed. This is related to link synchronization of CP.

Disclosure of Invention

Technical Problem

[11] Exemplary embodiments may overcome the above disadvantages and other disadvantages not described above. Also, the present invention is not required to overcome the disadvantages described above, and an exemplary embodiment may not overcome any of the problems described above.

[12] Exemplary embodiments provide a data transmitter, a data receiver, a data transceiving system, a data transmitting method, a data receiving method, and a data transceiving method, which provide a new content protection scheme and are capable of safely transmitting and receiving a parameter used for encryption of a content stream.

Solution to Problem

[13] According to an aspect of an exemplary embodiment, a data transmitter may

comprise a packet generator configured to generate a packet including encryption information of a content stream, and a transmitter which transmits the generated packet to a data receiver, wherein the generated packet may include a first field for indicating identification information of the content stream, and a second field for indicating a first encryption parameter value of the content stream.

- [14] The second field may comprise at least one from among a first sub-field for indicating a second encryption parameter value to distinguish the content stream, and a second sub-field for indicating a third encryption parameter value for link synchronization between the data transmitter and the data receiver.
- [15] The third encryption parameter value for link synchronization may be a value obtained by adding a number of lines of a transmission frame to a fourth encryption parameter value for link synchronization included in a previous packet of the generated packet.
- [16] The generated packet may be transmitted between a time point when a vertical synchronizing signal is enabled and a time point when a keep_out signal is enabled, in a clock signal period.
- [17] The generated packet may be transmitted between a time point when a transmission period of a general control packet finishes and a time point when a keep_out signal is enabled, in a clock signal period.
- [18] The generated packet may be included in a transmission frame of the content stream and be transmitted. In a clock signal period, an encryption enable signal may be transmitted and a result value of encrypting each line of the transmission frame may be output from a time point when a data enable signal is transmitted.
- [19] The generated packet may be included in a transmission frame of the content stream and be transmitted, and in a clock signal period, a result value of encrypting each line of the transmission frame may be output between a time point when a win_of_opp signal is disabled and a time point when the win_of_opp signal is enabled again, wherein a win_of_opp signal informs whether to encrypt a frame.
- [20] Whether to enable or disable the encryption enable signal may be determined according to a win_of_opp signal in a period when a keep_out signal is enabled in the clock signal period.
- [21] The generated packet may be included in a transmission frame of the content stream and be transmitted, and in a clock signal period, a transmission frame of the content stream may be encrypted in a period excluding a period between a time point when a vertical synchronizing signal (vsync) is enabled and a time point when a keep_out signal is enabled.
- [22] According to another aspect of the present invention, a data receiver may comprise a receiver configured to receive a packet including encryption information of a content

stream from a data transmitter, and a packet parser configured to parse the received packet, wherein the received packet may include a first field for indicating identification information of the content stream, and a second field for indicating a first encryption parameter value of the content stream.

[23] The second field may include at least one from among a first sub-field for indicating a second encryption parameter value to distinguish the content stream, and a second sub-field for indicating a third encryption parameter value for link synchronization between the data transmitter and the data receiver.

[24] The data receiver may determine whether a value obtained by adding a number of lines of a transmission frame to a fourth encryption parameter value for link synchronization included in a previous packet of the received packet coincides with the encryption parameter value for link synchronization included in the second field.

[25] The received packet may be transmitted between a time point when a vertical synchronizing signal is enabled and a time point when a keep_out signal is enabled, in a clock signal period.

[26] The received packet may be included in a transmission frame of the content stream and be transmitted, and in a clock signal period, an encryption enable signal may be transmitted and a result value of encrypting each line of the transmission frame may be output from a time point when a data enable signal is transmitted.

[27] According to yet another aspect of an exemplary embodiment, a data transmitting method may comprise generating a packet including encryption information of a content stream, and transmitting the generated packet to a data receiver, wherein the generated packet may include a first field for indicating identification information of the content stream, and a second field for indicating a first encryption parameter value of the content stream.

[28] The second field may include at least one from among a first sub-field for indicating an encryption parameter value to distinguish the content stream, and a second sub-field for indicating a third encryption parameter value for link synchronization between a data transmitter and a data receiver.

[29] According to yet another aspect of the present invention, a data receiving method may comprise receiving a packet including encryption information of a content stream from a data transmitter, and parsing the received packet, wherein the received packet may include a first field for indicating identification information of the content stream, and a second field for indicating a first encryption parameter value of the content stream.

[30] The second field may include at least one from among a first sub-field for indicating a second encryption parameter value to distinguish the content stream, and a second sub-field for indicating a third encryption parameter value for link synchronization

between the data transmitter and a data receiver.

[31] According to yet another aspect of an exemplary embodiment, a data transceiving system may include a source device which reads out Extended Display Identification Data (EDID) from a sink device, and if interface version information included in the EDID coincides with version information of an interface provided by the source device, generates a packet including encryption information of a content stream and transmits the generated packet to the sink device, and the sink device which receives and parses the transmitted packet, wherein the transmitted packet may include at least one from among a first field for indicating identification information of the content stream, and a second field for indicating an encryption parameter value of the content stream.

[32] According to yet another aspect of an exemplary embodiment, a data transceiving method may include by a source device, reading out Extended Display Identification Data (EDID) from a sink device, if version information of an interface supported by the sink device included in the EDID coincides with version information of an interface provided by the source device, generating, at the source device, a packet including encryption information of a content stream and transmitting the generated packet to the sink device, and at the sink device, receiving and parsing the transmitted packet, wherein the transmitted packet may include at least one from among a first field for indicating identification information of the content stream, and a second field for indicating an encryption parameter value of the content stream.

[33] Additional and/or other aspects of exemplary embodiments will be set forth in part in the description which follows and, in part, will be obvious from the description, or may be learned by practice of the aspects of exemplary embodiments.

[34]

Advantageous Effects of Invention

[35]

-

Brief Description of Drawings

[36] The above and/or other aspects of exemplary embodiments will be more apparent with reference to the accompanying drawings, in which:

[37] FIG. 1 illustrates a problem of compatibility between a source device and a sink device in HDMI 2.0;

[38] FIG. 2 illustrates a method for solving compatibility problem occurring when new CP is used;

[39] FIG. 3 is a flow chart illustrating a process of identifying an HDMI version of a sink device;

[40] FIG. 4 is a flow chart illustrating a data transceiving method consistent with an

exemplary embodiment of the present invention;

[41] FIGS. 5 and 6 illustrate a transmission period of a Content Protection Synchronization Packet (CPSP);

[42] FIG. 7 illustrates transmission and reception of a partially encrypted TMDS signal between an HDCP transmitter and an HDCP receiver;

[43] FIG. 8 is a block diagram illustrating a configuration of a data transceiving system consistent with an exemplary embodiment;

[44] FIG. 9 is a block diagram illustrating a configuration of a data transmitter consistent with an exemplary embodiment;

[45] FIG. 10 is a block diagram illustrating a configuration of a data receiver consistent with an exemplary embodiment;

[46] FIG. 11 is a flow chart illustrating a data transmitting method consistent with an exemplary embodiment; and

[47] FIG. 12 is a flow chart illustrating a data receiving method consistent with an exemplary embodiment.

