

(19) 日本国特許庁(JP)

(12) 公表特許公報(A)

(11) 特許出願公表番号

特表2007-525122

(P2007-525122A)

(43) 公表日 平成19年8月30日(2007.8.30)

(51) Int. Cl.		F I		テーマコード (参考)
<b>HO4H</b>	<b>1/00</b>		<b>236</b>	<b>5J104</b>
<b>HO4L</b>	<b>9/08</b>		<b>614</b>	
			<b>621</b>	
			<b>601B</b>	
			<b>601E</b>	
審査請求 未請求 予備審査請求 未請求 (全 15 頁)				

(21) 出願番号 特願2006-551964 (P2006-551964)  
 (86) (22) 出願日 平成17年1月24日 (2005.1.24)  
 (85) 翻訳文提出日 平成18年8月4日 (2006.8.4)  
 (86) 国際出願番号 PCT/IB2005/050274  
 (87) 国際公開番号 W02005/076574  
 (87) 国際公開日 平成17年8月18日 (2005.8.18)  
 (31) 優先権主張番号 04100418.5  
 (32) 優先日 平成16年2月5日 (2004.2.5)  
 (33) 優先権主張国 欧州特許庁 (EP)

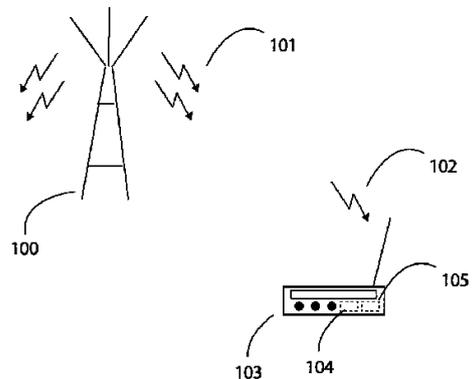
(71) 出願人 590000248  
 コーニンクレッカ フィリップス エレクトロニクス エヌ ヴィ  
 オランダ国 5621 ペーアー アイン  
 ドーフェン フルーネヴァウツウェッハ  
 1  
 (74) 代理人 100070150  
 弁理士 伊東 忠彦  
 (74) 代理人 100091214  
 弁理士 大貫 進介  
 (74) 代理人 100107766  
 弁理士 伊東 忠重

最終頁に続く

(54) 【発明の名称】 自由放送と平行して暗号化されたコンテンツ

(57) 【要約】

本発明は、情報送信(101)からコンテンツを取得するための方法及び装置(103)に関する。本発明は、情報送信が送信チャネルを介して受信されるという考えに基づく。例えばラジオショーからの放送である情報送信と共に、暗号化された、デジタル保存可能な形式の放送、又は放送の一部は、送信され、聴取者により受信される(102)。受信器において、聴取者は、受信器のフロントエンドにある専用のキーを押すことによって、現在再生中である歌曲のダウンロード動作を実施することができる。受信器は、歌曲の暗号化された、デジタル保存可能な複製を情報放送から抽出し、それを受信器に接続された記憶容量へダウンロードする。その後、聴取者は、再生動作を実施することにより、ダウンロードされた歌曲を再生するよう選択することができる。従って、受信器は、暗号化されたコンテンツを復号し、ダウンロードされたコンテンツをレンダリングしうる。



**【特許請求の範囲】****【請求項 1】**

情報送信からコンテンツを取得する方法であって：

第 1 のコンテンツと、該第 1 のコンテンツのデジタル保存可能な複製であって、暗号化された第 2 のコンテンツとを有する前記情報送信を受信するステップ；

前記情報送信の受信器が抽出動作を実施する場合に、前記情報送信に含まれる前記暗号化された第 2 のコンテンツを抽出するステップ；

前記暗号化された第 2 のコンテンツを前記受信器に保存するステップ；及び

前記第 2 のコンテンツがレンダリング可能とされるよう、前記暗号化された第 2 のコンテンツの復号化を可能にするステップ；

を有する方法。

10

**【請求項 2】**

前記暗号化された第 2 のコンテンツを復号するために、受信された情報放送に含まれる第 1 の復号化キーを抽出するステップを更に有する請求項 1 記載の方法。

**【請求項 3】**

前記第 1 の復号化キーが暗号化される場合に、

該暗号化された第 1 の復号化キーを復号するための第 2 の復号化キーをコンテンツプロバイダーから取得するステップを更に有する請求項 2 記載の方法。

**【請求項 4】**

前記第 1 のコンテンツ及び前記暗号化された第 2 のコンテンツは、別々のチャンネルで受信されることを特徴とする請求項 1 乃至 3 のうちいずれか一項記載の方法。

20

**【請求項 5】**

前記第 1 のコンテンツ及び前記暗号化された第 2 のコンテンツは、前記別々のチャンネルで互いに合わせられることを特徴とする請求項 4 記載の方法。

**【請求項 6】**

前記第 1 のコンテンツ及び前記暗号化された第 2 のコンテンツは、同じチャンネルで受信されることを特徴とする請求項 1 乃至 3 のうちいずれか一項記載の方法。

