

(19) 日本国特許庁(JP)

(12) 公開特許公報(A)

(11) 特許出願公開番号

特開2014-147065

(P2014-147065A)

(43) 公開日 平成26年8月14日(2014.8.14)

(51) Int.Cl.	F I	テーマコード (参考)
HO4N 21/4363 (2011.01)	HO4N 21/4363	5C164
HO4N 21/4402 (2011.01)	HO4N 21/4402	

審査請求 未請求 請求項の数 15 O L (全 21 頁)

<p>(21) 出願番号 特願2014-10982(P2014-10982)</p> <p>(22) 出願日 平成26年1月24日(2014.1.24)</p> <p>(31) 優先権主張番号 61/757,361</p> <p>(32) 優先日 平成25年1月28日(2013.1.28)</p> <p>(33) 優先権主張国 米国(US)</p> <p>(31) 優先権主張番号 10-2013-0042464</p> <p>(32) 優先日 平成25年4月17日(2013.4.17)</p> <p>(33) 優先権主張国 韓国(KR)</p>	<p>(71) 出願人 390019839 三星電子株式会社 Samsung Electronics Co., Ltd. 大韓民国京畿道水原市靈通区三星路129 129, Samsung-ro, Yeongtong-gu, Suwon-si, Gyeonggi-do, Republic of Korea</p> <p>(74) 代理人 100107766 弁理士 伊東 忠重</p> <p>(74) 代理人 100070150 弁理士 伊東 忠彦</p> <p>(74) 代理人 100091214 弁理士 大貫 進介</p>
---	--

最終頁に続く

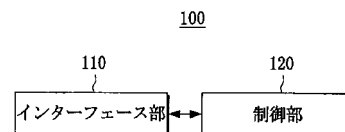
(54) 【発明の名称】 ソースデバイス、そのコンテンツ提供方法、シンクデバイス及びその制御方法

(57) 【要約】 (修正有)

【課題】 コンテンツに適用されるHDCPバージョンがシンクデバイスで対応していない場合、シンクデバイスで対応するHDCPバージョンで暗号化できるようにコンテンツを変換して提供。

【解決手段】 ソースデバイスは、シンクデバイスとHDCP認証を行うインターフェース部と、シンクデバイスで対応するHDCPバージョンを判断し、コンテンツに適用されるHDCPバージョンがシンクデバイスで未対応と判断されると、シンクデバイスで対応するHDCPバージョンで暗号化できるようにコンテンツを変換し、変換されたコンテンツをシンクデバイスで対応するHDCPバージョンで暗号化し、シンクデバイスに伝送するようにインターフェース部を制御する制御部とを含む。

【選択図】 図2



【特許請求の範囲】**【請求項 1】**

シンクデバイスにコンテンツを送信するソースデバイスにおいて、
前記シンクデバイスとHDCP (High-bandwidth Digital Content Protection) 認証を行うインターフェース部と、
前記シンクデバイスで対応する (Support) HDCP (High-bandwidth Digital Content Protection) バージョンを判断し、
前記コンテンツに適用されるHDCPバージョンが前記シンクデバイスで未対応 (Unsupported) と判断されると、前記シンクデバイスで対応するHDCPバージョンで暗号化できるように前記コンテンツを変換し、前記変換されたコンテンツを前記シンクデバイスで対応するHDCPバージョンで暗号化し、前記シンクデバイスに送信するように前記インターフェース部を制御する制御部と
を含むソースデバイス。

10

【請求項 2】

前記コンテンツは、第1HDCPバージョンで暗号化すべきプレミアムコンテンツであり、
前記シンクデバイスで対応するHDCPバージョンは、前記第1HDCPバージョンより低い第2HDCPバージョンであることを特徴とする請求項1に記載のソースデバイス。

【請求項 3】

前記制御部は、
ダウンスケーリングを通じて前記コンテンツの解像度を低下させて、前記シンクデバイスで対応するHDCPバージョンで暗号化できるように前記コンテンツを変換することを特徴とする請求項2に記載のソースデバイス。

20

【請求項 4】

前記制御部は、
前記シンクデバイスで対応するHDCPバージョン及び前記コンテンツに適用されるHDCPバージョンのそれぞれで定義された方式に応じて、前記シンクデバイスとHDCP認証実行ができるか否かに基づいて、前記シンクデバイスが対応するHDCPバージョンを判断することを特徴とする請求項1に記載のソースデバイス。

30

【請求項 5】

前記制御部は、
前記シンクデバイスに予め保存されたHDCPバージョンに関する情報の伝送を要求し、前記シンクデバイスから受信されたHDCPバージョンに関する情報に基づいて、前記シンクデバイスが対応するHDCPバージョンを判断することを特徴とする請求項1に記載のソースデバイス。

【請求項 6】

前記制御部は、
前記コンテンツに適用されるHDCPバージョンが前記シンクデバイスで対応すると判断されると、前記コンテンツに適用されるHDCPバージョンで前記コンテンツを暗号化し、前記シンクデバイスに送信することを特徴とする請求項1に記載のソースデバイス。

40

【請求項 7】

前記制御部は、
前記変換されたコンテンツを前記シンクデバイスに送信する場合、前記コンテンツが変換されたことを示すメッセージを出力するように前記シンクデバイスを制御することを特徴とする請求項1に記載のソースデバイス。

【請求項 8】

ソースデバイスから提供されるコンテンツを出力するシンクデバイスにおいて、
前記ソースデバイスとHDCP (High-bandwidth Digital Content Protection) 認証を行うインターフェース部と、

50

前記ソースデバイスから前記シンクデバイスで対応するHDCPバージョンに関する情報の要求が受信されると、予め保存された前記シンクデバイスで対応するHDCPバージョンに関する情報を前記ソースデバイスに伝送するように前記インターフェース部を制御する制御部と

を含むシンクデバイス。

【請求項9】

前記シンクデバイスで対応するHDCPバージョンに関する情報をEDID(Extended Display Identification Data)フォーマットで保存する保存部を更に含むことを特徴とする請求項8に記載のシンクデバイス。

【請求項10】

シンクデバイスにコンテンツを伝送するソースデバイスのコンテンツ伝送方法において、

前記シンクデバイスで対応するHDCP(High-bandwidth Digital Content Protection)バージョンを判断するステップと、

前記コンテンツに適用されるHDCPバージョンが前記シンクデバイスで未対応(Unsupported)と判断されると、前記シンクデバイスで対応するHDCPバージョンで暗号化できるように前記コンテンツを変換するステップと、

前記変換されたコンテンツを前記シンクデバイスで対応するHDCPバージョンで暗号化し、前記シンクデバイスに伝送するステップと

を含むコンテンツ伝送方法。

【請求項11】

前記コンテンツは、第1HDCPバージョンで暗号化すべきプレミアムコンテンツであり、

前記シンクデバイスで対応するHDCPバージョンは、前記第1HDCPバージョンより低い第2HDCPバージョンであることを特徴とする請求項10に記載のコンテンツ伝送方法。

【請求項12】

前記変換するステップは、

ダウンスケーリングを通じて前記コンテンツの解像度を低下させて、前記シンクデバイスで対応するHDCPバージョンで暗号化できるように前記コンテンツを変換することを特徴とする請求項11に記載のコンテンツ伝送方法。

【請求項13】

前記判断するステップは、

前記シンクデバイスで対応するHDCPバージョン及び前記コンテンツに適用されるHDCPバージョンのそれぞれで定義された方式に応じて、前記シンクデバイスとHDCP認証実行ができるか否かに基づいて、前記シンクデバイスが対応するHDCPバージョンを判断することを特徴とする請求項10に記載のコンテンツ伝送方法。

