

(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2007-502575

(P2007-502575A)

(43) 公表日 平成19年2月8日(2007.2.8)

(51) Int. Cl.	F I	テーマコード (参考)
HO4N 7/167 (2006.01)	HO4N 7/167 Z	5C164
HO4L 9/08 (2006.01)	HO4L 9/00 6O1B	5J104
	HO4L 9/00 6O1E	

審査請求 有 予備審査請求 未請求 (全 19 頁)

(21) 出願番号 特願2006-523169 (P2006-523169)
 (86) (22) 出願日 平成16年1月20日 (2004.1.20)
 (85) 翻訳文提出日 平成18年2月10日 (2006.2.10)
 (86) 国際出願番号 PCT/US2004/001573
 (87) 国際公開番号 W02005/020564
 (87) 国際公開日 平成17年3月3日 (2005.3.3)
 (31) 優先権主張番号 60/494,835
 (32) 優先日 平成15年8月13日 (2003.8.13)
 (33) 優先権主張国 米国 (US)

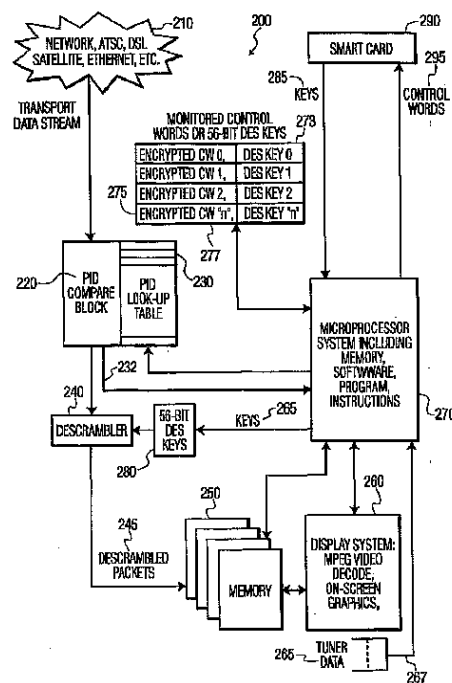
(71) 出願人 501263810
 トムソン ライセンシング
 Thomson Licensing
 フランス国, エフ-92100 ブロー
 ニュ ビヤンクール, ケ アルフォンス
 ル ガロ, 46番地
 46 Quai A. Le Gallo
 , F-92100 Boulogne-
 Billancourt, France
 (74) 代理人 100070150
 弁理士 伊東 忠彦
 (74) 代理人 100091214
 弁理士 大貫 進介
 (74) 代理人 100107766
 弁理士 伊東 忠重

最終頁に続く

(54) 【発明の名称】 チャンネル変更時間を削減する、スクランブル解除データの前処理

(57) 【要約】

本発明は、利用する前に、復号化するうえで暗号化鍵を必要とする複数の暗号化されたデジタルのビデオ、オーディオ及びデータを受信する装置及び方法を開示する。特に、本発明は、特定のチャンネルを選択すると複数のチャンネルへのアクセスをユーザに備える受信器に複数チャンネル情報を送信する、ケーブル・システムやデジタル放送衛星システムなどの装置に関する。そうしたチャンネル選択は、時間がかかる電子処理によって新たなデータストリームを復号し、フォーマットिंगすることを必要とする。本明細書及び特許請求の範囲記載の本発明は、新たなチャンネルをユーザが選択する前にバックグラウンドにおいてスクランブル解除データを監視することによってチャンネル変更時間を削減する。デジタル放送データは、利用可能な複数デジタル・データ・ストリーム各々に対するNビット・スクランブル解除鍵の復号化に必要な入力スクランブル解除制御語を含む。データ制御語又はNビット・スクランブル解除鍵を記憶することによって、後の取り出し復号化時間が削減される。しかし、制御語を利用して、Nビット・ス



【特許請求の範囲】**【請求項 1】**

受信器であって、

プログラムされる手段を利用して、2つ以上のチューニングされるチャンネルのうちの選択される1つに対するユーザ要求に、前記選択されるチャンネルに対するスクランブル解除鍵群のうちの1つを、選択されるビデオ・ディスプレイ内に情報をフォーマットするのに必要な関連スクランブル解除デジタル伝送ストリームによって出力させることによって応答する、2つ以上のチューニングされるチャンネルを備えることを特徴とする受信器。

【請求項 2】

請求項 1 記載の受信器であって、

前記スクランブル解除鍵群がメモリに記憶されることを特徴とする受信器。

10

【請求項 3】

請求項 1 記載の受信器であって、

前記スクランブル解除鍵群を、番組選択操作モードにおいて比較して所望のデジタル伝送ストリームを識別することを特徴とする受信器。

【請求項 4】

請求項 2 記載の受信器であって、

前記スクランブル解除鍵群が、前記 2 つ以上のチューニングされるチャンネルのうちの選択される 1 つに応じて、前記メモリから取り出されることを特徴とする受信器。

20

【請求項 5】

受信器であって、

デジタル伝送をチューニングし、復号化して、各々がスクランブル解除鍵と関連した 2 つ以上のチューニングされるチャンネルに関する制御語群を生成するチューニング及び復号化の装置と、

前記 2 つ以上のチューニングされるチャンネルのうちの選択される 1 つに対するユーザ要求に、前記選択されるチャンネルに対するスクランブル解除鍵の生成に対する、前記制御語群内の制御語のうちの 1 つを出力させて、ビデオ・ディスプレイ内にデジタル情報をフォーマットするのに必要なデジタル伝送ストリームをスクランブル解除することによって応答する、プログラムされる手段とを備えることを特徴とする受信器。