**【請求項 7】**

前記情報送信は、情報放送であることを特徴とする請求項 1 乃至 6 のうちいずれか一項記載の方法。

30

**【請求項 8】**

情報送信からコンテンツを取得する装置であって：

第 1 のコンテンツと、該第 1 のコンテンツのデジタル保存可能な複製であって、暗号化された第 2 のコンテンツとを有する前記情報送信を受信する手段；

当該装置が抽出動作を実施するよう動作する場合に、前記情報送信に含まれる前記暗号化された第 2 のコンテンツを抽出する手段；

前記暗号化された第 2 のコンテンツを当該装置で保存する手段；及び

前記第 2 のコンテンツがレンダリング可能とされるよう、前記暗号化された第 2 のコンテンツの復号化を可能にする手段；

を有する装置。

40

**【請求項 9】**

前記抽出手段は、更に、第 1 の復号化キーを抽出するよう配置され、

前記第 1 のキーは、前記暗号化された第 2 のコンテンツを復号するために、受信された情報放送に含まれることを特徴とする請求項 8 記載の装置。

**【請求項 10】**

前記第 1 の復号化キーは、暗号化され、

前記復号化手段は、更に、前記暗号化された第 1 の復号化キーを第 2 の復号化キーを用いて復号するよう配置されることを特徴とする請求項 9 記載の装置。

**【請求項 11】**

前記受信手段は、更に、前記第 1 のコンテンツ及び前記暗号化された第 2 のコンテンツ

50

を別々のチャンネルで受信するよう配置されることを特徴とする請求項 8 乃至 10 のうちいずれか一項記載の装置。

【請求項 12】

前記受信手段は、更に、前記第 1 のコンテンツ及び前記暗号化された第 2 のコンテンツを同じチャンネルで受信するよう配置されることを特徴とする請求項 8 乃至 10 のうちいずれか一項記載の装置。

【発明の詳細な説明】

【技術分野】

【0001】

本発明は、情報送信からコンテンツを取得する方法と、情報送信からコンテンツを取得するための装置とに関する。 10

【背景技術】

【0002】

小型ワンチップ放送無線受信器の導入以来ずっと、FM 放送無線受信を電子装置に加えたときの価格は、徐々に下がってきている。近年では、このような機能は、ほぼ携帯電話の標準機能の一部となっている。

【0003】

無線データシステム (RDS) は、無線聴取者が、繰り返し無線同調ダイヤルを操作する必要性を伴うことなく、特定の種類の番組をスキップすることを可能にするための規格である。更に、RDS では、データは、FM 無線信号に埋め込み可能である。RDS は、基地局の識別及び分類のために使用される。つい最近では、RDS は、例えば交通情報のような他の形式のデータを車載ラジオ受信器へ送信するために使用されている。RDS の具体的な応用は、トラフィックメッセージチャンネル (TMC) である。TMC は、リアルタイムの交通及び気象情報と、特に、動的な道路案内として知られるナビゲーション情報とを放送するために使用される。無線データは、TMS を装備した車載ラジオにより受信されてデコードされる。結果として得られる情報は、視覚的又は聴覚的に運転者へ伝えられる。 20

【0004】

デジタル音声放送 (DAB) は、圧縮された音楽に隣接してデータサービスを提供するデジタル無線放送システムである。DAB は、RDS - TMC 信号のキャリアとして使用されうる。マルチメディアオブジェクト転送 (MOT) 規格は、DAB がテキスト及びグラフィックと、更には動画像、インターネットページ等とを搬送することを可能にする。コピーライトコントロール、条件付きアクセス、付加価値サービスは、地上波及び/又は衛星通信による送信を用いて、局部的、局地的又は国家的なサービス範囲及び異なるデータ容量を有する DAB において実施されうる。 30

【0005】

今日の情報社会では、デジタル情報の迅速な拡大は、デジタル権利管理 (DRM) の概念に起源を与えている。この概念は、一般的にデジタルコンテンツと呼ばれるデジタル情報の作成者の権利と、情報又はコンテンツを頒布する情報提供者の権利とを保護するために使用される。この概念は、例えばラジオ、インターネット、CD 又は DVD 等のような如何なる形式の媒体を介して頒布された情報にも適用可能である。それは、また、例えば音声、映像、テキスト等の如何なる形式の情報にも適用可能である。このように、DRM 技術は、著作権を取得したコンテンツが侵害、悪用及び/又は不正頒布を受けることを防ぐために使用される。従って、DRM 技術は、例えば DAB のようなシステムにおいて、頒布されたデータを保護し、且つ、放送局が収益を上げるのを支援するために実施される。通常、DAB システムでは、所謂デジタル権利が、頒布されるコンテンツに関連づけられている。デジタル権利は、どんなアクセスをそのユーザがコンテンツに対して与えられているかを示す。共通のデジタル権利は、「再生」、「複製」、「CD - R への書き込み」、「転送」、「ダウンロード」等である。音声コンテンツに関連する標準的なデジタル権利は、「無制限の再生」である。しかし、制限されるデジタル権利も共通であり、その 40 50