【請求項14】

ソースデバイスから提供されるコンテンツを出力するシンクデバイスの制御方法において、

前記ソースデバイスから前記シンクデバイスで対応するHDCP(High-bandwidth Digital Content Protection)バージョンに関する情報の要求を受信するステップと、

前記HDCPバージョンに関する情報の伝送要求が受信されると、予め保存された前記シンクデバイスで対応するHDCPバージョンに関する情報を前記ソースデバイスに伝送するステップと

を含む制御方法。

【請求項15】

前記シンクデバイスは、

前記シンクデバイスで対応するHDCPバージョンに関する情報をEDID(Extended

10

20

30

40

50

nded Display Identification Data)フォーマットで保存することを特徴とする請求項14に記載の制御方法。

【発明の詳細な説明】

【技術分野】

【0001】

本発明は、ソースデバイス、そのコンテンツ提供方法、シンクデバイス及びその制御方法に関し、より詳細には、HDMI(登録商標)を通じて接続されてHDCP認証を行うソースデバイス、そのコンテンツ提供方法、シンクデバイス及びその制御方法に関する。

【背景技術】

【0002】

最近、高品質の映像及びオーディオを記録及び再生するための記録媒体として、DVD、ブルーレイディスク等が主流となっており、なお、高画質の映像のディスプレイが可能な多様なディスプレイ装置が広く普及されている。

【0003】

よって、記録媒体にコンテンツを記録したり再生する各種DVDプレーヤ、ブルーレイプレーヤとデジタルテレビを接続して使用する例が増加しており、これらの装備間のデータ伝送のためのデジタルインターフェースとしてHDMI(High-speed Multimedia Interface)が使用されている。

【0004】

このようなHDMIを対応する(Support)機器は、高解像度の映像及びオーディオを提供し、コンテンツの複製防止のためのHDCP(High-bandwidth Digital Content Protection)を対応する。

【0005】

なお、最近のコンテンツ提供者は、4kのコンテンツ、Full HDの3Dコンテンツ等の高解像度コンテンツを提供するうえで、これらをプレミアムコンテンツに分類し、HDCP 2.2バージョンを適用しようとする動きがある。それにより、HDCP 2.2バージョン以下のバージョンのみを対応していた既存のディスプレイ装置は、HDCP 2.2バージョンが適用される高解像度コンテンツと互換性を有することができないという問題点があった。

【先行技術文献】

【特許文献】

【0006】

【特許文献1】韓国特許第1099311号

【発明の概要】

【発明が解決しようとする課題】

【0007】

そこで、本発明は、上記問題に鑑みてなされたものであり、本発明の目的とするところは、コンテンツに適用されるHDCPバージョンがシンクデバイスで対応していない(Unsupported)場合、シンクデバイスで対応するHDCPバージョンで暗号化ができるようにコンテンツを変換して提供することができるソースデバイス、そのコンテンツ提供方法、シンクデバイス及びその制御方法を提供することにある。

【課題を解決するための手段】

【0008】

以上のような目的を達成するための本発明の一実施形態に係るシンクデバイスにコンテンツを送るソースデバイスは、前記シンクデバイスとHDCP(High-bandwidth Digital Content Protection)認証を行うインターフェース部と、前記シンクデバイスで対応する(Support)HDCP(High-bandwidth Digital Content Protection)バージョンを判断し、前記コンテンツに適用されるHDCPバージョンが前記シンクデバイスで未対応(Unsupported)と判断されると、前記シンクデバイスで対応する

10

20

30

40

50

HDCPバージョンで暗号化できるように前記コンテンツを変換し、前記変換されたコンテンツを前記シンクデバイスで対応するHDCPバージョンで暗号化し、前記シンクデバイスに伝送するように前記インターフェース部を制御する制御部とを含む。

【0009】

ここで、前記コンテンツは、第1HDCPバージョンで暗号化すべきプレミアムコンテンツであり、前記シンクデバイスで対応するHDCPバージョンは、前記第1HDCPバージョンより低い第2HDCPバージョンであってよい。

【0010】

なお、前記制御部は、ダウンスケリングを通じて前記コンテンツの解像度を低下させて、前記シンクデバイスで対応するHDCPバージョンで暗号化できるように前記コンテンツを変換してよい。

10

【0011】

そして、前記制御部は、前記シンクデバイスで対応するHDCPバージョン及び前記コンテンツに適用されるHDCPバージョンのそれぞれで定義された方式に応じて、前記シンクデバイスとHDCP認証実行ができるか否かに基づいて、前記シンクデバイスが対応するHDCPバージョンを判断してよい。

【0012】

なお、前記制御部は、前記シンクデバイスに予め保存されたHDCPバージョンに関する情報の伝送を要求し、前記シンクデバイスから受信されたHDCPバージョンに関する情報に基づいて、前記シンクデバイスが対応するHDCPバージョンを判断してよい。

20

【0013】

そして、前記制御部は、前記コンテンツに適用されるHDCPバージョンが前記シンクデバイスで対応すると判断されると、前記コンテンツに適用されるHDCPバージョンで前記コンテンツを暗号化し、前記シンクデバイスに伝送してよい。

【0014】

なお、前記制御部は、前記変換されたコンテンツを前記シンクデバイスに伝送する場合、前記コンテンツが変換されたことを示すメッセージを出力するように前記シンクデバイスを制御してよい。

【0015】

一方、本発明の一実施形態に係るソースデバイスから提供されるコンテンツを出力するシンクデバイスは、前記ソースデバイスとHDCP(High-bandwidth Digital Content Protection)認証を行うインターフェース部と、前記ソースデバイスから前記シンクデバイスで対応するHDCPバージョンに関する情報の要求が受信されると、予め保存された前記シンクデバイスで対応するHDCPバージョンに関する情報を前記ソースデバイスに伝送するように前記インターフェース部を制御する制御部とを含む。

30

【0016】

ここで、本実施形態に係るシンクデバイスは、前記シンクデバイスで対応するHDCPバージョンに関する情報をEDID(Extended Display Identification Data)フォーマットで保存する保存部を更に含んでよい。

40

【0017】

一方、本発明の一実施形態に係るシンクデバイスにコンテンツを伝送するソースデバイスのコンテンツ伝送方法は、前記シンクデバイスで対応するHDCP(High-bandwidth Digital Content Protection)バージョンを判断するステップと、前記コンテンツに適用されるHDCPバージョンが前記シンクデバイスで未対応(Unsupported)と判断されると、前記シンクデバイスで対応するHDCPバージョンで暗号化できるように前記コンテンツを変換するステップと、前記変換されたコンテンツを前記シンクデバイスで対応するHDCPバージョンで暗号化し、前記シンクデバイスに伝送するステップとを含む。

【0018】

50

ここで、前記コンテンツは、第1 HDCPバージョンで暗号化すべきプレミアムコンテンツであり、前記シンクデバイスで対応するHDCPバージョンは、前記第1 HDCPバージョンより低い第2 HDCPバージョンであってよい。

【0019】

なお、前記変換するステップは、ダウンスケーリングを通じて前記コンテンツの解像度を低下させて、前記シンクデバイスで対応するHDCPバージョンで暗号化できるように前記コンテンツを変換してよい。

【0020】

そして、前記判断するステップは、前記シンクデバイスで対応するHDCPバージョン及び前記コンテンツに適用されるHDCPバージョンのそれぞれで定義された方式に応じて、前記シンクデバイスとHDCP認証実行ができるか否かに基づいて、前記シンクデバイスが対応するHDCPバージョンを判断してよい。