Best Mode for Carrying out the Invention

[48] -

Mode for the Invention

[49] Certain exemplary embodiments will now be described in greater detail with reference to the accompanying drawings.

[50] In the following description, same drawing reference numerals are used for the same elements even in different drawings. The matters defined in the description, such as detailed construction and elements, are provided to assist in a comprehensive understanding of the invention. Thus, it is apparent that the exemplary embodiments can be carried out without those specifically defined matters. Also, well-known functions or constructions are not described in detail since they would obscure the invention with unnecessary detail.

[51] Exemplary embodiments may be applied to diverse wired interface transmission standards such as MHL as well as HDMI within the same scope as the technical idea of the exemplary embodiments. Accordingly, the scope of the exemplary embodiments may extend to similar wired interface transmission standards.

[52] Firstly, a method for solving compatibility problem which may occur when new content protection (CP) is defined in the HDMI 2.x standard, is described below.

[53] FIG. 2 illustrates a method for solving compatibility problem occurring when new CP is used.

[54] As illustrated in FIG. 2, HDMI 2.x may include new CP as well as HDCP 1.x. A source device checks information about a version of a sink device from Extended

Display Identification Data (EDID) or corresponding E-EDID which is received from the sink device. If the sink device supports HDMI 1.x, i.e. if the sink device decrypts a signal encrypted in HDCP 1.x, the source device transmits audio/video data based on legacy syncing capability. On the other hand, if the sink device supports HDMI 2.x, i.e. if the sink device supports the new CP (or decrypts a signal encrypted in HDCP 2.x), the source device transmits audio/video data based on a new syncing capability.

[55] Information about a version of HDMI may be written in a version control field of a Vendor-specific Data Block (VSDB) as shown below.

[56] The table shown below illustrates a VSDB containing a field indicating an HDMI version.

[57]

[58] <Table 1>

[59] HDMI-LLC Vendor-Specific Date Block (HDMI-VSDB)

Byte#	7	6	5	4	3	2	1	0
0	Vendor-specific Code(=3)			Length(=N)				
1	24-bit IEEE Registration Identifier (0x000C03) (least significant byte first)							
2								
3								
4	A				B			
5	C				D			
6	Supports_AI	DC_48bit	DC_36bit	DC_30bit	DC_Y444	HDMI Version		DVI DUAL
7	Max_TMDS_Clock							
8	Latency_Field_Presence	I_Latency_Field_Presence	HDMI_Video_Presence	Rsvd(0)	CNC3	CNC2	CNC1	CNC0
...	...							
13	3D	3D_Multi present			Rsvd(0)	Rsvd(0)	Rsvd(0)	Rsvd(0)
14	HDMI_VIC_LEN				HDMI_3D_LEN			
...	...							

Bit 1	Bit 2	Description
0	0	HDMI 1.x
0	1	HDMI 2.x
1	0	Reserved

[60]

[61] As shown in Table 1, HDMI version information may be shown using 2 bits. This shows that 00 indicates HDMI 1.x and 01 indicates HDMI 2.x.

[62] FIG. 3 is a flow chart illustrating a process of identifying an HDMI version of a sink device.

[63] With reference to FIG. 3, a process of identifying an HDMI version of a sink device by a source device proceeds in the following order.

[64] A source device receives E-EDID or EDID from a sink device. The source device checks information about an HDMI version from a VSDB. If bits are 00, the sink device is a legacy device. Accordingly, the source device acts as a legacy device. Or, if bits are 01, the sink device supports HDMI 2.x. Accordingly, the source device supports HDMI 2.x, too.

[65] This is more clearly shown in FIG. 4.

[66] FIG. 4 is a flow illustrating a data transceiving method consistent with the exemplary embodiment.

[67] With reference to FIG. 4, in operation S410, the source device reads out EDID from the sink device. In operation S420, the source device determines whether information, which contained in the EDID, regarding an interface version supported by the sink device coincides with information about an interface version provided by the source device. The interface version information may be contained in a VSDB, and may be an HDMI version or HDCP version.

[68] In operation S430, if the interface version information supported by the sink device coincides with interface version information provided by the source device, the sink device may output content of the source device as it is so that the source device generates a packet including encryption information of a content stream and transmits the packet to the sink device.

[69] In operation S440, the sink device receives and parses the packet and extracts the encryption information from the packet. Subsequently, the sink device decrypts the content using the extracted encryption information.

[70] HDCP 2.1 is described below as an example of new CP supported by HDMI 2.x.

[71] The technical idea described below may be also applied to HDCP 2.x version which uses the same or similar algorithm.

[72] HDCP 2.1 uses AES-CTR mode as an encryption algorithm. In HDMI 2.x, if AES-CTR mode is selected as new content protection mechanism, a method for transmitting a parameter of CP is required. Table 2 shown below defines CP Sync. Packet (CPSP: Content Protection Synchronization Packet) which is a new packet to transmit a parameter. CPSP also synchronizes CP.

[73]

[74] <Table 2>

[75] Packet Types

Packet Type Value	Packet Type
0x00	Null
0x01	Audio Clock Regeneration(N/CTS)
0x02	Audio Sample (L-PCM and ICE 61937 compressed formats)
0x03	General Control
0x04	ACP packet
...	...
0x0A	Gamut Metadata Packet
0x0B	CP Sync. Packet
0x80+InfoFrame Type	InfoFrame Packet

[76]

[77] The structure of CPSP is described in the following diverse exemplary embodiments.

[78] The following tables show the structure of CPSP.

[79] The first exemplary embodiment

[80] A counter value distinguishable between each audio and video may be maintained.