30

【請求項 6】

請求項 5 記載の受信器であって、

前記制御語群がメモリに記憶されることを特徴とする受信器。

【請求項 7】

請求項 5 記載の受信器であって、

前記制御語群を、番組選択操作モードにおいて比較して所望のデジタル・スクランブル解除鍵ストリームを識別することを特徴とする受信器。

【請求項 8】

請求項 6 記載の受信器であって、

前記制御語群が、前記メモリから取り出され、

制御語のうちの記憶された部分は、所望のデジタル伝送ストリームに関連したスクランブル解除手段と優劣つけがたいことを特徴とする受信器。

40

【請求項 9】

ビデオ伝送の受信方法であって、

デジタル伝送をチューニングし、復号化して、2つ以上のチューニングされるチャンネルに関連したスクランブル解除鍵群を生成する工程と、

前記 2 つ以上のチューニングされるチャンネルのうちの選択される 1 つに対するユーザ要求に、前記選択されるチャンネルに対する前記スクランブル解除鍵群を出力させて、デジタル情報をビデオ・ディスプレイ内にフォーマットするのに必要なデジタル伝送ストリームをスクランブル解除することによって応答するよう手段をプログラムす

50

る工程とを備えることを特徴とする受信方法。

【請求項 10】

請求項 9 記載の受信方法であって、

前記スクランブル解除鍵群をメモリに記憶する工程を更に備えることを特徴とする受信方法。

【請求項 11】

請求項 9 記載の受信方法であって、

前記スクランブル解除鍵群を、番組選択操作モードにおいて比較して所望のデジタル伝送ストリームを識別する工程を更に備えることを特徴とする受信方法。

【請求項 12】

請求項 10 記載の受信方法であって、

前記スクランブル解除鍵群を、前記メモリから取り出す工程を更に備え、

スクランブル解除鍵のうちの記憶された部分は、所望のデジタル伝送ストリームと優劣つけがたいことを特徴とする受信方法。

【請求項 13】

受信方法であって、

デジタル伝送をチューニングし、復号化して、各々がスクランブル解除鍵と関連した 2 つ以上のチューニングされるチャンネルに関する制御語群を生成する工程と、

前記 2 つ以上のチューニングされるチャンネルのうちの選択される 1 つに対するユーザ要求に、前記選択されるチャンネルに対するスクランブル解除鍵の生成に対する、前記制御語群内の制御語のうちの 1 つを出力させて、デジタル情報をビデオ・ディスプレイ内にフォーマットするのに必要なデジタル伝送ストリームをスクランブル解除することによって応答するよう手段をプログラムする工程とを備えることを特徴とする受信方法。

【請求項 14】

請求項 13 記載の受信方法であって、

前記制御語群をメモリに記憶する工程を更に備えることを特徴とする受信方法。

【請求項 15】

請求項 13 記載の受信方法であって、

前記制御語群を、番組選択操作モードにおいて比較して所望のデジタル伝送ストリームを識別する工程を更に備えることを特徴とする受信方法。

【請求項 16】

請求項 14 記載の受信方法であって、

前記制御語群を前記メモリから取り出す工程を更に備え、

制御語のうちの記憶された部分は、所望のスクランブル解除鍵と優劣つけがたいことを特徴とする受信方法。

【請求項 17】

受信方法であって、

視聴可能チャンネルを判定する工程と、

前記視聴可能チャンネルに関連した復号化鍵を復号化する工程と、

前記復号化鍵を、前記視聴可能チャンネルがユーザによって選択される場合に取り出し可能な状態でメモリに記憶する工程と、

視聴可能性を有するチャンネル全てが各々のスクランブル解除鍵を復号化させているかを判定し、

視聴可能性を有するチャンネル全てが各々のスクランブル解除鍵を復号化させている訳でない場合、時間変動放送において必要であるように、新たな制御語についてデジタル伝送を監視し続ける工程とを備えることを特徴とする受信方法。

【請求項 18】

請求項 17 記載の受信方法であって、

選択される視聴チャンネルに関連した前記スクランブル解除鍵を取り出す工程を更に備

10

20

30

40

50

えることを特徴とする受信方法。

【請求項 19】

請求項 18 記載の受信方法であって、
選択される視聴チャンネルに関連した前記スクランブル解除鍵を利用してデジタル・データを組み立てる工程を更に備えることを特徴とする受信方法。

【請求項 20】

受信方法であって、
視聴可能チャンネルを判定する工程と、
前記視聴可能チャンネルに関連した制御語を復号化する工程と、
前記制御語を、前記視聴可能チャンネルがユーザによって選択される場合に取り出し可能な状態でメモリに記憶する工程と、
視聴可能性を有するチャンネル全てが前記制御語を復号化させているかを判定し、
視聴可能性を有するチャンネル全てが前記制御語を復号化させている訳でない場合、時間変動放送において必要であるように、新たな制御語についてデジタル伝送を監視し続ける工程を更に備えることを特徴とする受信方法。 10

【請求項 21】

請求項 20 記載の受信方法であって、
前記制御語を取り出して、選択される視聴チャンネルに関連した鍵をスクランブル解除する工程を更に備えることを特徴とする受信方法。

【請求項 22】

請求項 21 記載の受信方法であって、
選択される視聴チャンネルに関連した鍵のスクランブル解除に対する前記制御語を利用してデジタル・データを組み立てる工程を更に備えることを特徴とする受信方法。 20

【発明の詳細な説明】

【技術分野】

【0001】

本発明は、一般的に、マルチチャンネルの、デジタルのビデオ/オーディオ/データ（「デジタル・データ」）の伝送を受信し、処理する方法及び装置に関し、特に、チャンネルを変更する旨のユーザ・コマンドに対する、よりすばやい応答を備えることができるデジタル放送受信器に関する。 30