10

【0021】

なお、前記判断するステップは、前記シンクデバイスに予め保存されたHDCPバージョンに関する情報の伝送を要求し、前記シンクデバイスから受信されたHDCPバージョンに関する情報に基づいて、前記シンクデバイスが対応するHDCPバージョンを判断してよい。

【0022】

そして、本実施形態に係るコンテンツ伝送方法は、前記コンテンツに適用されるHDCPバージョンが前記シンクデバイスで対応すると判断されると、前記コンテンツに適用されるHDCPバージョンで前記コンテンツを暗号化し、前記シンクデバイスに伝送するステップを更に含んでよい。

20

【0023】

なお、本実施形態に係るコンテンツ伝送方法は、前記変換されたコンテンツを前記シンクデバイスに伝送する場合、前記コンテンツが変換されたことを示すメッセージを出力するように前記シンクデバイスを制御するステップを更に含んでよい。

【0024】

一方、本発明の一実施形態に係るソースデバイスから提供されるコンテンツを出力するシンクデバイスの制御方法は、前記ソースデバイスから前記シンクデバイスで対応するHDCP(High-bandwidth Digital Content Protection)バージョンに関する情報の要求を受信するステップと、前記HDCPバージョンに関する情報の伝送要求が受信されると、予め保存された前記シンクデバイスで対応するHDCPバージョンに関する情報を前記ソースデバイスに伝送するステップとを含む。

30

【0025】

ここで、前記シンクデバイスは、前記シンクデバイスで対応するHDCPバージョンに関する情報をEDID(Extended Display Identification Data)フォーマットで保存してよい。

【発明の効果】

【0026】

以上説明したように、本発明によれば、シンクデバイスがコンテンツに適用されるHDCPバージョンと異なるバージョンを対応するとしても、ソースデバイスは、コンテンツ変換を通じてシンクデバイスで対応するHDCPバージョンでコンテンツをシンクデバイスに提供することができる。それにより、既存のシンクデバイスとの互換性を維持することができるようになる。

40

【図面の簡単な説明】

【0027】

【図1】本発明の一実施形態に係るコンテンツ提供システムについて説明するための図である。

【図2】本発明の一実施形態に係るソースデバイスの構成について説明するためのブロッ

50

ク図である。

【図3】本発明の一実施形態に係るコンテンツをダウンスケーリングする方法の一例について説明するための図である。

【図4】本発明の一実施形態に係るソースデバイスの細部構成について説明するためのブロック図である。

【図5】本発明の一実施形態に係るシンクデバイスの構成について説明するためのブロック図である。

【図6】本発明の一実施形態に係るシンクデバイスの細部構成について説明するためのブロック図である。

【図7】本発明の一実施形態に係るコンテンツ提供システムの動作について説明するための図である。

10

【図8】本発明の一実施形態に係るコンテンツ提供システムの動作について説明するためのフローチャートである。

【図9】本発明の一実施形態に係るシンクデバイスにコンテンツを送送するソースデバイスのコンテンツ伝送方法について説明するためのフローチャートである。

【図10】本発明の一実施形態に係るソースデバイスから提供されるコンテンツを出力するシンクデバイスの制御方法について説明するためのフローチャートである。

【発明を実施するための形態】

【0028】

以下に添付図面を参照しながら、本発明の好適な実施形態について詳細に説明する。

20

【0029】

図1は、本発明の一実施形態に係るコンテンツ提供システムについて説明するための図である。図1によると、コンテンツ提供システムは、ソースデバイス100及びシンクデバイス200を含む。

【0030】

ここで、ソースデバイス100は、セットトップボックス、DVDプレーヤ、ブルーレイディスクプレーヤ、パソコン、ゲーム機等のように、シンクデバイス200にコンテンツを提供することができる多様な電子装置で実現され、シンクデバイス200は、テレビやパソコン等のように、ソースデバイス100から提供されるコンテンツを出力することができる多様な電子装置で実現されてよい。

30

【0031】

なお、ソースデバイス100とシンクデバイス200とは、HDMI(High-speed Multimedia Interface)に接続され、互いに通信を行うことができる。

【0032】

一方、ソースデバイス100とシンクデバイス200とは、コンテンツが不正コピーされることを防止するために、HDCP規格によるHDCP(High-bandwidth Digital Content Protection)認証を行うことができる。

【0033】

40

具体的に、デバイス100は、予め保存されたALS V(Key Select Vector of host device)によってコンテンツを暗号化してシンクデバイス200に伝送し、シンクデバイス200は予め保存されたBAS V(Key Select Vector of display device)によってコンテンツを復号化して出力することができる。

【0034】

一方、各デバイス100、200は、定められた時間に擬似ランダム値(Pseudo-Random Value)を生成する(仮に、ソースデバイス100が生成する擬似ランダム値は、 R_i 、シンクデバイス200が生成する擬似ランダム値は R_i')。そして、ソースデバイス100は、シンクデバイス200からシンクデバイス200の生成し

50

た擬似ランダム値を一定周期で受信し、自分が生成した擬似ランダム値と比較して同一か否かを判断する。

【0035】

それにより、ソースデバイス100は、擬似ランダム値が同一と判断されると、コンテンツを引き続きシンクデバイス200に伝送し、擬似ランダム値が同一ではないと判断されると、コンテンツの伝送を中断することができる。

【0036】

一方、上述のようなHDCP認証を行うためには、次のような2段階が要求される。まず、最初に擬似ランダム値を生成して比較することで、ソースデバイス100とシンクデバイス200とが互いにコンテンツ保護に適した装置であるかを確認する過程である第1認証プロトコルパート(1st part of Authentication Protocol)と、その後持続的に(仮に、2秒おきに)両端で生成した擬似ランダム値を比較する第3認証プロトコルパート(3rd part of Authentication Protocol)がある。

10

【0037】

このような方式により、ソースデバイス100とシンクデバイス200とは、HDCP規格によるHDCP認証を行うことができる。

【0038】

一方、本発明の一実施形態によると、ソースデバイス100は、シンクデバイス200で対応するHDCPバージョンを考慮してコンテンツを暗号化してシンクデバイス200に伝送することができる。

20

【0039】

以下では、ソースデバイス100とシンクデバイス200との具体的な構成を参照してより具体的に説明する。

【0040】

図2は、本発明の一実施形態に係るソースデバイスの構成について説明するためのブロック図である。図2によると、ソースデバイス100は、インターフェース部110及び制御部120を含む。

【0041】

インターフェース部110は、シンクデバイス(図1の200)と通信を行い、シンクデバイス200にコンテンツを伝送することができる。

30

【0042】

この場合、インターフェース部110は、シンクデバイス200とHDCP認証を行うことができる。

【0043】

そのために、インターフェース部110は、HDMIで実現されてよい。具体的に、インターフェース部110は、R、G、B信号及びクロック信号が印加されるTMDSCハネルリンク、双方向I²C通信のためのDDC通信ライン、HDMI接続を検知するHPD検知ラインが接続されるピンを含んでよい。なお、インターフェース部110は、AKSVを保存するメモリ(図示せず)、HDCP規格による認証を行うHDCPエンジン(図示せず)を含んでよい。

40

【0044】

それにより、インターフェース部110は、HPD信号によってシンクデバイス200が接続されていると判断されると、シンクデバイス200とHDCP認証を行うことができる。そして、インターフェース部110は、HDCP認証に成功すると、コンテンツを暗号化してシンクデバイス200に伝送し、HDCP認証に失敗すると、コンテンツの伝送を中断することができる。

【0045】

制御部120は、ソースデバイス100の動作全般を制御する。制御部120は、マイクロコンピュータ(または、マイクロコンピュータ及びCPU(Central Pro

50

cessing Unit))、ディスプレイ装置100の動作のためのRAM(Random Access Memory)、ROM(Read Only Memory)を含んでよい。この場合、これらのモジュールは、SoC(System on Chip)形態で実現されてよい。