[81]

[82] <Table 3>

[83] CP Sync. Packet Format

Byte#	7	6	5	4	3	2	1	0
HB0	Packet Type (0x0B)							
HB1	Reserved		Stream_ID				Type	
HB2	Reserved							
PB0	StreamCtr[31:24]							
PB1	StreamCtr[23:16]							
PB2	StreamCtr[15:08]							
PB3	StreamCtr[07:00]							
PB4	InputCtr[63:56]							
PB5	InputCtr[55:48]							
PB6	InputCtr[47:40]							
PB7	InputCtr[39:32]							
PB8	InputCtr[31:24]							
PB9	InputCtr[23:16]							
PB10	InputCtr[15:08]							
PB11	InputCtr[07:00]							
PB12~PB31	Reserved							

Bit1	Bit0	Description
0	0	Audio
0	1	Video
1	0	Reserved
1	1	Reserved

[84]

[85] Each field is described below.

[86] Stream_ID (4 bits) is an identifier for identifying a stream from multi-streams.

[87] Type (2 bits) is a field for indicating audio data or video data. If bits are 00, Type indicates an audio signal, or if bits are 01, Type indicates a video signal.

[88] StreamCtr (32 bits) is a count value of audio/video streams among a plurality of streams. StreamCtr is a parameter value which is used for encryption in AES CTR mode.

[89] InputCtr (64 bits) is also a parameter value which is used for encryption in AES CTR mode. InputCtr is used for link synchronization between a sink device and a source device.

[90] InputCtr (64 bits) for an audio signal increases whenever an active line ends. Block size is 16 bytes. InputCtr (64 bits) for a video signal increases by 1 whenever an active line ends. That is, InputCtr becomes a value obtained by adding the number of lines of a transmission frame to InputCtr contained in a previous CPSP. However, InputCtr

may not increase by 1 but may increase by a preset number.

[91] second exemplary embodiment

[92]

[93] <Table 4>

[94] Cy Sync Packet Format

Byte#	7	6	5	4	3	2	1	0
HB0	Packet Type(0x0B)							
HB1	Reserved						Type	
HB2	Reserved							
PB0	StreamCtr[31:24]							
PB1	StreamCtr[23:16]							
PB2	StreamCtr[15:08]							
PB3	StreamCtr[07:00]							
PB4	InputCtr[63:56]							
PB5	InputCtr[55:48]							
PB6	InputCtr[47:40]							
PB7	InputCtr[39:32]							
PB8	InputCtr[31:24]							
PB9	InputCtr[23:16]							
PB10	InputCtr[15:08]							
PB11	InputCtr[07:00]							
PB12~31	Reserved							

Bit1	Bit0	Description
0	0	Audio
0	1	Video
1	0	Shared
1	1	Reserved

[95]

[96] The second exemplary embodiment is similar to the first exemplary embodiment, but further includes a shared counter value of audio and video. That is, bits "10" indicates shared type of audio and video. This is named as hybrid scheme.

[97] Description of each field is the same as in the first exemplary embodiment.

[98] The third exemplary embodiment

[99] The third exemplary embodiment may include a field indicating whether encryption is enabled or disabled and a field indicating HDCP version information by using the "Reserved" section in HB1 and HB2 of the first exemplary embodiment.

[100]

[101] <Table 5>

[102] CP Sync Packet Format

Byte#	7	6	5	4	3	2	1	0
HB0	Packet Type(0x0B)							
HB1	Reserved		Stream_ID				Type	
HB2	ENC	Reserved	HDCP major version			HDCP major version		
PB0	StreamCtr[31:24]							
PB1	StreamCtr[23:16]							
PB2	StreamCtr[15:08]							
PB3	StreamCtr[07:00]							
PB4	InputCtr[63:56]							
PB5	InputCtr[55:48]							
PB6	InputCtr[47:40]							
PB7	InputCtr[39:32]							
PB8	InputCtr[31:24]							
PB9	InputCtr[23:16]							
PB10	InputCtr[15:08]							
PB11	InputCtr[07:00]							
PB12~PB31	Reserved							

Bit1	Bit0	Description
0	0	Audio
0	1	Video
1	0	Reserved
1	1	Reserved

Enc	Description
0	Encryption disable
1	Encryption disable

HDCP	HDCP	Description
010	010	HDCP2.2

[103]

[104] Each field is described below.

[105] Enc (1bit) indicates whether encryption is enabled or disabled. If Enc is 0, HDCP Encryption for a corresponding frame is disabled, or if Enc is 1, HDCP Encryption for a corresponding frame is enabled.

[106] HDCP major version (3 bits) indicates a major version of HDCP.

[407] HDCP minor version (3 bits) indicates a minor version of HDCP.

[108] In HDCP x.y, x indicates a major version, and y indicates a minor version. For example, in HDCP 2.0, x is 2, and y is 0. In the third exemplary embodiment, both HDCP major version and HDCP minor version are 2 so that HDCP version becomes 2.2.

[109] The fourth exemplary embodiment

[110] Unlike the aforementioned exemplary embodiments, audio and video may be defined as different packets as shown in Tables 6 and 7 below. For example, audio CPSP and video CPSP may be identified by 0x0B and 0x0C, respectively.

[111]

[112] <Table 6>

[113] Audio CP sync. Packet Format

Byte#	7	6	5	4	3	2	1	0
HB0	Packet Type(0x0B)							
HB1	Reserved							
HB2	Reserved							
PB0	audiostreamCtr[31:24]							
PB1	audiostreamCtr[23:16]							
PB2	audiostreamCtr[15:08]							
PB3	audiostreamCtr[07:00]							
PB4	audioInputctr[63:56]							
PB5	audioInputctr[55:48]							
PB6	audioInputctr[47:40]							
PB7	audioInputctr[39:32]							
PB8	audioInputctr[31:24]							
PB9	audioInputctr[23:16]							
PB10	audioInputctr[15:08]							
PB11	audioInputctr[07:00]							
PB12~PB31	Reserved							

[114]

[115]

[116] <Table 7>

[117] Video CP Sync. Packet Format

Byte#	7	6	5	4	3	2	1	0
HB0	Packet Type(0x0C)							
HB1	Reserved							
HB2	Reserved							
PB0	videoStreamCtr[31:24]							
PB1	videoStreamCtr[23:16]							
PB2	videoStreamCtr[15:08]							
PB3	videoStreamCtr[07:00]							
PB4	videoInputctr[63:56]							
PB5	videoInputctr[55:48]							
PB6	videoInputctr[47:40]							
PB7	videoInputctr[39:32]							
PB8	videoInputctr[31:24]							
PB9	videoInputctr[23:16]							
PB10	videoInputctr[15:08]							
PB11	videoInputctr[07:00]							
PB12~31	Reserved							

[118]

[119] Description of each field is the same as in the first exemplary embodiment.