【背景技術】

【0002】

マルチチャンネル・デジタル・ビデオ受信器がチャンネルを変更するのに必要な時間は、アナログ・ビデオ・システムにおいてチャンネルを変更する時間よりも大きい。何れのシステムでも、選択されるチャンネルの受信処理には、チューナが所望のキャリア周波数にチューニングし、所望のパケットを選択し、信号を復調することが必要である。デジタル放送信号は、通常はスクランブル解除されている情報を復号化する工程、MPEG符号化データを復元する工程、誤り訂正を備える工程などの更なる工程と、生成されるデータ・パケットをデジタル復号器に伝送する工程とを、所望の番組を表示できる前に通常必要とする。大容量の、複数チャンネルの直接放送衛星システムでは、受信器は、ハードウェア及びソフトウェアの実施形態と、デジタル・データ伝送のビット・レートとによってチャンネルを変更するうえで、1秒から5秒に及ぶ、数秒を必要とし得る。しかし、時間遅延の少なくとも一部分は、デジタル・データをスクランブル解除し、ビデオ表示を順次形成するというきまりによって生じる。米国特許第5,933,192号明細書及び米国特許第6,118,498号明細書は、チャンネル変更時間を削減するうえでの装置及び方法の2例を開示している。 40

【0003】

現行のデジタル・ビデオ復号器システムは、暗号化デジタル・データ・ストリームを復号化する（図1、従来技術参照。）。こうしたシステムは、ケーブル・システムやデジタル衛星放送（「DBS」）システムを例とするものなどのデジタル放送の技術分 50

野では周知であり、チューナ、変調器、デコーダ、伝送逆多重化装置、マイクロプロセッサ、番組メモリ、ビデオ・ピクチャ・メモリ、MPEGビデオ・デコーダ、ディスプレイ及びスマート・カードを含む。

【0004】

従来技術では、スクランブル・データは、データをスクランブル解除するための関連制御語と一緒に送信され、制御語は、エクスプロイト鍵によって暗号化され、暗号化形式で送信される。スクランブル・データ及び関連制御語は更に、受信器に挿入されて、暗号化制御語を復号し、その後、Nビットのスクランブル解除鍵を生成して送信デジタル・データを復号化するスマート・カード上に記憶されているエクスプロイト鍵に同等なものへのアクセスを有するデコーダによって受信される。例えば、払い込み済みのデジタル放送システムでは、加入者は、56ビットのスクランブル解除鍵を復号化して伝送の視聴を可能にするのに必要な暗号化制御語を復号するのに必要なエクスプロイト鍵を構成するエンタイトルメント・コントロール・メッセージを受信する。

10

【0005】

ユーザがチャンネルを選択すると、ソフトウェアは、伝送逆多重化装置を番組識別情報(PID)によって構成し、PIDは更に、入力デジタル・データ・パケットをフィルタリングする。システムは更に、デジタル・データ・ストリームにおける全パケットを検査するPID比較ブロックに伝送データストリームが流れることを可能にし、データ・パケットを、ルックアップ・テーブル内のエントリのリストと比較する。通常、一致が存在する場合、データ・パケットはスクランブル解除器に送信される。大半のデジタル放送システム・データ・ストリーム及び大半のデジタル・ケーブル・データ・ストリームは、セキュリティの目的でスクランブルされる。デジタル放送システムのスクランブル解除は、入力データの形式で復号仕様を含む制御語パケットを送受信することによって達成される。復号制御語は、スマート・カードにプログラムされるアルゴリズムによって処理され、それによって、Nビットのスクランブル解除鍵が生成される。現行のシステムは通常、最大56ビットの鍵を利用する。Nビットの鍵は更に、データ暗号化スクランブルを行うよう、伝送レジスタに記憶される。スクランブル解除が行われると、システムは、ビデオ複合ピクチャをメモリ内に、通常はMPEG-2標準によって構築し、所望のピクチャをディスプレイ上に表示する。ユーザがチャンネルを変更すると、システムは現行の復号化処理をディセーブルし、新たなチャンネルのパラメータによって上記の手順全てをやり直す。例えば、天候や、劣悪な信号受信状態が理由で、信号に誤りが存在する場合、ユーザは、チャンネルを変更するのに、更なる遅延時間、待たなければならない。

20

30

【発明の開示】

【発明が解決しようとする課題】

【0006】

チャンネル獲得に関連した遅延は、隣接するチャンネルの順次移動を行うテレビ・ユーザにとって特に気になるものであり、こうした操作は、多くのユーザが、すばやく行いことを好む。部分的には、遅延は、デジタル・コンテンツが暗号化されていることによるものであり、それによって、デコーダが、特定の順次処理でスクランブル解除データを処理することが必要である。本発明は、伝送逆多重化装置及びスマート・カードに焦点を当てて、ユーザ・チャンネル変更時間を、新たなチャンネルをユーザが選択する前に、次の予測チャンネル毎に、スクランブル解除鍵に関連した制御語又は、スクランブル解除鍵を復号化することによって削減する。

40

【課題を解決するための手段】

【0007】

本明細書及び特許請求の範囲開示の本発明は、デジタル伝送をチューニングし、復号化して、2つ以上のチューニング・チャンネルに関連した、Nビットのスクランブル解除鍵群を生成する、チューニング及び復号化の手段と、選択チャンネルに対するスクランブル解除鍵群を出力させて、デジタル情報をビデオ・ディスプレイ内にフォーマットするに必要なデジタル伝送ストリームをスクランブル解除することによって、2つ

50

以上のチューニング・チャンネルのうちの選択された1つに対するユーザ要求に応答する、プログラムされたマイクロプロセッサとを含む。

【0008】

別の実施例では、デジタル・ビデオ伝送受信器装置は、制御語を記憶する装置を備える。これは、デジタル伝送をチューニングし、復号化して、各々がNビットのスクランブル解除鍵と関連した2つ以上のチューニング・チャンネルに関する制御語群を生成する、チューニング及び復号化の手段と、制御語群内の制御語のうちの1つに、選択チャンネルが出力されるうえでのスクランブル解除鍵を出力させて、デジタル情報をデジタル・ディスプレイ内にフォーマットするのに必要なデジタル伝送ストリームをスクランブル解除することによって、2つ以上のチューニング・チャンネルのうちの選択された1つに対するユーザ要求に応答する、プログラムされたマイクロプロセッサとを含む。