【0046】

制御部120は、シンクデバイス200で対応するHDCPバージョンを判断することができる。ここで、HDCPバージョンは、HDCP 1.Xバージョン(仮に、HDCP 1.4バージョン等)、HDCP 2.Xバージョン(仮に、HDCP 2.2バージョン等)等のように、HDCP規格で定義した多様なバージョンであってよい。

【0047】

具体的に、制御部120は、シンクデバイス200で対応するHDCPバージョン及びコンテンツに適用されるHDCPバージョンのそれぞれで定義された方式に応じて、シンクデバイス200とHDCP認証実行が可能か否かを判断し、シンクデバイス200が対応するHDCPバージョンを判断することができる。ここで、コンテンツに適用されるHDCPバージョンは、HDCP 1.Xバージョン(仮に、HDCP 1.4バージョン等)、HDCP 2.Xバージョン(仮に、HDCP 2.2バージョン等)等のように、HDCP規格で定義した多様なバージョンであってよい。

【0048】

例えば、コンテンツに適用されるバージョンがHDCP 2.2バージョンであり、シンクデバイス200で対応するHDCPバージョンがHDCP 1.4バージョンの場合を仮定する。

【0049】

この場合、制御部120は、HDCP 1.4バージョンで定義する方式に応じて、シンクデバイス200とHDCP認証を行うようにインターフェース部110を制御し、HDCP 1.4バージョンによるHDCP認証実行ができるか否かを判断することができる。それにより、制御部120は、シンクデバイス200とHDCP 1.4バージョンによるHDCP認証実行ができれば、シンクデバイス200はHDCP 1.4バージョンを対応すると判断し、HDCP 1.4バージョンによるHDCP認証実行ができなければ、シンクデバイス200はHDCP 1.4バージョンを対応していないと判断することができる。

【0050】

同様に、制御部120は、HDCP 2.2バージョンで定義する方式に応じて、シンクデバイス200とHDCP認証を行うようにインターフェース部110を制御し、HDCP 2.2バージョンによるHDCP認証実行が可能か否かを判断することができる。それにより、制御部120は、シンクデバイス200とHDCP 2.2バージョンによるHDCP認証実行が可能であれば、シンクデバイス200はHDCP 2.2バージョンを対応すると判断し、HDCP 2.2バージョンによるHDCP認証実行ができなければ、シンクデバイス200はHDCP 2.2バージョンを対応していないと判断することができる。

【0051】

このように、制御部120は、シンクデバイス200がHDCP 1.4バージョンまたはHDCP 2.2バージョンを対応すると仮定し、各HDCPバージョンに応じてシンクデバイス200とHDCP認証実行の可否を判断し、シンクデバイス200で対応するHDCPバージョンを判断することができる。

【0052】

なお、制御部120は、シンクデバイス200に予め保存されたHDCPバージョンに関する情報の伝送を要求し、シンクデバイス200から受信されたHDCPバージョンに関する情報に基づいて、シンクデバイス200が対応するHDCPバージョンを判断することができる。

【0053】

10

20

30

40

50

そのために、シンクデバイス200は、EDID(Extended Display Identification Data)に自分のHDCPバージョンに関する情報を保存することができる。この場合、制御部120は、DCC通信ラインを用いて、シンクデバイス200からEDIDを受信してシンクデバイス200で対応するHDCPバージョンを判断することができる。

【0054】

なお、シンクデバイス200は、RAMに自分のHDCPバージョンに関する情報を保存することができる。この場合、制御部120は、HDCPバージョンに関する情報をシンクデバイス200から受信し、シンクデバイス200で対応するHDCPバージョンを判断することができる。

10

【0055】

一方、制御部120は、コンテンツに適用されるHDCPバージョンがシンクデバイス200で対応していないと判断されると、シンクデバイス200で対応するHDCPバージョンで暗号化できるようにコンテンツを変換し、変換されたコンテンツをシンクデバイス200で対応するHDCPバージョンで暗号化してシンクデバイス200に伝送するようにインターフェース部110を制御することができる。

【0056】

ここで、コンテンツは、第1HDCPバージョンで暗号化すべきプレミアムコンテンツであり、シンクデバイス200で対応するHDCPバージョンは第1HDCPバージョンより低い第2HDCPバージョンであってよい。例えば、コンテンツはHDCP 2.Xバージョンで暗号化すべきプレミアムコンテンツであり、シンクデバイス200で対応するHDCPバージョンはHDCP 1.Xバージョンであってよい。

20

【0057】

そのために、制御部120は、コンテンツに適用されるHDCPバージョンを判断することができる。具体的に、制御部120は、コンテンツがプレミアムコンテンツかに基づいて、コンテンツに適用されるHDCPバージョンを判断することができる。

【0058】

ここで、プレミアムコンテンツは、4kのコンテンツ、Full HDの3Dコンテンツ、未開封コンテンツ等のように、強い保護が要求されるコンテンツとして、HDCP規格ではプレミアムコンテンツに対してHDCP 2.Xバージョンを適用するように定義されている。

30

【0059】

それにより、制御部120は、コンテンツの解像度及びタイプに基づいてコンテンツがプレミアムコンテンツかを判断したり、コンテンツを構成するパケットのヘッダから当該コンテンツがプレミアムコンテンツかを示す情報を抽出し、コンテンツがプレミアムコンテンツかを判断することができる。

【0060】

なお、制御部120は、ユーザ命令に基づいてコンテンツがプレミアムコンテンツかを判断することもできる。例えば、コンテンツがプレミアムコンテンツであることを示すユーザ命令が入力されると、制御部120は当該コンテンツがプレミアムコンテンツであると判断することもできる。

40

【0061】

このように、制御部120は、コンテンツがプレミアムコンテンツであると判断されると、コンテンツに適用されるHDCPバージョンをHDCP 2.Xバージョンと判断することができる。

【0062】

一方、制御部120は、コンテンツがHDCP 2.Xバージョンが適用されるプレミアムコンテンツか、シンクデバイス200で対応するHDCPバージョンはHDCP 1.Xバージョンであると判断されると、シンクデバイス200で対応するHDCPバージョンで暗号化できるようにコンテンツを変換することができる。

50

【0063】

具体的に、制御部120は、ダウンスケーリングを通じてコンテンツの解像度を低下させて、シンクデバイス200で対応するHDCPバージョンで暗号化できるようにコンテンツを変換することができる。そのために、ソースデバイス100は、スケーラ（図示せず）を含んでよい。

【0064】

HDCP規格で、4kのコンテンツに対してHDCP 2.Xバージョンを適用するように定義することは、4kのコンテンツと同様に、元解像度の高いコンテンツをより強く保護するためである。よって、4kのコンテンツがダウンスケーリングによって解像度が低くなると、HDCP規格によるとしても、必ずしもHDCP 2.Xバージョンを適用しなければならないというわけではない。

10

【0065】

よって、制御部120は、コンテンツをダウンスケーリングして解像度を低下させて、解像度の低下しているコンテンツに対して、シンクデバイス200が対応するHDCPバージョンでシンクデバイス200とHDCP認証を行い、コンテンツを暗号化して伝送するように制御することができる。

【0066】

すなわち、HDCP規格によると、プレミアムコンテンツの場合、HDCP 2.Xバージョンを適用しなければならないが、シンクデバイスがHDCP 2.Xバージョンに対応していない場合、ソースデバイスはプレミアムコンテンツに適用されるHDCP 2.Xバージョンに応じて、シンクデバイスとHDCP認証を行うことができない。それにより、HDCP 2.Xバージョンに対応していないシンクデバイスのユーザは、ソースデバイスが提供するプレミアムコンテンツを視聴することができなかつた。