[120] In the present general inventive concept, it is possible to transmit a parameter value used for encryption of audio and video signals of HDCP using at least one of the packets defined in the exemplary embodiments above.

[121] CPSP is included in a transmission frame constituting a transfer stream. CPSP may be transmitted prior to a transmission frame. Transmission timing of CPSP is explained

below.

[122] Transmission period of CPSP

[123] FIGs. 5 and 6 illustrate a transmission period of CPSP.

[124] With reference to FIG. 5, a CPSP may be transmitted between an active edge period and a keep out period of a vertical synchronizing signal (vsync). For example, in an exemplary embodiment shown in FIG. 5, a CPSP may be transmitted between clock 0 and clock 508. A CPSP should not collide with other packets which are previously defined and transmitted.

[125] In FIG. 5, if a keep_out signal is enabled, the CPSP cannot be transmitted any longer and a source device performs operation for preparation of encryption such as generation of a frame key. A sink device performs an operation for decoding. When the keep_out signal is enabled, no packet is permitted to be transmitted until the keep_out signal is disabled. In this period the encryption and decryption can be performed.

[126] In the source device, an encryption enable signal (enc_en/enc_dis) is transmitted in a clock signal period, and a random number which is a result value of encrypting each line of the transmission frame is output from a time point when a data enable signal is transmitted. In other words, this period may be a period from a time point when a win_of_opp signal is disabled until a time point when the win_of_opp signal is enabled again in the clock signal period.

[127] Further, with reference to FIG. 6, in a clock signal period, a CPSP may be transmitted between a time point when a transmission period of a general control packet finishes and a time point when a keep_out signal is enabled. In an exemplary embodiment shown in FIG. 6, a CPSP may be transmitted between clock 384 and clock 508. As in FIG. 5, a CPSP should not collide with other packets which are previously defined and transmitted such as a general control packet.

[128] Fundamentally, HDCP 2.x performs encryption from a time point when an encryption enable signal (enc_en/enc_dis) is transmitted, and encrypts the entire frames to be transmitted. Accordingly, after the first frame is encrypted, all the subsequent frames may be encrypted. By the way, since every frame includes a CPSP, all the CPSPs after the first frame are encrypted and transmitted.

[129] However, it may be inefficient to encrypt the CPSPs included in all the frames starting from the second frame in consideration of the purpose of CPSP of transmitting a parameter for encryption. Accordingly, as an alternative to the present general inventive concept, encryption may not be performed from a time point when a vertical synchronizing signal (vsync) is enabled until a time point when a keep_out signal is enabled. That is, in a clock signal period, encryption may be performed in a period excluding the period between a time point when a vertical synchronizing signal (vsync)

is enabled and a time point when a keep_out signal is enabled. In this case, the CPSPs of all the frames are not encrypted.

[130] Whether to encrypt a transmission frame is determined based on an encryption status signal value (ex. EESS: Enhance Encryption Status Signaling) which is displayed in a period when a win_of_opp signal is transmitted. According to the EESS, an encryption enable signal (enc_en/enc_dis) determines whether encryption is applied to a current frame (enc_en) or not (enc_dis). That is, a win_of_opp signal informs whether to encrypt a subsequent frame. Thus, it is determined whether to perform encryption.

[131] Table 8 shows a table of EESS.

[132]

[133] <Table 8>

[134]

CTL3:	CTL2:	CTL1:	CTL0:	Description
1	0	0	1	Encryption is enabled for this frame.
0	0	0	1	Encryption is disabled for this framw.

Enhanced Encryption Status Signaling(EESS)

[135]

[136] Partial Encryption

[137] If there is a large amount of resource of audio and video signals to be transmitted, high-speed data transmission becomes difficult and it may be a burden to support audio and video having a large transmission quantity in terms of security. To solve this problem, partial encryption may be considered. For example, video stream bit encryption of 24 bits may be a standard.

[138] In addition, in color coordinate, only some bits may be encrypted instead of 8-bit encryption of each color. For example, the most significant 4 bits from among 8 bits may be encrypted, or 4bits may be encrypted at random.

[139] Partial encryption information may be transmitted to a sink device in the authentication period.

[140] Partial encryption may be performed by scrambling some bits from among Red[7:0], Green[7:0], and Blue[7:0] of video stream bits of HDMI Transition Minimized Differential Signaling (TMDS).

[141] For example, the most significant 4 bits of each TMDS channel may be scrambled or all bits (8 bits) of a TMDS channel may be scrambled.

[142] FIG. 7 illustrates transmission and reception of a partially encrypted TMDS signal between an HDCP transmitter and an HDCP receiver.

[143] As illustrated in FIG. 7, the HDCP transmitter encrypts some or all of the bits of a color coordinate and transmits an encrypted TMDS to the HDCP receiver. The HDCP receiver receives and decrypts the encrypted TMDS.

[144] Table 9 below shows bit match of a TMDS channel and a video stream.

[145]

[146] <Table 9>

[147]

Cipher Output	T.M.D.S Channel	Video stream bits
23:16	2	Red[7:0]
15:8	1	Green[7:0]
7:0	0	Blue[7:0]

Encryption stream Mapping

[148]

[149] In TMDS, a bit scrambling position may be diverse. Table 10 below shows an example.

[150]

[151] <Table 10>

[152]

Scrambling Position(3 bits)	Description
0x0	The whole 24-bits (default, n=24)
0x1	MSB 4 bits of each video stream bit (n=12)
0x2	Channel 1 (n=8)
0x3~0x7	Reserved

[153]

[154] As shown in Table 10, 0~2 bits correspond to a method of scrambling each bit. If bit 0x0 is 1, all the bits are scrambled. If bit 0x1 is 1, the most significant 4 bits of each video stream bit are scrambled. If bit 0x2 is 1, only channel 1 is scrambled.

[155] In the HDMI authentication process, a source device and a sink device share information about a scrambling point of video data. More specifically, a source device encrypts scrambling point information using a master key (Km) and a session key (Ks) and

transmits the information to a sink device. The master key (Km) and the session key (Ks) are described in specifications of HDCP 1.x and HDCP 2.x.

[156] Hereinbelow, a sink device, a source device, and a data transceiving system consisting of the sink device and the source device are described according to an exemplary embodiment.

[157] FIG. 8 is a block diagram illustrating a configuration of a data transceiving system 1000 consistent with an exemplary embodiment.

[158] As illustrated in FIG. 8, the data transceiving system 1000 consistent with an exemplary embodiment may include a source device 100 and a sink device 200.