10

【発明を実施するための最良の形態】

【0009】

本発明は、添付図面に関して検討すると、以下の詳細な説明から最も良く分かる。添付図面の種々の特徴は、網羅的に規定されているものでない。逆に、種々の特徴は、明瞭にするよう、拡張してもよく、縮減してもよい。

【0010】

本発明は、複数のデジタル・データ伝送ストリームに対する、スクランブル解除鍵の復号化に必要なデジタル・データ入力スクランブル解除制御語、又は生成される、Nビットのスクランブル解除鍵自体を記憶する装置及び方法を開示する。データ制御語を記憶することによって、デジタル・データ・ストリームを復号化する関連スクランブル鍵をスクランブル解除するのに制御語が必要な場合に、後の取り出し時間が削減されることになる。しかし、制御語を利用してNビットのスクランブル解除鍵をスクランブル解除し、更に、Nビットのスクランブル解除鍵を記憶することによって、チャンネル変更時間を削減するうえで最大の利得がもたらされる。複数の番組を同時に監視することは、複数の番組識別情報すなわちPIDをPIDテーブルに追加することによって行うことができる。

20

【実施例】

【0011】

図1を参照すれば、放送システム1は、スクランブル・デジタル情報を受信器100に備え、それには、ユーザによって認識することができるデータ・フレームを組み立てる前にスクランブル解除することを必要とする。ビデオ、オーディオ及びデータの放送システム110は、データ・ストリーム125における各データ・パケット131をPIDルックアップ・テーブル124における既存のエントリと比較するPID比較ブロック122に受信器入力によって受信されるデータ・パケット131を含むデータストリーム125を備える。入力データ・パケット131と既存のエントリとの間で一致が見出されれば、出力データ・パケット130がスクランブル解除器140に転送される。データ・パケット130内では、制御語132は、入力データのビデオ、オーディオ、及びデータのストリームを後に復号化するスクランブル解除鍵を復号するのに必要な情報である復号入力データを備える。復号入力データ制御語132は、通常、その中に含まれる情報を利用してNビットのスクランブル解除鍵185を生成するマイクロプロセッサ170を介してスマート・カード190に備えられる。スクランブル解除鍵185は、伝送レジスタ180に記憶され、伝送レジスタでは、ユーザが認識するのに必要な、スクランブルされたビデオ、オーディオ及びデータを解読するのに鍵を用いる。通常のビデオ・システムでは、スクランブル解除パケット145を用いて、メモリ150におけるビデオ・フレームを、MPEG-2などの既存の標準によって構成する。その後、ビデオ・ディスプレイ160によって、番組を視聴することが可能になる。

30

40

【0012】

ユーザがチャンネルを変更すると、受信器システム100は、それ自体を動作不能にし、データストリーム125におけるデータ・パケット131各々をPIDルックアップ・テーブル124内の既存のエントリと比較するPID比較ブロック122へ入力するよう

50

、データ・パケット131を獲得する上記手順をやり直さなければならない。一致が生じると、復号入力データを備える制御語132は、新たなチャンネルの後のスクランブル解除を行うための56ビット鍵の終局的な生成を行うよう、マイクロプロセッサ170及びスマート・カード190に中継される。

【0013】

図2を参照すれば、放送システム210のユーザがチャンネル変更を開始すると、受信器システム200は、所望の番組に関連した現行のデジタル・データ・ストリームに対する、Nビットの、記憶されたスクランブル解除鍵を変更するだけでよい。バックグラウンドにおいて先行して復号化されたか、それと同時に復号化された、Nビットのスクランブル解除鍵は、何れかの新たに選択されるデジタル・データ・チャンネルのすばやいスクランブル解除を可能にする。本発明が現行の技術に施されれば、こうしたチャンネル変更の方法は、チャンネル選択遅延時間において最大40%の削減を実現することができる。

10

【0014】

図2は本発明を示し、デジタル受信器200は、ユーザによって認識されるようにデジタル情報をフォーマットするのに必要な関連スクランブル解除デジタル伝送ストリーム245によって、選択されるチャンネルに対するスクランブル解除鍵群273を出力させることによって、プログラムされた手段270を利用して、2つ以上のチューニング・チャンネルのうち選択される1つに対するユーザ要求に応答して、2つ以上のチューニング・チャンネル265に関連した、Nビットのスクランブル解除鍵群273を生成する、放送の伝送205を受信する。通常、そうした認識は、選択されるビデオ・ディスプレイ260が、陰極線管上や他のそうした2次元ビデオ・ディスプレイ上にピクチャを投影する場合に達成される。

20

【0015】

前述の監視及び復号化は、Nビットのスクランブル解除鍵の生成に将来、利用されることになる入力スクランブル解除データ制御語294の記憶によって達成することができ、メモリ275における56ビット鍵を直ちに生成することによっても達成することができる。56ビット鍵を記憶することによって、チャンネル変更時間の削減において最大の利得をもたらすが、それは、Nビット鍵を作成するよう適切な番組への入力として制御語を必要とする工程は、それが必要である際に既の実現されているものであるからである。同時のスクランブル・データ・パケットは複数存在するので、各々が、メモリ275内の別の場所に記憶される。複数の番組を同時に監視することは、複数の番組PIDをPIDテーブル230に追加することによって行うことができる。

30

【0016】

本発明は、例として、米国特許第5,933,192号明細書又は米国特許第6,118,498号明細書記載の、予測される次のユーザ・コマンドから導き出される制御語295を監視することによって、ユーザ・チャンネル変更時間を削減する。任意的には、放送システム210におけるチャンネル全てを、衛星受信システム開発の技術分野における当業者によって周知である技術を利用して監視し得る。所望の受信番組の前にスクランブル解除鍵全てを処理することによって、受信システム200は、トランスポンダ上に存在するチャンネル全てを監視することができる。よって、ユーザがチャンネルを変更する場合、チューナ・データ265は、スクランブル・デジタル・データを直ちに復号化させることができるが、それは、復号入力鍵が先行して受信され、スマート・カード290に転送され、その結果、出力鍵群277がメモリ275に記憶されるからである。