20

【0067】

しかし、本発明によると、ソースデバイス100はシンクデバイス200で対応するHDCPバージョンの適用ができるように、プレミアムコンテンツの解像度を低下させるため、プレミアムコンテンツに適用されるHDCP 2.Xバージョンに対応していないシンクデバイス200と互換性を維持することができるようになる。

【0068】

例えば、シンクデバイス200で対応するHDCPバージョンがHDCP 1.4バージョンであり、コンテンツがHDCP 2.2バージョンが適用される4kのコンテンツの場合を仮定する。

30

【0069】

この場合、制御部120は、3840×2160の解像度を有する4kのコンテンツを1920×1080の解像度にダウンスケーリングすることができる。このように、1920×1080に解像度の低下したコンテンツに対してHDCP 2.2バージョンを必ずしも適用しなければならないわけではないため、制御部120はシンクデバイス200が対応するHDCP 1.4バージョンに応じてシンクデバイス200と認証を行い、ダウンスケーリングされたコンテンツを暗号化してシンクデバイス200に伝送することができる。

40

【0070】

一方、上述の例においては、4kのコンテンツを例として挙げているが、それは一例に過ぎない。すなわち、制御部120は4kのコンテンツだけでなく、Full HDの3Dコンテンツ及び未開封のコンテンツに対しても、解像度を低下させてシンクデバイスで対応するHDCPバージョンが適用できるように制御することができる。

【0071】

なお、上述の例においては、コンテンツの解像度を低下させるものとして説明したが、それは一例に過ぎない。すなわち、制御部120は、ダウンスケーリングを通じてコンテンツの解像度を低下させるだけでなく、シンクデバイスに対応するHDCPバージョンが適用できるコンテンツを再加工することができる。例えば、コンテンツにHDCP 1.

50

Xバージョン及びHDCP 2.Xバージョン両方に適用が可能であり、シンクデバイス200でHDCP 1.Xバージョンを対応する場合、制御部120は別途の変換過程なく、コンテンツをHDCP 1.Xバージョンに応じて暗号化してシンクデバイス200に伝送することができる。しかし、それは一例に過ぎず、制御部120は、シンクデバイスで対応するHDCPバージョンが適用できるようにデータのフォーマットを変更する等、多様な方式でコンテンツを再加工し、再加工されたコンテンツをシンクデバイスで対応するHDCPバージョンに応じて暗号化し、シンクデバイスに伝送することができる。

【0072】

一方、制御部120は、コンテンツに適用されるHDCPバージョンがシンクデバイス200で対応されるものとして判断されると、コンテンツに適用されるHDCPバージョンでコンテンツを暗号化し、シンクデバイス200に伝送することができる。すなわち、制御部120は、シンクデバイス200でプレミアムコンテンツに適用されるHDCP 2.Xバージョンを対応すると判断されると、別途の処理なく、HDCP 2.Xバージョンによってシンクデバイス200と認証を行い、コンテンツを暗号化してシンクデバイス200に伝送することができる。

10

【0073】

一方、制御部120は、一般の方法を用いて、プレミアムコンテンツをダウンスケーリングを行うことができる。ただ、この場合、コンテンツの解像度が低くなることから、制御部120は、図3に示す方法を用いてプレミアムコンテンツをダウンスケーリングすることもできる。

20

【0074】

制御部120は、プレミアムコンテンツを構成する各フレームをより低いフレームで構成された4つのフレームでダウンスケーリングすることができる。具体的に、制御部120は、プレミアムコンテンツの各フレームで横及び縦で奇数番目に存在するピクセルを抽出して第1フレームを生成し、プレミアムコンテンツの各フレームで横は偶数番目であり、縦は奇数番目に存在するピクセルを抽出して第2フレームを生成し、プレミアムコンテンツの各フレームで横は奇数番目であり、縦は偶数番目に存在するピクセルを抽出して第3フレームを生成し、プレミアムコンテンツの各フレームで横及び縦で偶数番目に存在するピクセルを抽出して第4フレームを生成することができる。

30

【0075】

例えば、制御部120は、図3のように、 3840×2160 の解像度を有する4kのコンテンツの各フレームを 1920×1080 の解像度を有する4つのフレームでダウンスケーリングすることができる。

【0076】

そして、制御部120は、ダウンスケーリングされたコンテンツをシンクデバイス200で対応するHDCPバージョンで暗号化してシンクデバイス200に伝送することができる。この場合、シンクデバイス200は、ダウンスケーリングされたコンテンツを受信してプレミアムコンテンツが有する元解像度に復元して出力することができる。それにより、ユーザは解像度が低下することなく、コンテンツを視聴することができるようになる。

40

【0077】

一方、制御部120は、変換されたコンテンツをシンクデバイス200に伝送する場合、コンテンツが変換されたことを示すメッセージを出力するようにシンクデバイス200を制御することができる。

【0078】

すなわち、ソースデバイス100がシンクデバイス200が対応するHDCPバージョンを考慮し、プレミアムコンテンツの解像度を低下させ、シンクデバイス200に伝送するようになると、ユーザは元解像度より低下された解像度を有するコンテンツを視聴するようになる。

【0079】

50

それにより、制御部 120 は、解像度の低下したコンテンツが出力されていることを示すメッセージを出力するようにシンクデバイス 200 を制御し、解像度の低下したコンテンツを出力されていることをユーザに通知することができる。この場合、制御部 120 は、当該メッセージで構成されたグラフィックデータをシンクデバイス 200 に伝送したり、シンクデバイス 200 に予め保存されたグラフィックデータを出力するための制御命令をシンクデバイス 200 に伝送することができる。

【0080】

一方、上述の例のように、制御部 120 は、コンテンツに適用される HDCPバージョンがシンクデバイス 200 に対応していないと判断されると、別途のユーザ命令がなくても、自動的にシンクデバイス 200 に対応する HDCPバージョンで暗号化できるようにコンテンツを変換し、シンクデバイス 200 に伝送することができる。ただ、制御部 120 は、別途のユーザ命令が入力されると、コンテンツをシンクデバイス 200 に対応する HDCPバージョンに変換し、シンクデバイス 200 に伝送することもできる。

10

【0081】

なお、制御部 120 は、コンテンツを出力することができないことを示すメッセージを出力するようにシンクデバイス 200 を制御することができる。すなわち、制御部 120 は、コンテンツに適用される HDCPバージョンがシンクデバイス 200 に対応していないと判断されると、シンクデバイス 200 に対応する HDCPバージョンで暗号化できるようにコンテンツを変換することなく、コンテンツを出力することができないことを示すメッセージで構成されたグラフィックデータをシンクデバイス 200 に伝送することができる。または、制御部 120 は、シンクデバイス 200 に予め保存されたグラフィックデータを出力するための制御命令をシンクデバイス 200 に伝送することができる。

20

【0082】

図 4 は、本発明の一実施形態に係るソースデバイスの細部構成について説明するためのブロック図である。図 4 によると、ソースデバイス 100 は、インターフェース部 110 及び制御部 120 の他に、コンテンツ提供部 130 を更に含んでよく、それは制御部 120 によって制御されてよい。一方、図 4 に示す構成要素のうち、図 1 に示す構成要素と重複する箇所については、詳細な説明は省略する。