ユーザに、権利に関連づけられたコンテンツへのアクセスや、例えば「24時間再生」といった有限な時間を与える。

【0006】

公開された欧州特許出願EP1113605は、放送用デジタル音楽及び他の形式の情報の識別のための方法並びに装置を開示する。EP1113605では、識別情報は、1曲の音楽、又はユーザにとって関心のある他の形式の情報に係る現在の放送から抽出され、ユーザ命令に回答して記憶装置に保存される。識別情報は、特定の曲数の音楽を含む例えばCD又はMP3ファイルといった、現在の放送に関連づけられた少なくとも1つの伝送可能な情報項目において、識別するに十分な情報を有する。

【0007】

ユーザが有線又は無線のネットワーク接続へのアクセスを有する場合に、抽出された識別情報は、放送に関連づけられた伝送可能な情報項目を識別するよう、伝送された情報を処理するサーバーへのネットワーク接続により伝送される。その場合に、ユーザは、サーバーとの適切なやり取りにより、伝送可能な情報項目を獲得することができる。

【特許文献1】欧州特許出願EP1113605

【発明の開示】

【発明が解決しようとする課題】

【0008】

EP1113605の開示に係る問題は、識別子が放送情報に埋め込まれるので、識別情報を抽出した後、ユーザは、放送の識別情報に関連づけられた情報項目を取得するために、サーバーとの接続を確立しなければならないことである。情報項目を繰り返し獲得するユーザは、おそらく、この手順を退屈で不便であると考えられるであろう。

【0009】

本発明は、前出の問題を解決し、ユーザが例えばラジオチャンネル又はインターネットを介して送信される所望のコンテンツの一部分の取得を簡単に適応性があると評価するところの解決法を提供することを目的とする。

【0010】

本発明は、また、コンテンツ提供者が送信チャンネル上でデータを安全に送信することを可能にすることを目的とする。

【0011】

更に、本発明は、送信されるコンテンツの提供者、又は著作権を取得したコンテンツの保有者が、不正なコンテンツ頒布/聴取により損害を被らないように、条件付きアクセスを許可する解決法を提供することを目的とする。

【課題を解決するための手段】

【0012】

これらの目的は、請求項1に従う情報送信からコンテンツを取得するための方法と、請求項8に従う情報送信からコンテンツを取得するための装置とによって達成される。

【0013】

本発明の第1の態様に従って、情報送信が受信されるところの方法が提供される。情報送信は、第1のコンテンツと、暗号化された第2のコンテンツとを有し、第2のコンテンツは、第1のコンテンツの、デジタル保存可能な複製である。受信された情報送信に含まれる暗号化された第2のコンテンツは、受信器が抽出動作を実施する場合に情報送信から抽出される。次に、暗号化された第2のコンテンツは、受信器で保存される。最後に、暗号化された第2のコンテンツは復号され、これによって、第2のコンテンツはレンダリング可能とされる。

【0014】

本発明の第2の態様に従って、情報送信を受信するよう配置された手段を有する装置が提供される。情報送信は、第1のコンテンツと、暗号化された第2のコンテンツとを有し、第2のコンテンツは、第1のコンテンツの、デジタル保存可能な複製である。更に、当該装置は、当該装置が抽出動作を実施するよう動作する場合に、情報送信に含まれる暗号

10

20

30

40

50

化された第2のコンテンツを抽出する手段と、暗号化された第2のコンテンツを当該装置で保存する手段とを有する。更に、当該装置は、暗号化された第2のコンテンツを復号する手段と共に配置される。これによって、第2のコンテンツはレンダリング可能とされる。本発明は、情報送信が適切な送信チャネルを介して受信されるという考えに基づく。本発明が適用されるところのシステムは、例えば、DABシステム又はデジタルAM/FMラジオシステムでありうるが、使用されるシステムは、また、インターネットベースのシステム若しくは衛星放送システム、又は本願明細書等で記載される適切なサービスを可能にする如何なる他の送信システムであっても良い。本開示は主に放送送信について記載しているが、考えられる多数の送信形式は、例えば、放送、マルチキャスト又は如何なるキャストであっても良い。

10

**【0015】**

例えばラジオショーからの放送である情報送信と共に、暗号化された、デジタル保存可能な形式の放送、又は放送の一部は、送信され、ラジオショーの聴取者により受信される。望ましくは、聴取者がダウンロードを望む放送部分のみが、例えば放送がラジオショーである場合には歌曲が、暗号化された、デジタル保存可能な形式で送信される。従って、情報放送は、2つの異なった形式のコンテンツ、即ち、聴取者が受信する実際の情報である第1のコンテンツと、第1のコンテンツの複製であって、第2の、暗号化された、デジタル保存可能なコンテンツとを有すると考えられる。

**【0016】**

受信器において、聴取者は、現在再生中であって、チャンネル上で送信されている歌曲のダウンロード動作を実施することができる。聴取者が歌曲をダウンロードすることを望む場合には、例えば、受信器のフロントエンドにある専用のキーを押すことによって、受信器は、歌曲の暗号化された、デジタル保存可能な複製を情報放送から抽出し、それを受信器に接続された記憶容量へダウンロードする。その後、聴取者は、再生動作を実施することにより、ダウンロードされた歌曲を再生するよう選択することができる。従って、受信器は、暗号化されたコンテンツを復号し、ダウンロードされたコンテンツをレンダリングしうる。