[159] The source device 100 reads out EDID from the sink device 200 and determines whether interface version information contained in the EDID coincides with version information of an interface provided by the source device 100. If the version in-

formation coincides with each other, the source device 100 generates a packet including encryption information of a content stream and transmits the packet to the sink device 200.

[160] The sink device 200 receives and parses the packet.

[161] In this case, the packet may include the first field for indicating identification information of the content stream, and the second field for indicating an encryption parameter value of the content stream.

[162] FIG. 9 is a block diagram illustrating a configuration of a data transmitter 100 consistent with an exemplary embodiment .

[163] With reference to FIG. 9, the data transmitter 100 may include a packet generating unit 110 and a transmitting unit 120. The data transmitter also may include a memory and a processor to assist in performing the operations described in detail below.

[164] The packet generating unit 110 generates a packet including encryption information of a content stream.

[165] The transmitting unit 120 transmits the generated packet to a data receiver 200.

[166] The generated packet may include the first field for indicating identification information of the content stream, and the second field for indicating an encryption parameter value of the content stream. Detailed composition and a transmission period of the packet has been described above.

[167] FIG. 10 is a block diagram illustrating a configuration of a data receiver 200 consistent with an exemplary embodiment of the present invention.

[168] With reference to FIG. 10, the data receiver 200 may include a receiving unit 210 and a packet parsing unit 220. The data receiver also may include a memory and a processor to assist in performing the operations described in detail below.

[169] The receiving unit 210 receives a packet including encryption information of a content stream from the data transmitter 100.

[170] The packet parsing unit 220 parses the received packet.

[171] The received packet may include the first field for indicating identification information of the content stream, and the second field for indicating an encryption parameter value of the content stream. Detailed composition and transmission period of the packet has been described above.

[172] Hereinbelow, a data transmitting method and a data receiving method consistent with an exemplary embodiment are described. A data transceiving method has been described above with reference to FIG. 4, and thus is not repeated here.

[173] FIG. 11 is a flow chart illustrating a data transmitting method consistent with an exemplary embodiment, and FIG. 12 is a flow chart illustrating a data receiving method consistent with an exemplary embodiment.

[174] With reference to FIG. 11, the data transmitting method may include generating a

packet including encryption information of a content stream in operation S1110, and transmitting the generated packet to a data receiver in operation S1120. The generated packet may include at least one of the first field for indicating identification information of the content stream, and the second field for indicating an encryption parameter value of the content stream. Detailed composition, transmission period, and operations of the packet have been described above.

[175] With reference to FIG. 12, the data receiving method may include receiving a packet including encryption information of a content stream from a data transmitter in operation S1210, and parsing the received packet in operation S1120. The received packet may include at least one of the first field for indicating identification information of the content stream, and the second field for indicating an encryption parameter value of the content stream. Detailed composition, transmission period, and operations of the packet have been described above.

[176] The foregoing exemplary embodiments and advantages are merely exemplary and are not to be construed as limiting the present invention. The present teaching can be readily applied to other types of apparatuses. Also, the description of the exemplary embodiments is intended to be illustrative, and not to limit the scope of the claims, and many alternatives, modifications, and variations will be apparent to those skilled in the art.

Claims

- [Claim 1] A data transmitter comprising:
a packet generator configured to generate a packet including encryption information of a content stream; and
a transmitter which transmits the generated packet to a data receiver, wherein the generated packet comprises a first field for indicating identification information of the content stream, and a second field for indicating a first encryption parameter value of the content stream.
- [Claim 2] The data transmitter as claimed in claim 1, wherein the second field comprises at least from among a first sub-field for indicating a second encryption parameter value to distinguish the content stream, and a second sub-field for indicating a third encryption parameter value for link synchronization between the data transmitter and the data receiver.
- [Claim 3] The data transmitter as claimed in claim 2, wherein the third encryption parameter value for link synchronization is a value obtained by adding a number of lines of a transmission frame to a fourth encryption parameter value for link synchronization included in a previous packet of the generated packet.
- [Claim 4] The data transmitter as claimed in claim 1, wherein the generated packet is transmitted between a time point when a vertical synchronizing signal is enabled and a time point when a keep_out signal is enabled, in a clock signal period.
- [Claim 5] The data transmitter as claimed in claim 1, wherein the generated packet is transmitted between a time point when a transmission period of a general control packet finishes and a time point when a keep_out signal is enabled, in a clock signal period.
- [Claim 6] The data transmitter as claimed in claim 1, wherein the generated packet is included in a transmission frame of the content stream and is transmitted, and
in a clock signal period, an encryption enable signal (enc_en/enc_dis) is transmitted and a result value of encrypting each line of the transmission frame is output from a time point when a data enable signal is transmitted.
- [Claim 7] The data transmitter as claimed in claim 1, wherein the generated packet is included in a transmission frame of the content stream and is transmitted, and
in a clock signal period, a result value of encrypting each line of the

transmission frame is output between a time point when a win_of_opp signal is disabled and a time point when the win_of_opp signal is enabled again.

[Claim 8] The data transmitter as claimed in claim 6, wherein whether to enable or disable the encryption enable signal is determined according to a win_of_opp signal in a period when a keep_out signal is enabled in the clock signal period.

[Claim 9] The data transmitter as claimed in claim 1, wherein the generated packet is included in a transmission frame of the content stream, and is transmitted, and
in a clock signal period, a transmission frame of the content stream is encrypted in a period excluding a period between a time point when a vertical synchronizing signal (vsync) is enabled and a time point when a keep_out signal is enabled.

[Claim 10] A data receiver comprising:
a receiver configured to receive a packet including encryption information of a content stream from a data transmitter; and
a packet parser configured to parse the received packet,
wherein the received packet comprises a first field for indicating identification information of the content stream, and a second field for indicating a first encryption parameter value of the content stream.

[Claim 11] The data receiver as claimed in claim 10, wherein the second field comprises at least one from among a first sub-field for indicating a second encryption parameter value to distinguish the content stream, and a second sub-field for indicating a third encryption parameter value for link synchronization between the data transmitter and the data receiver.

[Claim 12] The data receiver as claimed in claim 11, wherein the data receiver determines whether a value obtained by adding a number of lines of a transmission frame to a fourth encryption parameter value for link synchronization included in a previous packet of the received packet coincides with the third encryption parameter value for link synchronization included in the second field.

[Claim 13] The data receiver as claimed in claim 10, wherein the received packet is transmitted between a time point when a vertical synchronizing signal is enabled and a time point when a keep_out signal is enabled, in a clock signal period.

[Claim 14] The data receiver as claimed in claim 10, wherein the received packet is

included in a transmission frame of the content stream and is transmitted, and
in a clock signal period, an encryption enable signal (enc_en/enc_dis) is transmitted and a result value of encrypting each line of the transmission frame is output from a time point when a data enable signal is transmitted.