【0083】

コンテンツ提供部 130 は、シンクデバイス 200 に伝送されるコンテンツを提供することができ、実施形態に応じて多様な形態で実現されてよい。

30

【0084】

例えば、コンテンツ提供部 130 は、チューナ（図示せず）、復調器（図示せず）、等化器（図示せず）等のような構成を含む形態で実現され、放送局から伝送される放送コンテンツを受信することができる。なお、コンテンツ提供部 130 は、DVD、ブルーレイディスク等のような光ディスクから光ディスクに記録されたコンテンツを読み取ることができる。なお、コンテンツ提供部 130 は、USBメモリ、HDD等のような外部記録媒体からコンテンツを受信することもできる。

【0085】

それにより、制御部 120 は、シンクデバイス 200 に対応する HDCPバージョンを考慮し、コンテンツ提供部 130 から伝達されるコンテンツをシンクデバイス 200 に伝送するように制御する。

40

【0086】

一方、図 4 に示す構成要素の他にも、ソースデバイス 100 はソースデバイス 100 を動作させるために必要な各種プログラムを保存する保存部（図示せず）、ユーザ命令を受信するための入力部（図示せず）、ユーザ命令に対応するリモコン信号を受信するためのリモコン信号受信部（図示せず）を更に含んでよい。

【0087】

図 5 は、本発明の一実施形態に係るシンクデバイスの構成について説明するためのブロック図である。図 5 によると、シンクデバイス 200 は、インターフェース部 210 及び

50

制御部 220 を含む。

【0088】

インターフェース部 210 は、ソースデバイス (図 1 の 100) と通信を行い、ソースデバイス 100 からコンテンツを受信することができる。

【0089】

この場合、インターフェース部 210 は、ソースデバイス 100 と HDCP 認証を行うことができる。

【0090】

そのために、インターフェース部 210 は HDMI で実現されてよい。具体的に、インターフェース部 110 は、R、G、B 信号及びクロック信号が印加される TMD S チャネルリンク、双方向 I²C 通信のための DDC 通信ライン、HDMI 接続を検知する HPD 検知ラインが接続されるピンを含んでよい。なお、インターフェース部 210 は、BKSV を保存するメモリ (図示せず)、HDCP 規格による認証を行う HDCP エンジン (図示せず) を含んでよい。

10

【0091】

それにより、インターフェース部 210 は、HPD 信号によってシンクデバイス 200 が接続されていると判断されると、シンクデバイス 200 と HDCP 認証を行うことができる。そして、インターフェース部 210 は、HDCP 認証に成功すると、暗号化されたコンテンツをソースデバイス 100 から受信して復号化し、HDCP 認証に失敗すると、コンテンツを受信することができない。

20

【0092】

制御部 120 は、シンクデバイス 200 の動作全般を制御する。制御部 220 は、マイクロコンピュータ (または、マイクロコンピュータ及び CPU (Central Processing Unit))、ディスプレイ装置 100 の動作のための RAM (Random Access Memory)、ROM (Read Only Memory) を含んでよい。この場合、これらのモジュールは、SoC (System on Chip) 形態で実現されてよい。

【0093】

制御部 220 は、ソースデバイス 100 からシンクデバイス 200 で対応する HDCP バージョンに関する情報の要求が受信されると、予め保存されたシンクデバイス 200 で対応する HDCP バージョンに関する情報をソースデバイス 100 に伝送するようにインターフェース部 210 を制御する。

30

【0094】

そのために、シンクデバイス 200 は、自分の HDCP バージョンに関する情報が含まれた EDID を予め保存することができる。すなわち、シンクデバイス 200 は製造会社を表す生産者 ID、製品のモデル名を示す製造 ID、シンクデバイス 200 で映像及びオーディオ出力規格等に関する情報だけでなく、HDCP バージョンに関する情報を含む EDID を予め保存することができる。

【0095】

なお、シンクデバイス 200 は、RAM に自分の HDCP バージョンに関する情報を別途に保存することもできる。

40

【0096】

例えば、制御部 220 は、HPD 信号に応じてソースデバイス 100 が接続されていると判断されると、HDCP バージョンに関する情報を含む EDID をソースデバイス 100 に伝送したり、RAM に保存された HDCP バージョンに関する情報をソースデバイス 100 に伝送することができる。ただ、制御部 220 は、別途の伝送要求をソースデバイス 100 から受信する場合にも、HDCP バージョンに関する情報をソースデバイス 100 に伝送することができる。

【0097】

図 6 は、本発明の一実施形態に係るシンクデバイスの細部構成について説明するための

50

ブロック図である。図6によると、シンクデバイス200は、インターフェース部210及び制御部220の他にも、出力部230と、保存部240と、受信部250と、信号処理部260と、リモコン信号受信部270及び入力部280を更に含んでよく、これらの動作は制御部220によって制御されてよい。一方、図6に示す構成要素のうち、図4に示す構成要素と重複する箇所については、詳細な説明を省略する。

【0098】

出力部230は、多様な映像及びオーディオを出力する。そのために、出力部230は、ディスプレイ部(図示せず)及びオーディオ出力部(図示せず)を含んでよい。

【0099】

ディスプレイ部(図示せず)は、コンテンツに対する映像をディスプレイし、オーディオ出力部(図示せず)はコンテンツに対するオーディオを出力することができる。例えば、制御部220は、HDCP認証に成功し、ソースデバイス100からコンテンツが受信されると、受信されたコンテンツを復号化し、復号化されたコンテンツに対する映像をディスプレイ部(図示せず)にディスプレイし、コンテンツに対するオーディオをオーディオ出力部(図示せず)を介して出力することができる。

10

【0100】

一方、ディスプレイ部(図示せず)は、液晶表示装置(Liquid Crystal Display: LCD)、有機電気発光ダイオード(Organic Light Emitting Diode: OLED)またはプラズマ表示パネル(Plasma Display Panel: PDP)等で実現され、オーディオ出力部(図示せず)は、スピーカ、オーディオ出力ポート等で実現されてよい。

20

【0101】

一方、ディスプレイ部(図示せず)は、多様なメッセージをOSD(On Screen Display)形態で出力することができる。具体的に、制御部220は、ソースデバイス100から受信されたり、シンクデバイス200に予め保存されたグラフィックデータを用いて、多様なメッセージをOSD形態で生成し、それをディスプレイ部(図示せず)を介して出力することができる。ここで、メッセージは、ソースデバイス100から受信されるコンテンツの解像度が変更されたことを示すメッセージ、コンテンツを出力することができないことを示すメッセージを含んでよい。

【0102】

保存部240は、シンクデバイス200を動作させるために保存された各種プログラムを保存することができる。

30

【0103】

特に、保存部240は、シンクデバイス200で対応するHDCPバージョンに関する情報をEDIDフォーマットで保存することができる。そのために、保存部240は、フラッシュメモリ、EEPROM(Electrically Erasable and Programmable ROM)等で実現されてよい。

【0104】

それにより、制御部220は、ソースデバイス100でHDCPバージョンに関する情報の伝送要求が受信されると、保存部240からEDIDを読み取ってソースデバイス100に伝送するように制御することができる。

40

【0105】

受信部250は、放送コンテンツを受信することができる。放送コンテンツは、映像、オーディオ及び付加データ(例えば、EPG)を含んでよく、受信部250は、地上波放送、ケーブル放送、衛星放送、インターネット放送等のように多様なソースから放送コンテンツを受信することができる。

【0106】

例えば、受信部250は、放送局から伝送される放送コンテンツを受信するために、チューナ(図示せず)、復調器(図示せず)、等化器(図示せず)等のような構成を含む形態で実現されてよい。