20

**【0017】**

本発明は、ユーザが放送に含まれる暗号化されたデジタル情報をダウンロードすることが可能であるので、有利である。更に、ユーザは、インターネットのコンテンツをダウンロードするためにサービス提供者との専用の接続を確立する必要がない。ユーザは、このような有利な点を、所望のコンテンツを取得するための円滑で適応性のある方法として経験しうる。暗号保護を用いるDRMシステムを使用することによって、コンテンツ提供者は、情報チャンネル上で安全にデータを送信することが可能である。更に、DRMシステムを使用することによって、認定ユーザが保護されたコンテンツにアクセスすべき権利の管理は、著しく容易となりうる。本発明は、著作権を取得したコンテンツの権利所有者及び/又はコンテンツ提供者が、不正なコンテンツ頒布/聴取によって損害を与えられることを防ぐ。

30

**【0018】**

本発明の実施例に従って、受信された情報送信に含まれる第1の復号化キーが、暗号化された第2のコンテンツを復号するために抽出される。この第1の復号化キーは、同じく暗号化されており、対応する第2の復号化キーが、暗号化された第1の復号化キーを復号するためにコンテンツ提供者から取得されなければならない。

40

**【0019】**

従って、暗号化されたデジタル方式の第2のコンテンツに付随する第1の復号化キーを解読することは、他の放送コンテンツの安全性を危険にさらさない。これは、第2のコンテンツを保護するために使用されるキーを選択する際に、放送局に柔軟性を与える。第1のキーを復号するための第2のキーは、例えば、ユーザがコンテンツ提供者又は提供者に関連する頒布者から購入するCDで、前もって頒布されうる。

**【0020】**

50

本発明の他の実施例に従って、第1のコンテンツ及び暗号化された第2のコンテンツは、別々のチャンネルで受信される。これは、共通チャンネルの帯域幅限界の可能性により、1つの共通チャンネルを用いることに比べて有利である。1つのチャンネルは、第2のデジタル保存可能なコンテンツを送るために必要とされる十分な予備の帯域幅を有し得ない。更に、放送局は、聴取者が受信する情報を搬送するチャンネル上で、絶対的に必要であるよりも多いデータを送ることができない。本実施例は、また、別々のチャンネルが異なる提供者によりある程度動作することができるので有利である。別々のチャンネルが使用される場合に、第1のコンテンツと暗号化された第2のコンテンツとを別々のチャンネル上で互いに協調させる必要がある。また、2つの異なった形式の情報を別々に管理することは、放送局により大きな自由度を与える。

10

**【0021】**

本発明の更なる実施例に従って、第1のコンテンツ及び暗号化された第2のコンテンツは、同じチャンネルで受信される。これは、放送局が、別々のチャンネルを用いる場合に生ずる情報オーバーヘッドを回避するという利点を有する。

**【0022】**

例えば、放送制作は、より容易となり、放送コンテンツ及びデジタル保存可能なコンテンツの協調は、放送コンテンツ及びデジタル保存可能なコンテンツが同じストリームで搬送されるので、同程度必要であるわけではない。従って、放送のタイミングは、デジタル保存可能なコンテンツのタイミングに自動的に結び付けられる。更に、受信装置でのハードウェア必要条件是、第2の別のチャンネルを動作する費用と共に減少しうる。

20

**【0023】**

本発明の更なる特徴及び利点は、添付の特許請求の範囲及び以下の説明を検討すると明確となるであろう。当業者は、本発明の様々な特徴が、以下で記載されている以外の実施例を作るために組み合わせられうることを理解する。

**【発明を実施するための最良の形態】****【0024】**

本発明の好ましい実施例について、添付の図面を参照して説明する。

**【0025】**

図1は、例えばFMラジオシステムのような従来の放送システムを示す。このシステムにおいて、本発明は実施されうる。放送局100は、空気界面を介してラジオショーの送信100を実施する。ラジオショーは、FMスペクトラムに内のあるチャンネルで放送される。放送情報、即ち、聴取者が受け取る情報は、以下、主要コンテンツと呼ばれる。受信器103において、放送の受信102が起こりうる。受信器は、受信回路、この場合にはFM受信器104と、更に、以下で述べられるように、例えば受信された送信から抽出した情報等のデータの処理、復号化及び暗号化を実行するためのマイクロプロセッサ105とを有する。しばしば、受信器側の聴取者が後にアクセスを望むことがある歌曲が、放送される。当然、聴取者は、受信したラジオショーを録音することによって、アナログ受信の複製を作ることができる。この録音は、例えば、アナログ音声カセット又はデジタルミニディスクにおいて実行されうる。通常、この手順は、録音装置に予め記録媒体がセットされているとの仮定の下、聴取者が歌曲を録音し始めると、歌曲の5から10秒が既に経過してしまっているという欠点を有する。そうではないにせよ、相当により長い時間期間が、聴取者が記録媒体を置いて、録音装置を設定する前に経過している。歌曲の経過時間が長くなればなるほど、聴取者は、録音をますます意味のないものと考ええる。他の欠点は、アナログ信号が記録される場合には、高品質録音を実現するのが困難であることである。更に、また、多数のディスクジョッキー(DJ)は歌曲の一部(特に、フェードイン/フェードアウト部分)の間に話す傾向を有し、即ち、歌曲全体が放送されないという問題がある。