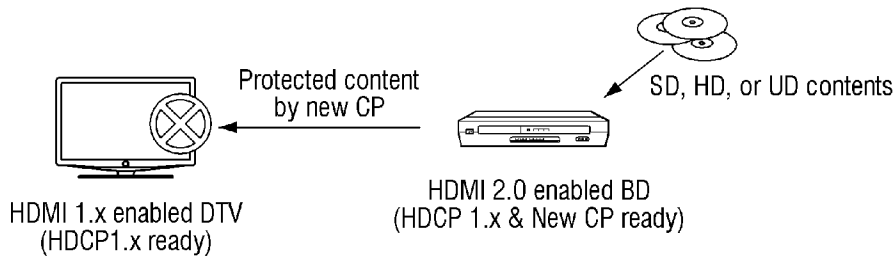
[Claim 15]

A data transceiving system comprising:

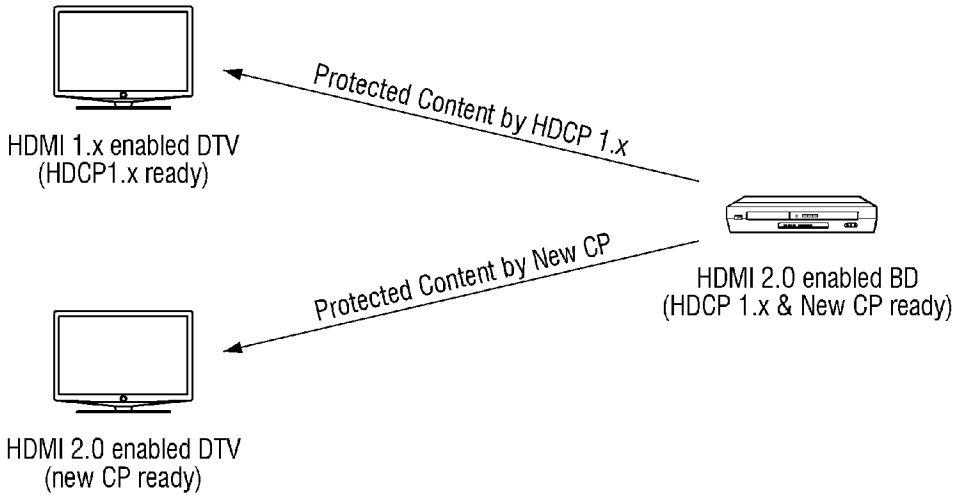
a source device which reads out Extended Display Identification Data (EDID) from a sync device, and if interface version information included in the EDID coincides with version information of an interface provided by the source device, generates a packet including encryption information of a content stream and transmits the generated packet to the sync device; and

the sync device which receives and parses the transmitted packet, wherein the transmitted packet comprises at least one from among a first field for indicating identification information of the content stream, and a second field for indicating an encryption parameter value of the content stream.

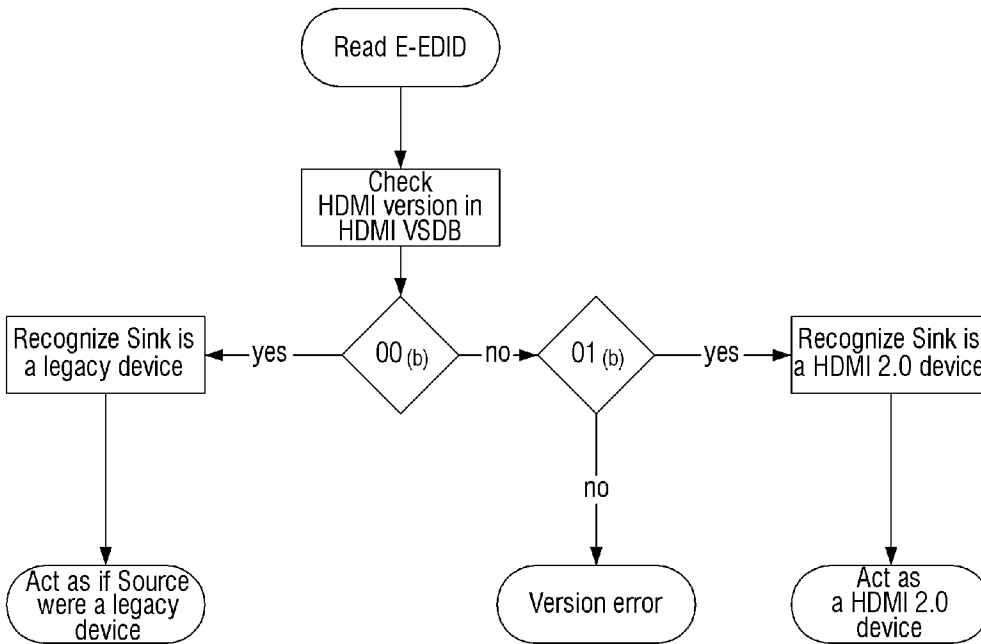
[Fig. 1]



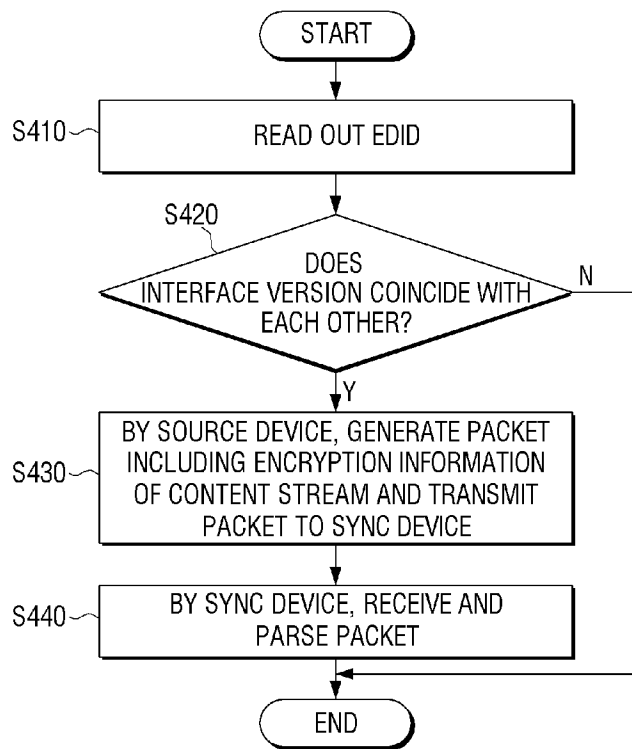
[Fig. 2]