40

【0017】

本明細書及び特許請求の範囲記載の本発明は、通常の実験システムでは、ユーザ起動チャンネル変更の完了において約400ミリ秒の処理時間を削減することができる。

【0018】

ストリーム内のスクランブル解除入力データは、データストリームにおいて一周期レートで繰り返される。例として、一商用システムでは、このレートは、最大200ミリ秒で

50

ある。スマート・カード 290 は通常、56 ビット鍵 285 を生成するのに最大 150 秒が許容される。復号器システムは、スマート・カード 290 に応答し、56 ビット鍵 285 を伝送レジスタ 280 に移動させ、生伝送データストリーム 245 の復号化を始めるのに最大 50 ミリ秒が許容される。

【0019】

3つの工程全てが、チャンネル変更毎に順次必要である。

【0020】

ユーザがチャンネル変更を起動させると、システムは、チューナ・データ 265 を介して現行番組から、メモリ 277 内のバックグラウンド復号化 56 ビット鍵に切り替えるだけでよい。プログラミングの技術分野における当業者に周知であるプログラミング手法を利用して、多くの 56 ビット鍵が、アクセス可能な状態で記憶される。

10

【0021】

従来技術では、一般的に、一度に 1 つのビデオ・ストリームのみが表示され、その例外としては、ピクチャ・イン・ピクチャ (PIP) や同様のシステムがあげられる。PIP システムは、2 つ以上のピクチャを同時に表示することを可能にする。しかし、現在、市場に存在するデジタル PIP システムはわずかである。スクランブル解除データの予測的な復号化及び監視は、デジタル PIP とともに用いることができる。更に、本発明は、デジタル PIP 機能の速度を増加させることになるが、それは、2 次チャンネルが既に、ユーザが第 2 のピクチャを表示することを選択する前に、監視され、復号化されているからである。PIP を備えるシステムも、PIP を備えないシステムも本発明の恩恵を受けるものである。

20

【0022】

本明細書及び特許請求の範囲記載の本発明は、スマート・カード 290 が制御語 295 の入力を利用して、N ビット・データ暗号化復号化鍵を生成して、デジタル・データを後にスクランブル解除することを可能にするように入力データストリームをスクランブル解除する方法を含む。スクランブル解除鍵 285 は、生成されると、メモリ 273 に記憶され、伝送データをスクランブル解除デジタル・データ 245 に復号化するように、例えば、N ビット鍵として、56 ビット鍵 280 及び伝送 240 に直ちに利用可能にされる。チャンネルが変更される都度、当該処理は上記工程を繰り返す。

【0023】

特に、図 3 及び図 4 を参照すれば、チャンネル変更可能数は最大、デジタル放送システム 210 によって放送されるチャンネルの数、存在する。しかし、各受信器システム 200 は、変更可能なものの全体集合のうちの部分集合のみを利用し得る。そうした変更可能性が存在するとすれば、更に、図 3 を参照すれば、システム 300 は、ウェイト状態 312 にあるものでなくなり、受信器システム 200 は、視聴可能チャンネル 320 を判定する工程を開始することになる。その後、視聴チャンネルに関連した 56 ビットの鍵 (56 は例証の目的で用いているに過ぎない。) が、復号化され (330)、視聴可能チャンネルがユーザによって選択される場合に取り出し可能な状態で、メモリに記憶される。チャンネルがユーザによって選択された (360) 場合、選択視聴チャンネルに関連した復号化鍵を取り出し (370)、利用して (380)、N ビット・スクランブル解除コードをスクランブル解除する (380)。スクランブル解除鍵を更に用いて、デジタル・データ・ストリームを、視聴者によって認識可能な手段に組み立てる (390)。スクランブル解除鍵が復号化されると、システム 300 は、視聴可能なチャンネル全てがスクランブル解除鍵を復号化させている (330) が、否かを判定する。それらが自らの鍵を復号化させている (330) 場合、システム 300 は、新たな視聴可能性 (355) を待つ (355)。視聴可能性 (355) がなくなっていない場合、判定 (350) によって、当該処理が工程 314 に戻って、新たなスクランブル解除鍵の復号化 (330) の処理が始まる。時間変動放送セキュリティ手法では、判定 350 は、ネットワーク・データ・パケット 220 を常に監視して、新たな制御語が、予測されるチャンネル放送の伝送 205 に施される時点を判定しなければならない。

30

40

50

【0024】

再度、変更可能性が存在するものとする場合、更に、図4を参照すれば、システム400は、ウェイト状態412にないことになり、システムは、視聴可能チャンネル420を判定する工程を開始することになる。その後、スクランブル解除するNビット・スクランブル解除コードに関連した制御語と、関連した視聴チャンネルが復号化され(430)、メモリに記憶され(440)、それらは、視聴可能チャンネルがユーザによって選択される場合に取り出し可能である。チャンネルがユーザによって選択された(460)場合、制御語を取り出し(470)、利用して、Nビット・スクランブル解除コードをスクランブル解除する(480)。スクランブル解除鍵を更に利用して(480)、デジタル・データ・ストリームを、視聴者によって認識可能な手段に組み立てる。制御語が復号化されると(430)、システム(400)は、視聴可能性(450)を有するチャンネル全てが自らの制御語(410)を記憶させているかを判定する。それらが自らの鍵を記憶させている場合(440)、システムは、新たな視聴可能性(455)を待つ(455)。視聴可能性がなくなっていない場合、判定(450)によって、当該処理は工程420に戻り、新たな制御語を記憶する処理が始まる(440)。時間変動放送セキュリティ手法では、判定(450)は、ネットワーク・データ・パケット(220)を常に監視して、新たな制御語が、予測されるチャンネル放送の伝送205に施される時点を判定する。