30

40

**【0026】**

更に、この手順は、著作権で保護されているコンテンツの権利所有者/コンテンツ提供者が、実際には、頒布されたコンテンツの全体に亘る支配を有さない点で、権利所有者及

50

び / 又は提供者に損害を与えうる。上述したシナリオでは、コンテンツ消費者を告発する方法は存在しない。

【0027】

本発明に従って、暗号化された、デジタル保存可能な形式の放送、又は放送の一部は、主要コンテンツに沿って送信され、聴取者によって受信される。例えばMP3のような、デジタル保存可能な形式は、以下、派生的コンテンツと呼ばれる。望ましくは、聴取者がダウンロードしたいと望みそうな主要コンテンツに関連する派生的コンテンツのみが送信される。通常、ラジオショーは、歌曲のようなコンテンツと共に、モノログや、ニュースや、ラジオアナウンサーと聴取者との間の対話を含む。これらは、聴取者がダウンロードするに望ましいと考えられる。従って、前で述べたように、情報放送102は、2つの異なる形式のコンテンツ、即ち、聴取者が受信する実際の情報である第1のコンテンツ（主要コンテンツ）と、第1のコンテンツの複製であって、第2の、暗号化された、デジタル保存可能なコンテンツ（派生的コンテンツ）とを有すると考えられる。望ましくは、派生的コンテンツは、派生的コンテンツを送信するためのチャンネルの帯域幅を節約するために圧縮される。

10

【0028】

受信器103は、歌曲がラジオショーで呼び物となる場合に、ユーザが所望の歌曲をダウンロードすることを可能にする機能を設けられる。通常、聴取者は、この目的のために受信器上のキーを押す。これによって、受信器は、派生的コンテンツを取得する。送信チャンネルでは、放送局は、暗号化された派生的コンテンツを送信する。聴取者がダウンロードを実施する場合に、受信器は、（場合により、少し待機した後に、）暗号化及び圧縮をなされた派生的コンテンツを復元し、それを受信器に接続された、例えばSFFO（Small Form Factor Optical）ディスク（図2参照。）のような、ある適切な記憶容量に保存しうる。放送局は、暗号化された派生的コンテンツを繰り返し送信しても良い。それは、また、放送局が、場合により、ユーザがコンテンツの取得を望むか否かを決定する機会（即ち、時間。）をユーザに与えるための遅延を伴って、派生的コンテンツを一度しか送信しない場合であっても良い。他の実現可能なモデルは、受信装置が、ユーザが申し込む又は資格を有する全ての派生的コンテンツを抽出することである。歌曲の終了までに、ユーザが歌曲の保持を望むことを示さなかった場合には、その歌曲は削除の印を付され、次に記憶容量の量が問題となるときに削除されうる。購買契約は、限られた数の抽出を特定しうるので、ユーザによる明確な選択が、歌曲を保持するために必要とされる。

20

30

【0029】

コンテンツの抽出が終了し、ダウンロードが完了すると、受信器は、その表示を、例えば受信器の表示部を介して視覚的に、あるいは受信器のスピーカーを介して聴覚的にユーザに然るべく与えうる。

【0030】

このとき、暗号化された派生的コンテンツは、聴取者の記憶容量に存在する。しかし、対応する復号化キーを用いなければ、聴取者は、コンテンツをレンダリングすることができない。聴取者が復号化キーへのアクセスを予め取得していない場合に、聴取者は、コンテンツをレンダリングすることを望む場合には、復号化キーへのアクセスを取得するよう要求される。

40

【0031】

送信チャンネルが、例えばRDSにおいて問題であるところの低データレートを提供する場合に、送信のスケジュールは、歌曲の間又は直後に埋め込まれる。送信のスケジュールは、放送に埋め込まれ、いつ、どのチャンネルから歌曲が取得可能であるかを詳述する。復号化キーは、スケジュールに従う。このように、多数のラジオショーは、暗号化された派生的コンテンツの同じ送信を参照することができる。