50

【0107】

信号処理部260は、インターフェース部210及び受信部250を介して受信されたコンテンツに対する信号処理を行う。具体的に、信号処理部260は、コンテンツを構成する映像に対して、デコード、スケーリング及びフレームレート変換等の動作を行い、ディスプレイ部(図示せず)から出力可能な形態で信号処理を行うことができる。なお、信号処理部260は、コンテンツを構成するオーディオに対してデコード等の信号処理を行って、オーディオ出力部(図示せず)から出力可能な形態で信号処理を行うことができる。

【0108】

リモコン信号受信部270は、リモコン(図示せず)から入力されるリモコン制御信号を受信する。例えば、リモコン信号受信部270は、シンクデバイス200の動作を制御するための多様なユーザ命令に対応するリモコン制御信号を受信することができ、制御部220は、受信されたリモコン制御信号に対応する機能を行うことができる。

10

【0109】

入力部280は、多様なユーザ命令を受信する。制御部220は、入力部280で入力されたユーザ命令に対応する機能を行うことができる。そのために、入力部280は、入力パネルで実現されてよい。入力パネルは、タッチパッド(Touch Pad)或いは各種機能キー、数字キー、特殊キー、文字キー等を備えたキーパッド(Key Pad)またはタッチスクリーン(Touch Screen)方式で行われてよい。

【0110】

図7は、本発明の一実施形態に係るコンテンツ提供システムの動作について説明するための図である。一方、ソースデバイス100及びシンクデバイス200のそれぞれの具体的な動作については、図1ないし図6について詳細に説明しているため、図7ではこれらの構成の動作を概略に説明する。

20

【0111】

図7によると、ソースデバイス100は、放送局、光ディスク、USB等からプレミアムコンテンツ(仮に、4kのコンテンツ)を伝達される。

【0112】

そして、ソースデバイス100は、シンクデバイス200で対応するHDCPバージョンに関する情報を判断する。

30

【0113】

具体的に、ソースデバイス100は、HDCP 1.4バージョンで定義された方式によって、シンクデバイス200とHDCP認証実行が可能か否かを判断し(図7の1)、HDCP 2.2バージョンで定義された方式に応じてシンクデバイス200とHDCP認証実行が可能か否かを判断する(図7の2)。

【0114】

判断の結果、ソースデバイス100はHDCP 1.4バージョンとHDCP 2.2バージョンとのうち、HDCP 1.4バージョンで定義された方式でシンクデバイス200とHDCP認証実行が可能と判断されると、シンクデバイス200がHDCP 1.4バージョンを対応すると判断する。

40

【0115】

それにより、ソースデバイス100はプレミアムコンテンツをHDCP 1.4バージョンで暗号化し、シンクデバイス200に伝送するために、プレミアムコンテンツをダウンスケーリングする。例えば、ソースデバイス100は、2160×3840の解像度を有する4kのコンテンツを1920×1080の解像度にダウンスケーリングすることができる。

【0116】

その後、ソースデバイス100は、HDCP 1.4バージョンによるHDCP認証をシンクデバイス200と行い、ダウンスケーリングされたコンテンツをHDCP 1.4バージョンで暗号化してシンクデバイス200に伝送することができる。

50

【0117】

それにより、ソースデバイス100は、ソースデバイス100から受信されたコンテンツを復号化して出力することができる。この場合、シンクデバイス200は、解像度の低下したコンテンツが出力されていることを示すメッセージ310をOSD形態で出力することができる。

【0118】

図8は、本発明の一実施形態に係るコンテンツ提供システムの動作について説明するためのフローチャートである。

【0119】

まず、ソースデバイス100とシンクデバイス200とがHDMI通信方式によって接続されると(S810)、ソースデバイス100とシンクデバイス200とは、HDCP 1.4バージョンで定義された方式で通信接続を行う(S820)。すなわち、ソースデバイス100とシンクデバイス200とは、HDCP 1.4バージョンで定義された方式によって、HDCP認証実行ができるか否かを判断する。

10

【0120】

そして、ソースデバイス100は、HDCP 1.4バージョンの通信接続の実行可否を判断する(S830)。

【0121】

それにより、HDCP 1.4バージョンによる通信接続に失敗すると、ソースデバイス100はシンクデバイス200でHDCP 1.4バージョンを対応していないと判断することができる(S840)。

20

【0122】

一方、HDCP 1.4バージョンによる通信接続に成功すると、ソースデバイス100はシンクデバイス200でHDCP 1.4バージョンを対応できると判断することができる。

【0123】

その後、ソースデバイス100は、HDCP 2.2バージョンの通信接続の実行可否を判断する(S850及びS860)。すなわち、ソースデバイス100は、シンクデバイス200とHDCP 2.2バージョンで定義されたHDCP認証実行ができるか否かを判断する。

30

【0124】

それにより、HDCP 2.2バージョンによる通信接続に失敗すると、ソースデバイス100はシンクデバイス200でHDCP 2.2バージョンを対応していないと判断することができる。結果的に、ソースデバイス100は、シンクデバイス200でHDCP 1.4バージョンのみを対応すると判断することができる(S870)。

【0125】

一方、HDCP 2.2バージョンによる通信接続に成功すると、ソースデバイス100はシンクデバイス200でHDCP 2.2バージョンを対応できると判断することができる。結果的に、ソースデバイス100は、シンクデバイス200でHDCP 1.4バージョン及びHDCP 2.2バージョンの両方を対応すると判断することができる(S880)。

40

【0126】

その後、ソースデバイス100は、プレミアムコンテンツの再生命令が入力されると(S890及びS910)、シンクデバイス200で対応するバージョンに応じてプレミアムコンテンツを暗号化してシンクデバイス200に伝送することができる。

【0127】

具体的に、ソースデバイス100は、シンクデバイス200でHDCP 2.2バージョンを対応すると判断されると、プレミアムコンテンツをHDCP 2.2バージョンで暗号化し(S920)、HDMIを通じてシンクデバイス200に伝送することができる(S930)。

50

【0128】

一方、ソースデバイス100は、シンクデバイス200でHDCP 2.2バージョンを対応せずに、HDCP 1.4バージョンを対応すると判断されると、プレミアムコンテンツをダウンスケーリングし(S940)、ダウンスケーリングされたコンテンツをHDCP 1.4バージョンで暗号化し(S950)、HDMIを通じてシンクデバイス200に伝送することができる(S960)。

【0129】

図9は、本発明の一実施形態に係るシンクデバイスにコンテンツを送るソースデバイスのコンテンツ伝送方法について説明するためのフローチャートである。

【0130】

まず、シンクデバイスで対応するHDCPバージョンを判断する(S1010)。

【0131】

具体的に、シンクデバイスで対応するHDCPバージョン及びコンテンツに適用されるHDCPバージョンのそれぞれで定義された方式に応じて、シンクデバイスとHDCP認証実行が可能か否かに基づいて、シンクデバイスが対応するHDCPバージョンを判断することができる。

【0132】

なお、シンクデバイスに予め保存されたHDCPバージョンに関する情報の伝送を要求し、シンクデバイスから受信されたHDCPバージョンに関する情報に基づいてシンクデバイスが対応するHDCPバージョンを判断することもできる。

【0133】

その後、コンテンツに適用されるHDCPバージョンが前記シンクデバイスで対応していないと判断されると、シンクデバイスで対応するHDCPバージョンで暗号化できるようにコンテンツを変換する(S1020)。

【0134】

ここで、コンテンツは、第1HDCPバージョンで暗号化すべきプレミアムコンテンツであり、シンクデバイスで対応するHDCPバージョンは、第1HDCPバージョンより低いHDCPバージョンであってよい。

【0135】

具体的に、ダウンスケーリングを通じてコンテンツの解像度を低下させてシンクデバイスで対応するHDCPバージョンで暗号化できるようにコンテンツを変換することができる。