10

【0025】

本願に示す本発明の形態は、好ましい実施例にすぎないこととする。種々の変更を部分の機能及び配置において行い得る。同等の手段を、本願で例証し、記載したものと置き換え得る。更に、特定の特徴を他のものとは無関係に、本特許請求の範囲記載の、本発明の技術思想及び範囲から逸脱することなく用い得る。

20

【図面の簡単な説明】

【0026】

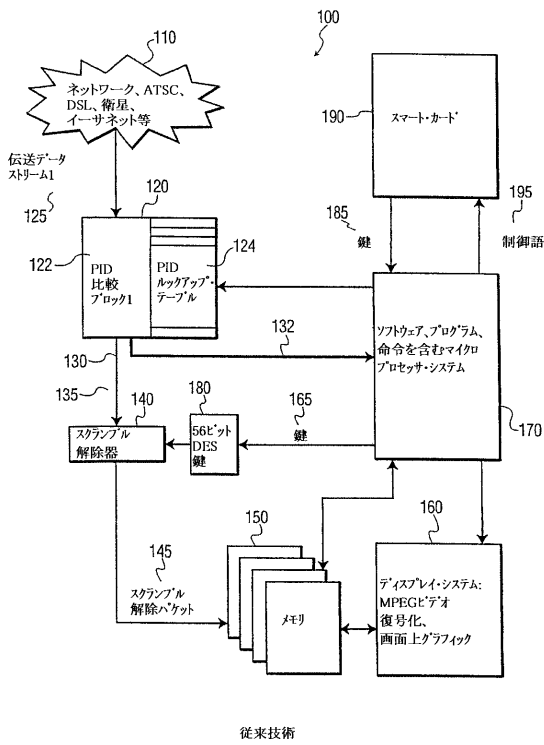
【図1】従来技術の受信装置を示す構成図である。

【図2】本発明を示す構成図である。

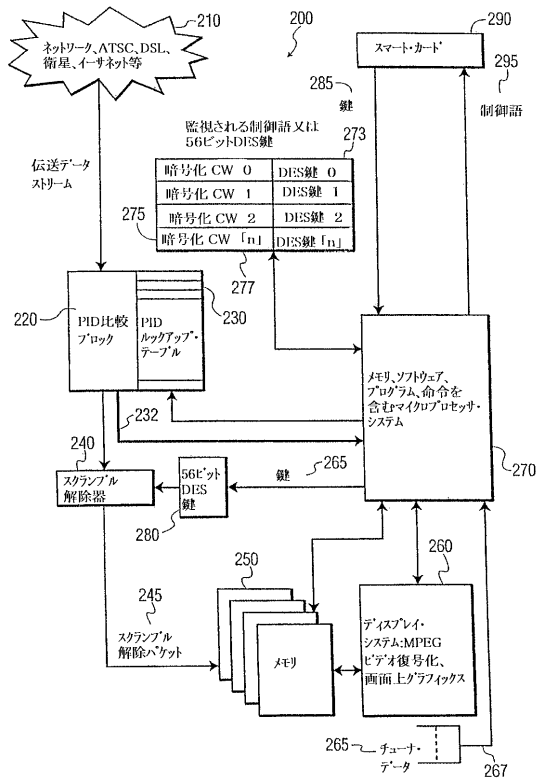
【図3】記憶されている、Nビットの復号化鍵を利用してチャンネル選択における遅延を削減する方法を示す構成図である。

【図4】制御語を利用してチャンネル選択における遅延を削減する方法を示す図である。

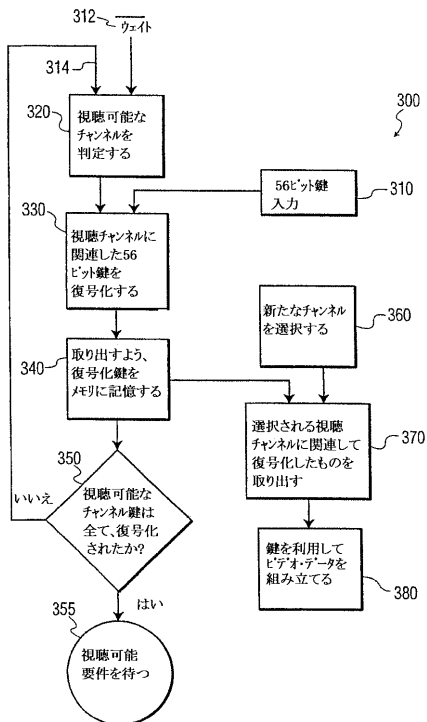
【図1】



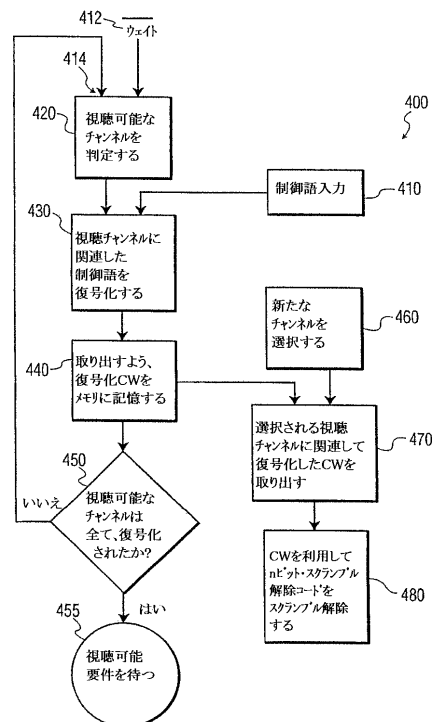
【図2】



【図3】



【図4】



【手続補正書】

【提出日】平成16年11月2日(2004.11.2)