【0032】

留意すべきは、図1において、本発明はFMラジオシステムに適用されているが、当業

50

者は、本発明が適用可能であるところの、例えば、AMラジオ、インターネットラジオ、衛星放送システム、等のような様々な通信システムを考えることができることである。

【0033】

図2を参照すると、聴取者は、現在のコンテンツが送信された特定のラジオ局から、又は、ラジオ局とのキー頒布の合意を有するキー頒布者から、復号化キーをもたらされている。キーは、聴取者がレンドリング装置202に挿入するディスク202に保存されても良い。例えばSFFOディスクのような、コンテンツを保持する記憶容量203は、レンドリング装置202に接続されている。装置202は、また、例えばサファイヤ(Sapphire)のような、既存のDRMシステムを設けられている。既存のDRMシステムは、聴取者がコンテンツに関連するデジタル権利を実際に取得しない限り、派生的コンテンツが自由となる時点で派生的コンテンツが頒布され得ないことを確実にする。なお、デジタル権利は、ユーザが派生的コンテンツを取得することを許可する。ユーザのコンテンツへのアクセスを示唆するデジタル権利は、通常、復号化キーと共にディスクに保存される。留意すべきは、無制限の頒布権(又は、ついでに言えば、制限された頒布権)は、それによってコンテンツ提供者がコンテンツの頒布の全てに亘る支配を失うので、むしろ珍しいことである。更に留意すべきは、ディスクでのキーの配信案は、人々を無線放送へ引き込むために物理的な物品が用いられることを意味し、多数の販売を促進する利点及び機会を有することである。

10

【0034】

本発明の実施例に従って、放送局100は、情報放送101において第1の復号化キーを有する。この第1の復号化キーは、例えば、暗号化された派生的コンテンツに添付されても良い。第1の復号化キーは、派生的コンテンツを暗号化した暗号化キーに対応する。本実施例では、受信器102が、図1に関連して記述されたように、暗号化された派生的コンテンツを抽出する場合に、それは、また、第1の復号化キーも抽出する。更に、第1の復号化キーは暗号化されており、対応する第2の復号化キーが、暗号化された第1の復号化キーを復号するためにコンテンツ提供者から取得されなければならない。第2の復号化キーは、図1及び2を参照して説明された実施例において論じられた復号化キーと同一である。第2の復号化キーが、暗号化された第1の復号化キーを復号するために使用されると、第1のキーが、暗号化された派生的コンテンツを復号するために使用される。これによって、派生的コンテンツは、いつでもレンドリング可能とされる。

20

30

【0035】

この「2つのキー」アプローチは、同一のキーを用いて暗号化/復号化がなされる(重要な)データが多くなればなるほど、キーが解読されることがますます起こり得るので、システムの安全性を高める。従って、夫々の歌曲をそれ自体のキーで暗号化する場合において、ある安全性の利点がある。

【0036】

しかし、主な利点は、アプローチが順応性を高めることである。例えば、聴取者が2種類の購買契約、即ち、(i)シュガーベイブスによる全ての歌曲(関連するキーはK3である。)と、(ii)あるDJからの全ての歌曲(関連するキーはK9である。)とを有するとする。この特定のDJがそのショーにおいてシュガーベイブスの歌曲を有する場合に、両方の購買契約が、その歌曲に対する権利を聴取者に与えうる。このようにして、歌曲は、上述した第1の暗号化キーを用いて暗号化され、対応する第1の復号化キーは、(上述した第2の復号化キーに対応する)K3及びK9を用いて暗号化される。これにより、データが2度送信されることを防ぐ。

40

【0037】

図3を参照すると、本発明の実施例に従って、主要コンテンツ及び暗号化された派生的コンテンツは、別々のチャンネルで受信される。放送局300は、第1の搬送周波数を有する第1のチャンネル301で主要コンテンツを、且つ、第2の搬送周波数を有する第2のチャンネル302で派生的コンテンツを送信する。受信器303は、主要コンテンツをレンドリングするよう第1のチャンネルを復調する。受信器303は、派生的コンテンツが抽出さ

50

れるようになるまでは、第2のチャンネルを復調する必要はない。留意すべきは、別々のチャンネルの場合には、主要コンテンツ及び派生的コンテンツを送信する放送局は、必ずしも同じではない。本実施例に関する主な利点は、例えば、レコード会社、又は他の何らかの種類のコンテンツ提供者が、暗号化された派生的コンテンツを放送するよう第2のチャンネルへのアクセスを得ることが可能であることである。別々のチャンネルが使用される場合には、主要コンテンツの、暗号化された、デジタル保存可能な複製が、第2のチャンネルで送信されるように、主要コンテンツ及び暗号化された派生的コンテンツを協調させることが必要である。

【0038】

別々のチャンネルの考え方への拡張は、聴取者が、例えばSMS (Short Message Service) を介して、又はページングを用いて、暗号化された派生的コンテンツを要求することを可能にすることが可能である。

10

【0039】

それでもなお、暗号化された第1のキーが、ダウンロードする機会を特定のラジオショーへ結び付けて、聴取者を魅了し、チャンネル/ショーを広告主にとって更に魅力的なものとするよう、第1のチャンネルを介して送信されても良い。広告主は、例えばキーが彼らのコマーシャルの間に送信される場合に、派生的コンテンツの販売さえ後援しうる。

【0040】

図4を参照すると、本発明の他の実施例に従って、放送局400は、同じチャンネル401で主要コンテンツ及び暗号化された派生的コンテンツを送信する。(それによって、受信器403は、1つのチャンネルでコンテンツを受信する。)放送局400は、主要コンテンツ及び暗号化された派生的コンテンツに対して単一の送信チャンネルを用いることによって、別々のチャンネルを用いる場合に生じる様々な種類のオーバーヘッドを回避することができる。