[Fig. 3]



[Fig. 4]



[Fig. 5]

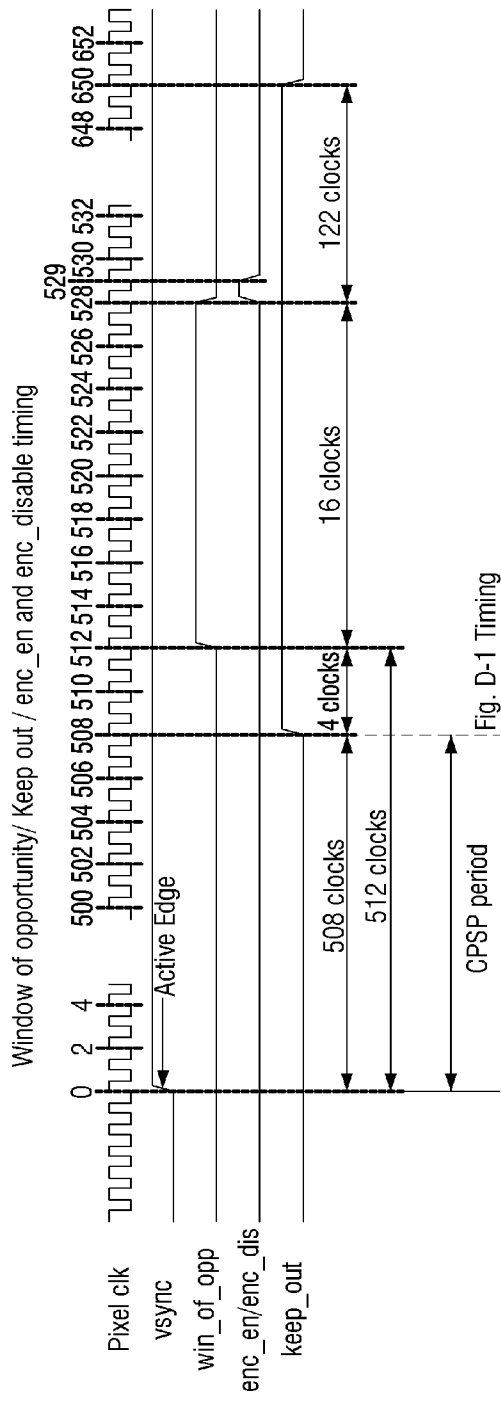


Fig. D-1 Timing

[Fig. 6]

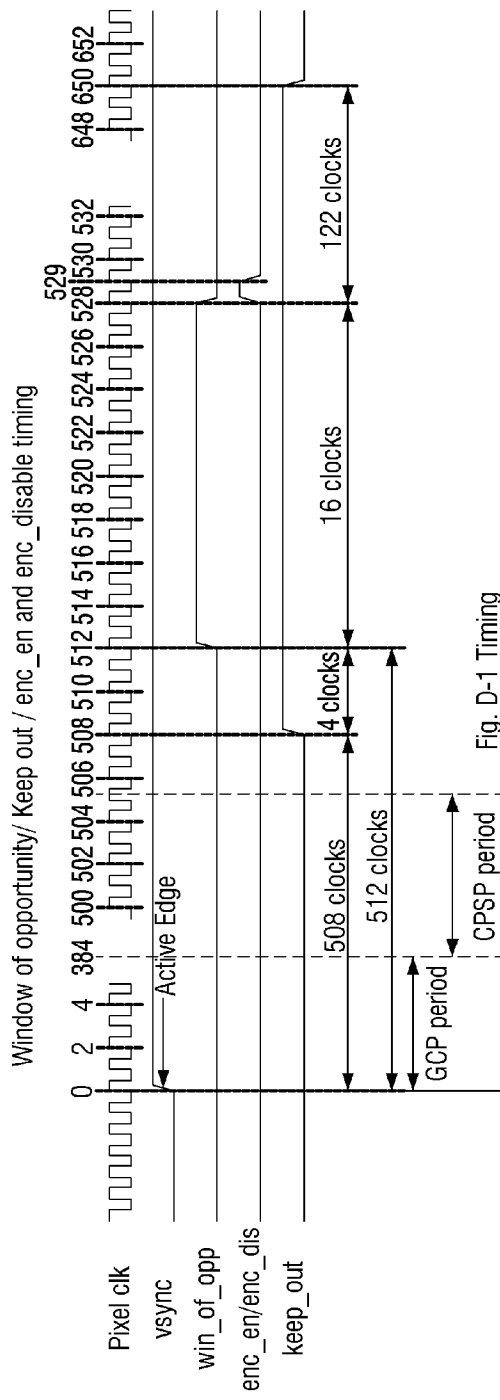
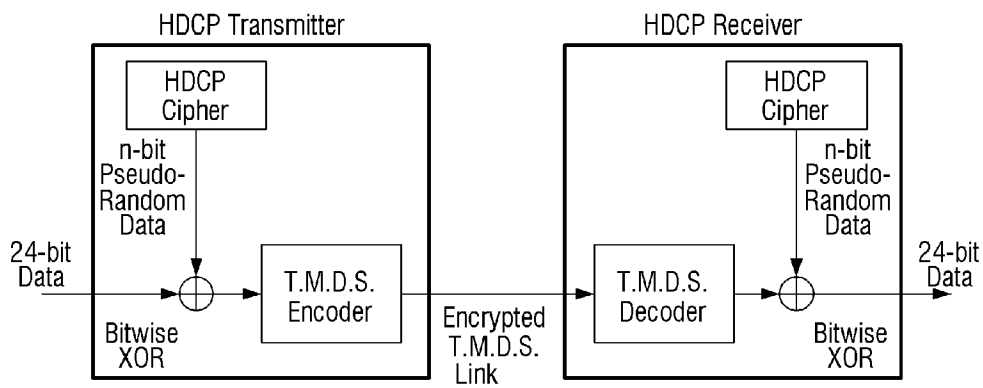


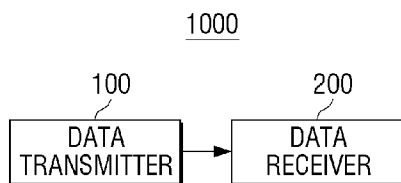
Fig. D-1 Timing

[Fig. 7]