【0136】

そして、変換されたコンテンツをシンクデバイスで対応するHDCPバージョンで暗号化してシンクデバイスに伝送する(S1030)。

【0137】

一方、コンテンツに適用されるHDCPバージョンが前記シンクデバイスで対応すると判断されると、コンテンツに適用されるHDCPバージョンで前記コンテンツを暗号化してシンクデバイスに伝送することができる。

【0138】

なお、変換されたコンテンツをシンクデバイスに伝送する場合、コンテンツが変換されたことを示すメッセージを出力するようにシンクデバイスを制御することができる。なお、コンテンツを出力することができないことを示すメッセージを出力するようにシンクデバイスを制御することもできる。

【0139】

図10は、本発明の一実施形態に係るソースデバイスから提供されるコンテンツを出力するシンクデバイスの制御方法について説明するためのフローチャートである。

【0140】

まず、ソースデバイスから前記シンクデバイスで対応するHDCP(High-bandwidth Digital Content Protection)バージョンに

10

20

30

40

50

関する情報の要求を受信する（S1110）。

【0141】

その後、HDCPバージョンに関する情報の伝送要求を受信されると、予め保存されたシンクデバイスで対応するHDCPバージョンに関する情報をソースデバイスに伝送する（S1120）。

【0142】

そのために、シンクデバイスは、シンクデバイスで対応するHDCPバージョンに関する情報をEDID（Extended Display Identification Data）フォーマットで保存することができる。

【0143】

なお、本発明に係るメニューコンテンツ提供方法及び制御方法を順次に行うプログラムが保存された非一時的な読み取り可能な媒体（Non-transitory computer readable medium）が提供されてよい。

【0144】

非一時的な読み取り可能な媒体とは、レジスタやキャッシュ、メモリ等のように短い間だけデータを保存する媒体ではなく、半永久的にデータを保存し、機器によって読み取り（reading）が可能な媒体を意味する。具体的には、上述の多様なアプリケーションまたはプログラムは、CDやDVD、ハードディスク、ブルーレイディスク、USB、メモリカード、ROM等のような非一時的な読み取り可能な媒体に保存されて提供されてよい。

【0145】

なお、ソースデバイス及びシンクサーバに対して示す上述のブロック図では、バス（bus）を示していないが、ディスプレイ装置で各構成要素間の通信はバスを通じて行われてよい。なお、各デバイスには、上述の多様なステップを行うCPU、マイクロプロセッサ等のようなプロセッサが更に含まれてよい。

【0146】

以上、添付図面を参照しながら本発明の好適な実施形態について詳細に説明したが、本発明は以上の実施形態に限定されない。本発明の属する技術の分野における通常の知識を有する者であれば、特許請求の範囲に記載された技術的趣旨の範疇内において、各種の変更例または修正例に想到し得ることは明らかであり、これらについても、当然に本発明の技術的範囲に属するものと了解される。

【符号の説明】

【0147】

- 100 ソースデバイス
- 110、210 インターフェース部
- 120、220 制御部
- 130 コンテンツ提供部
- 200 シンクデバイス
- 230 出力部
- 240 保存部
- 250 受信部
- 260 信号処理部
- 270 リモコン信号受信部
- 280 入力部

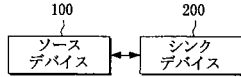
10

20

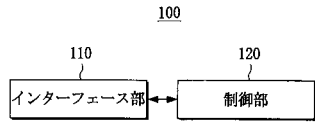
30

40

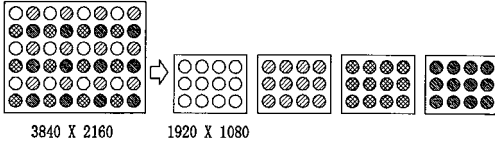
【 図 1 】



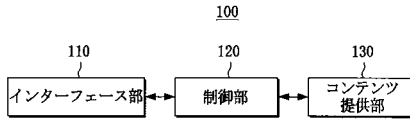
【 図 2 】



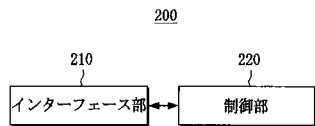
【 図 3 】



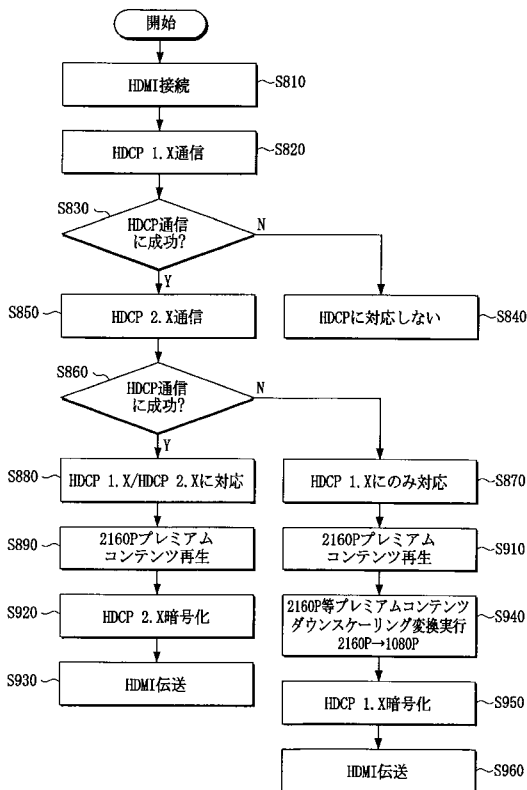
【 図 4 】



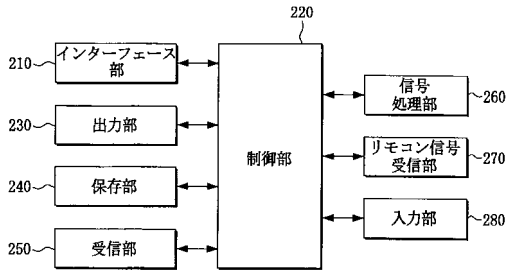
【 図 5 】



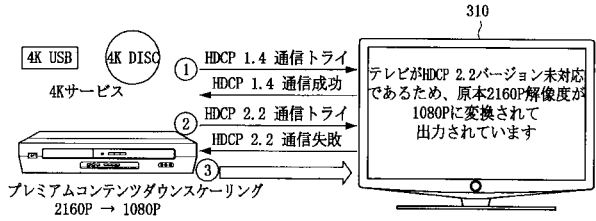
【 図 8 】



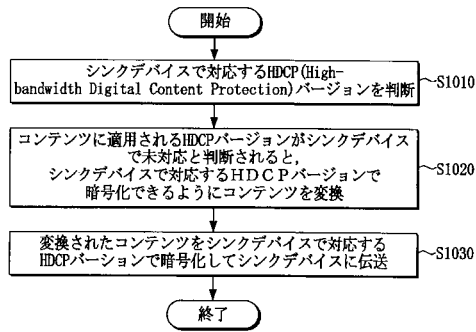
【 図 6 】



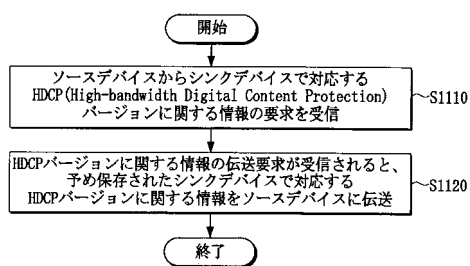
【 図 7 】



【 図 9 】



【 図 10 】



フロントページの続き

(72)発明者 お 昇 保

大韓民国京畿道水原市靈通区三星路268番-ギル7 ビー-201

Fターム(参考) 5C164 FA17 PA33 UB02P UB72P