20

【0041】

本発明は、その特定の実施例を参照して説明されてきたが、多種多様な変形及び変更等が、当業者には認識されるであろう。従って、上述した実施例は、添付の特許請求の範囲によって定義される本発明の主旨を限定するわけではない。

【図面の簡単な説明】

【0042】

30

【図1】本発明が有利に用いられるシステムを示す。

【図2】取得されたコンテンツの本発明の実施例に従うレンダリングを表す。

【図3】本発明の実施例に従って主要コンテンツ及び暗号化された派生的コンテンツが別々のチャンネルで送信されうる様子を示す。

【図4】本発明の他の実施例に従って主要コンテンツ及び暗号化された派生的コンテンツが同じチャンネルで送信されうる様子を示す。

【 図 1 】

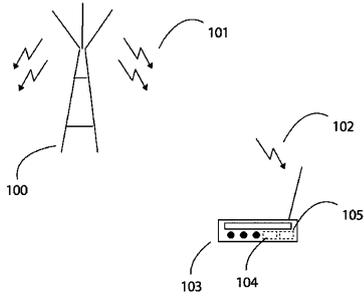


FIG. 1

【 図 2 】

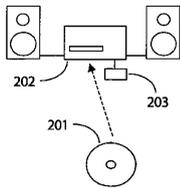


FIG. 2

【 図 3 】

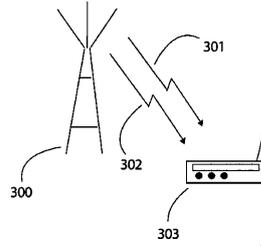


FIG. 3

【 図 4 】

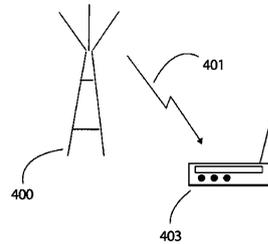


FIG. 4

## 【 手続 補正 書 】

【 提出 日 】 平成 18 年 9 月 11 日 (2006.9.11)

## 【 手続 補正 1 】

【 補正 対 象 書 類 名 】 特 許 請 求 の 範 囲

【 補正 対 象 項 目 名 】 全 文

【 補正 方 法 】 変 更

【 補正 の 内 容 】

【 特 許 請 求 の 範 囲 】

## 【 請 求 項 1 】

情報送信からコンテンツを取得する方法であって：

第 1 のコンテンツと、該第 1 のコンテンツのデジタル保存可能な複製であって、暗号化された第 2 のコンテンツとを有する前記情報送信を受信するステップ；

前記情報送信の受信器が抽出動作を実施する場合に、前記情報送信に含まれる前記暗号化された第 2 のコンテンツを抽出するステップ；

前記暗号化された第 2 のコンテンツを前記受信器に保存するステップ；

前記暗号化された第 2 のコンテンツを復号するために、受信された情報放送に含まれる第 1 の復号化キーを抽出するステップ；及び

前記第 2 のコンテンツがレンダリング可能とされるよう、前記暗号化された第 2 のコンテンツの復号化を可能にするステップ；

を有する方法。

## 【 請 求 項 2 】

前記第 1 の復号化キーが暗号化される場合に、

該暗号化された第 1 の復号化キーを復号するための第 2 の復号化キーをコンテンツプロバイダーから取得するステップを更に有する請求項 1 記載の方法。

## 【 請 求 項 3 】

前記第 1 のコンテンツ及び前記暗号化された第 2 のコンテンツは、別々のチャンネルで受信されることを特徴とする請求項 1 又は 2 記載の方法。

【請求項 4】

前記第 1 のコンテンツ及び前記暗号化された第 2 のコンテンツは、前記別々のチャンネルで互いに合わせられることを特徴とする請求項 3 記載の方法。

【請求項 5】

前記第 1 のコンテンツ及び前記暗号化された第 2 のコンテンツは、同じチャンネルで受信されることを特徴とする請求項 1 又は 2 記載の方法。

【請求項 6】

前記情報送信は、情報放送であることを特徴とする請求項 1 乃至 5 のうちいずれか一項記載の方法。

【請求項 7】

情報送信からコンテンツを取得する装置であって：

第 1 のコンテンツと、該第 1 のコンテンツのデジタル保存可能な複製であって、暗号化された第 2 のコンテンツとを有する前記情報送信を受信する手段；

当該装置が抽出動作を実施するよう動作する場合に、前記情報送信に含まれる前記暗号化された第 2 のコンテンツを抽出する手段；

前記暗号化された第 2 のコンテンツを当該装置で保存する手段；

前記暗号化された第 2 のコンテンツを復号するために、受信された情報放送に含まれる第 1 の復号化キーを抽出する手段；及び

前記第 2 のコンテンツがレンダリング可能とされるよう、前記暗号化された第 2 のコンテンツの復号化を可能にする手段；

を有する装置。

【請求項 8】

前記第 1 の復号化キーは、暗号化され、

前記復号化手段は、更に、前記暗号化された第 1 の復号化キーを第 2 の復号化キーを用いて復号するよう配置されることを特徴とする請求項 7 記載の装置。

【請求項 9】

前記受信手段は、更に、前記第 1 のコンテンツ及び前記暗号化された第 2 のコンテンツを別々のチャンネルで受信するよう配置されることを特徴とする請求項 7 又は 8 記載の装置。