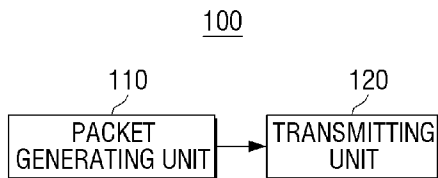
note: $4 \leq n \leq 24$

HDCP Encryption and Decryption

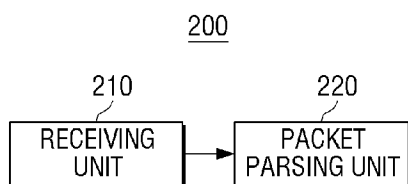
[Fig. 8]



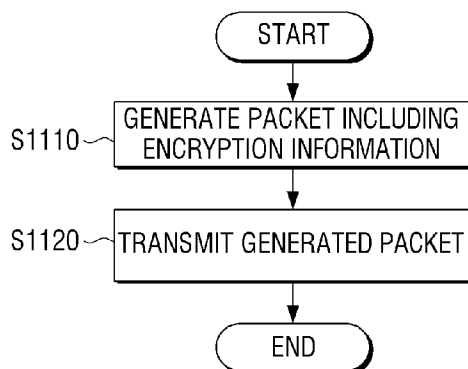
[Fig. 9]



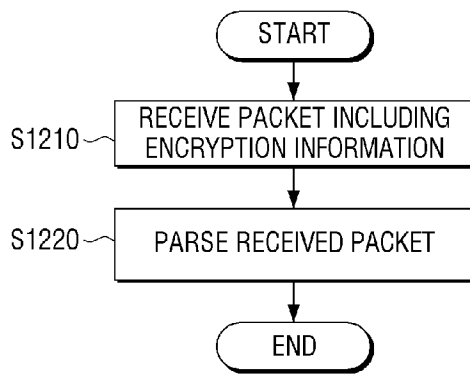
[Fig. 10]



[Fig. 11]



[Fig. 12]



A. CLASSIFICATION OF SUBJECT MATTER**H04L 12/70(2013.01)i, H04L 9/12(2006.01)i**

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)

H04L 12/70; G06F 12/02; H04J 3/06; H04N 7/167; H04L 12/26; H04N 7/00; G06F 3/12; H04N 5/445

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

Korean utility models and applications for utility models

Japanese utility models and applications for utility models

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

eKOMPASS(KIPO internal) & Keywords: HDMI, packet, encryption, EDID, synchronization

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	US 2007-0091359 A1 (HIROYUKI SUZUKI et al.) 26 April 2007 See paragraphs 31, 40, 152, 213; and figure 2.	1, 10
Y		15
A		2-9, 11-14
Y	US 2012-0008044 A1 (SHIGETAKA NAGATA et al.) 12 January 2012 See paragraphs 49, 50, 52, 66; and figure 2.	15
A	US 2008-0013725 A1 (OSAMU KOBAYASHI et al.) 17 January 2008 See paragraphs 24, 30; and figure 1.	1-15
A	US 2009-0027409 A1 (MING-CHIH KAO et al.) 29 January 2009 See paragraphs 20, 36; and figures 1, 3.	1-15
A	US 2010-0260055 A1 (JON JAMES ANDERSON et al.) 14 October 2010 See paragraphs 208, 226; and figure 6.	1-15

 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 application or patent 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 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

07 June 2013 (07.06.2013)

Date of mailing of the international search report

10 June 2013 (10.06.2013)

Name and mailing address of the ISA/KR


 Korean Intellectual Property Office
 189 Cheongsa-ro, Seo-gu, Daejeon Metropolitan City,
 302-701, Republic of Korea

Facsimile No. 82-42-472-7140

Authorized officer

BYUN, Sung Cheal

Telephone No. 82-42-481-8262



INTERNATIONAL SEARCH REPORT

Information on patent family members

International application No.

PCT/KR2013/001052

Patent document cited in search report	Publication date	Patent family member(s)	Publication date		
US 2007-0091359 A1	26.04.2007	CN 1946080 A	11.04.2007		
		CN 1946080 B	03.11.2010		
		EP 1773060 A2	11.04.2007		
		EP 1773060 A3	09.01.2013		
		JP 04581955 B2	10.09.2010		
		JP 2007-104236 A	19.04.2007		
		KR 10-2007-0037994 A	09.04.2007		
		US 2012-0096260 A1	19.04.2012		
		US 2013-0067223 A1	14.03.2013		
		US 8098388 B2	17.01.2012		
		US 8363258 B2	29.01.2013		
		US 2012-0008044 A1	12.01.2012	WO 2010-073299 A1	01.07.2010
		US 2008-0013725 A1	17.01.2008	CN 101304420 A	12.11.2008
CN 1607793 A	20.04.2005				
EP 1519581 A1	30.03.2005				
EP 1990999 A2	12.11.2008				
EP 1990999 A3	06.05.2009				
JP 2005-110248 A	21.04.2005				
JP 2008-283688 A	20.11.2008				
KR 10-2005-0030877 A	31.03.2005				
KR 10-2008-0100122 A	14.11.2008				
SG 148090 A1	31.12.2008				
TW 200910960 A	01.03.2009				
US 2005-0069130 A1	31.03.2005				
US 2010-0046751 A1	25.02.2010				
US 7613300 B2	03.11.2009				
US 7634090 B2	15.12.2009				
US 8385544 B2	26.02.2013				
US 2009-0027409 A1	29.01.2009	TW 200905661 A	01.02.2009		
		US 8269785 B2	18.09.2012		
US 2010-0260055 A1	14.10.2010	CA 2548412 A1	23.06.2005		
		CA 2548412 C	19.04.2011		
		CA 2731265 A1	23.06.2005		
		CA 2731269 A1	23.06.2005		
		CA 2731363 A1	23.06.2005		
		CN 101867516 A	20.10.2010		
		CN 102394895 A	28.03.2012		
		CN 102497368 A	13.06.2012		
		CN 1914875 A	14.02.2007		
		EP 1698146 A1	06.09.2006		
		EP 2247068 A1	03.11.2010		
		EP 2247069 A1	03.11.2010		
		EP 2247070 A1	03.11.2010		
		EP 2247071 A1	03.11.2010		
		EP 2247072 A1	03.11.2010		

INTERNATIONAL SEARCH REPORT

Information on patent family members

International application No.

PCT/KR2013/001052

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
		EP 2247075 A1	03.11.2010
		JP 04902355 B2	13.01.2012
		JP 05043968 B2	20.07.2012
		JP 2007-513591 A	24.05.2007
		JP 2010-183593 A	19.08.2010
		KR 10-0906319 B1	06.07.2009
		US 2005-0204057 A1	15.09.2005
		WO 2005-057881 A1	23.06.2005