【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】

受信器であって、

デジタル伝送をチューニングし、復号化して、前記デジタル伝送に含まれる各々のチャンネルに関連した制御語を生成するチューニング及び復号化の装置と、

選択されるチャンネルをチューニングし、復号化する旨のユーザ要求に応じて、選択される制御語を用いて、出力される対象の前記選択されるチャンネルに対するスクランブル解除鍵を生成し、前記選択されるチャンネルに関連したデジタル伝送ストリームをスクランブル解除する、プログラムされる手段とを備え、

前記チューニング及び復号化の手段は更に、非選択チャンネルを監視して該非選択チャンネルに関連した制御語を導き出し、該制御語をメモリに記憶し、

該記憶制御語は、前記非選択チャンネルが前記ユーザによって後に選択される場合にデジタル伝送ストリームを復号化するのに用いられることを特徴とする受信器。

【請求項2】

請求項1記載の受信器であって、

前記非選択チャンネルは、更新された制御語について周期的に監視され、前記更新された制御語は、前記メモリに記憶されることを特徴とする受信器。

【請求項3】

請求項1記載の受信器であって、

前記非選択チャンネルは、視聴可能チャンネル群を備えることを特徴とする受信器。

【請求項4】

請求項1記載の受信器であって、

前記制御語を、番組選択操作モードにおいて比較して、所望のデジタル・スクランブル解除鍵ストリームを識別することを特徴とする受信器。

【請求項5】

請求項1記載の受信器であって、

前記制御語群が、前記メモリから取り出され、

制御語のうちの記憶された部分は、所望のデジタル伝送ストリームに関連したスクランブル解除鍵と優劣つけがたいことを特徴とする受信器。

【請求項6】

ビデオ伝送の受信方法であって、

デジタル伝送をチューニングし、復号化して、前記デジタル伝送に含まれる各々のチャンネルに関連したスクランブル解除鍵を生成する工程と、

選択されるチャンネルに対するスクランブル解除鍵を判定し、前記選択されるチャンネルをチューニングし、復号化する旨のユーザ要求に応じて、前記選択されるチャンネルに関連したデジタル伝送ストリームをスクランブル解除する工程と、

非選択チャンネルを監視して該非選択チャンネルに関連したスクランブル解除鍵を導き出し、該スクランブル解除鍵をメモリに記憶する工程とを備え、

該記憶スクランブル解除鍵は、前記非選択チャンネルが前記ユーザによって後に選択される場合にデジタル伝送ストリームを復号化するのに用いられることを特徴とする受信方法。

【請求項7】

請求項6記載の受信方法であって、

前記監視する工程は、更新されたスクランブル解除鍵を判定するよう周期的に行われ、更に、更新されたスクランブル解除鍵を前記メモリに記憶する工程を更に備えることを特徴とする受信方法。

【請求項 8】

請求項 6 記載の受信方法であって、

前記非選択チャンネルは、視聴可能チャンネル群を備えることを特徴とする受信方法。

【請求項 9】

請求項 6 記載の受信方法であって、

前記スクランブル解除鍵を、番組選択操作モードにおいて比較して、所望のデジタル・伝送ストリームを識別することを特徴とする受信方法。

【請求項 10】

請求項 7 記載の受信方法であって、

前記スクランブル解除鍵を前記メモリから取り出す工程を更に備え、

前記スクランブル解除鍵のうちの記憶された部分は、所望のデジタル伝送ストリームと優劣つけがたいことを特徴とする受信方法。

【請求項 11】

受信方法であって、

デジタル伝送における視聴可能チャンネルを判定する工程と、

前記デジタル伝送から、前記視聴可能チャンネルに関連した復号化鍵を、ユーザ選択チャンネルをチューニングし、復号化する間に判定する工程と、

前記復号化鍵を、前記視聴可能チャンネルがユーザによって選択される場合に取り出し可能な状態でメモリに記憶する工程と、

視聴可能性を有するチャンネル全てが各々の復号化鍵を判定させているかを判定し、

視聴可能性を有するチャンネル全てが各々の復号化鍵を判定させている訳でない場合、新たな制御語について前記デジタル伝送を監視し続ける工程とを備えることを特徴とする受信方法。

【請求項 12】

請求項 11 記載の受信方法であって、

新たに選択される視聴チャンネルに関連したスクランブル解除鍵を前記メモリから取り出す工程を更に備えることを特徴とする受信方法。

【請求項 13】

請求項 12 記載の受信方法であって、

前記選択される視聴チャンネルに関連した前記スクランブル解除鍵を利用して、前記新たに選択される視聴チャンネルに関連したデジタル伝送ストリームをスクランブル解除する工程を更に備えることを特徴とする受信方法。

【請求項 14】

請求項 11 記載の受信方法であって、

判定する工程が、時間変動セキュリティ手法に必要な、更新される復号化鍵を周期的に判定する工程を備えることを特徴とする受信方法。

【請求項 15】

受信方法であって、

デジタル伝送における視聴可能チャンネルを判定する工程と、

前記デジタル伝送から、前記視聴可能チャンネルに関連した制御語を、ユーザ選択チャンネルをチューニングし、復号化する間に判定する工程と、

前記制御語を、前記視聴可能チャンネルがユーザによって選択される場合に取り出し可能な状態でメモリに記憶する工程と、

視聴可能性を有するチャンネル全てが各々の制御語を判定させているかを判定し、

視聴可能性を有するチャンネル全てが各々の制御語を判定させている訳でない場合、新たな制御語について前記デジタル伝送を監視し続ける工程とを備えることを特徴とする

受信方法。

【請求項 16】

請求項 15 記載の受信方法であって、
スクランブル解除コードを前記制御語から生成し、
選択されるチャンネルに関連したデジタル伝送ストリームを、前記スクランブル解除コードを用いてスクランブル解除する工程を更に備えることを特徴とする受信方法。