【請求項 10】

前記受信手段は、更に、前記第 1 のコンテンツ及び前記暗号化された第 2 のコンテンツを同じチャンネルで受信するよう配置されることを特徴とする請求項 7 又は 8 記載の装置。

## 【 国際調査報告 】

INTERNATIONAL SEARCH REPORT		International Application No PCT/IB2005/050274		
<b>A. CLASSIFICATION OF SUBJECT MATTER</b> IPC 7 H04L29/06 H04H1/00				
According to International Patent Classification (IPC) or to both national classification and IPC				
<b>B. FIELDS SEARCHED</b> Minimum documentation searched (classification system followed by classification symbols) IPC 7 H04L H04H				
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				
<b>C. DOCUMENTS CONSIDERED TO BE RELEVANT</b>				
Category *	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.		
X	EP 1 073 222 A (LUCENT TECHNOLOGIES INC) 31 January 2001 (2001-01-31) paragraph '0006! - paragraph '0009! paragraph '0031! - paragraph '0049! paragraph '0052!	1,4-8, 11,12		
A	-----	2,3,9,10		
X	WO 01/16840 A (XM SATELLITE RADIO INC) 8 March 2001 (2001-03-08) page 3, line 8 - line 32 page 4, line 19 - page 8, line 28	1,8		
A	-----	2-7,9-12		
X	US 2004/006634 A1 (FERRIS GAVIN ROBERT) 8 January 2004 (2004-01-08) paragraph '0012! - paragraph '0027! paragraph '0029! - paragraph '0041!	1,8		
A	-----	2-7,9-12		
	-/--			
<input checked="" type="checkbox"/> Further documents are listed in the continuation of box C. <input checked="" type="checkbox"/> Patent family members are listed in annex.				
* Special categories of cited documents: <table border="0" style="width: 100%;"> <tr> <td style="vertical-align: top; width: 50%;">           "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         </td> <td style="vertical-align: top; width: 50%;">           "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.            "Z" document member of the same patent family         </td> </tr> </table>			"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. "Z" document member of the same patent family
"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. "Z" document member of the same patent family			
Date of the actual completion of the international search <b>13 April 2005</b>		Date of mailing of the international search report <b>20/04/2005</b>		
Name and mailing address of the ISA European Patent Office, P.B. 5818 Patentlaan 2 NL - 2280 HV Rijswijk Tel. (+31-70) 340-2040, Tx. 31 651 epo nl, Fax: (+31-70) 340-3016		Authorized officer <b>Raposo Pires, J</b>		

## INTERNATIONAL SEARCH REPORT

International Application No. PCT/IB2005/050274
--

C.(Continuation) DOCUMENTS CONSIDERED TO BE RELEVANT		
Category *	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	EP 1 113 605 A (LUCENT TECHNOLOGIES INC) 4 July 2001 (2001-07-04) cited in the application the whole document -----	1-12
A	US 2002/076051 A1 (NII NAOAKI) 20 June 2002 (2002-06-20) paragraph '0019! - paragraph '0021! paragraph '0026! - paragraph '0027! paragraph '0033! paragraph '0059! -----	1-12

## INTERNATIONAL SEARCH REPORT

 International Application No  
 PCT/IB2005/050274

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
EP 1073222 A	31-01-2001	CA 2314427 A1 EP 1073222 A2 JP 2001111505 A	30-01-2001 31-01-2001 20-04-2001
WO 0116840 A	08-03-2001	AU 7338400 A WO 0116840 A1	26-03-2001 08-03-2001
US 2004006634 A1	08-01-2004	EP 1310056 A2 WO 0205112 A2 GB 2369022 A ,B	14-05-2003 17-01-2002 15-05-2002
EP 1113605 A	04-07-2001	EP 1113605 A2 JP 2001216434 A	04-07-2001 10-08-2001
US 2002076051 A1	20-06-2002	AU 1261302 A WO 0250642 A2	01-07-2002 27-06-2002

## フロントページの続き

(81) 指定国 AP(BW, GH, GM, KE, LS, MW, MZ, NA, SD, SL, SZ, TZ, UG, ZM, ZW), EA(AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), EP(AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HU, IE, IS, IT, LT, LU, MC, NL, PL, PT, RO, SE, SI, SK, TR), OA(BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG), AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BW, BY, BZ, CA, CH, CN, CO, CR, CU, CZ, DE, DK, DM, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MA, MD, MG, MK, MN, MW, MX, MZ, NA, NI, NO, NZ, OM, PG, PH, PL, PT, RO, RU, SC, SD, SE, SG, SK, SL, SY, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, YU, ZA, ZM, ZW

(72) 発明者 フォンテイン, ウィルヘルムス エフ イェー  
オランダ国, 5 6 5 6 アーアー アインドーフエン, プロフ・ホルストラーン 6  
Fターム(参考) 5J104 EA17 PA07 PA10