【請求項 17】

請求項 16 記載の受信方法であって、
新たに選択される視聴チャンネルに関連した所要制御語を前記メモリから取り出す工程を更に備えることを特徴とする受信方法。

【請求項 18】

請求項 17 記載の受信方法であって、
前記所要制御語を利用して、所要スクランブル解除コードを生成し、該所要スクランブル解除コードを用いて、前記新たに選択される視聴チャンネルに関連したデジタル伝送ストリームを処理する工程を更に備えることを特徴とする受信方法。

【請求項 19】

請求項 15 記載の受信方法であって、
前記判定する工程が、時間変動セキュリティ手法に必要な、更新される復号化鍵を周期的に判定する工程を備えることを特徴とする受信方法。

【手続補正書】

【提出日】平成 18 年 12 月 7 日 (2006.12.7)

【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】

受信器であって、
デジタル伝送をチューニングし、復号化して、前記デジタル伝送に含まれる各々のチャンネルに関連した制御語を生成するチューニング及び復号化の装置と、
選択されるチャンネルをチューニングし、復号化する旨のユーザ要求に応じて、選択される制御語を用いて、出力される対象の前記選択されるチャンネルに対するスクランブル解除鍵を生成し、前記選択されるチャンネルに関連したデジタル伝送ストリームをスクランブル解除する、プログラムされる手段とを備え、
前記チューニング及び復号化の手段は更に、非選択チャンネルを監視して該非選択チャンネルに関連した制御語を導き出し、該制御語をメモリに記憶し、
該記憶制御語は、前記非選択チャンネルが前記ユーザによって後に選択される場合にデジタル伝送ストリームを復号化するのに用いられることを特徴とする受信器。

【請求項 2】

請求項 1 記載の受信器であって、
前記非選択チャンネルは、更新された制御語について周期的に監視され、前記更新された制御語は、前記メモリに記憶されることを特徴とする受信器。

【請求項 3】

請求項 1 記載の受信器であって、
前記非選択チャンネルは、視聴可能チャンネル群を備えることを特徴とする受信器。

【請求項 4】

請求項 1 記載の受信器であって、
前記制御語を、番組選択操作モードにおいて比較して、所望のデジタル・スクランブル解除鍵ストリームを識別することを特徴とする受信器。

【請求項 5】

請求項 1 記載の受信器であって、
前記制御語群が、前記メモリから取り出され、
制御語のうちの記憶された部分は、所望のデジタル伝送ストリームに関連したスクランブル解除鍵と優劣つけがたいことを特徴とする受信器。

【請求項 6】

ビデオ伝送の受信方法であって、
デジタル伝送をチューニングし、復号化して、前記デジタル伝送に含まれる各々のチャンネルに関連したスクランブル解除鍵を生成する工程と、
選択されるチャンネルに対するスクランブル解除鍵を判定し、前記選択されるチャンネルをチューニングし、復号化する旨のユーザ要求に応じて、前記選択されるチャンネルに関連したデジタル伝送ストリームをスクランブル解除する工程と、
非選択チャンネルを監視して該非選択チャンネルに関連したスクランブル解除鍵を導き出し、該スクランブル解除鍵をメモリに記憶する工程とを備え、
該記憶スクランブル解除鍵は、前記非選択チャンネルが前記ユーザによって後に選択される場合にデジタル伝送ストリームを復号化するのに用いられることを特徴とする受信方法。

【請求項 7】

請求項 6 記載の受信方法であって、
前記監視する工程は、更新されたスクランブル解除鍵を判定するよう周期的に行われ、
更に、
更新されたスクランブル解除鍵を前記メモリに記憶する工程を更に備えることを特徴とする受信方法。

【請求項 8】

請求項 6 記載の受信方法であって、
前記非選択チャンネルは、視聴可能チャンネル群を備えることを特徴とする受信方法。

【請求項 9】

請求項 6 記載の受信方法であって、
前記スクランブル解除鍵を、番組選択操作モードにおいて比較して、所望のデジタル・伝送ストリームを識別することを特徴とする受信方法。

【請求項 10】

請求項 7 記載の受信方法であって、
前記スクランブル解除鍵を前記メモリから取り出す工程を更に備え、
前記スクランブル解除鍵のうちの記憶された部分は、所望のデジタル伝送ストリームと優劣つけがたいことを特徴とする受信方法。

【請求項 11】

受信方法であって、
デジタル伝送における視聴可能チャンネルを判定する工程と、
前記デジタル伝送から、前記視聴可能チャンネルに関連した復号化鍵を、ユーザ選択チャンネルをチューニングし、復号化する間に判定する工程と、
前記復号化鍵を、前記視聴可能チャンネルがユーザによって選択される場合に取り出し可能な状態でメモリに記憶する工程と、
視聴可能性を有するチャンネル全てが各々の復号化鍵を判定させているかを判定し、
視聴可能性を有するチャンネル全てが各々の復号化鍵を判定させている訳でない場合、
新たな制御語について前記デジタル伝送を監視し続ける工程とを備えることを特徴とする受信方法。

【請求項 12】

請求項 11 記載の受信方法であって、
判定する工程が、時間変動セキュリティ手法に必要な、更新される復号化鍵を周期的に判定する工程を備えることを特徴とする受信方法。

【 国際調査報告 】

INTERNATIONAL SEARCH REPORT

International Application No
PCT/US2004/001573

A. CLASSIFICATION OF SUBJECT MATTER IPC 7 H04N5/00		
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) IPC 7 H04N		
Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched		
Electronic data base consulted during the international search (name of data base and, where practical, search terms used) EPO-Internal		
C. DOCUMENTS CONSIDERED TO BE RELEVANT		
Category *	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	US 5 594 492 A (LEW EUGENE L ET AL) 14 January 1997 (1997-01-14) abstract	1-16
Y	column 7, lines 7-35 figures 4,5,element426,element560	17-22
Y	US 5 933 192 A (CROSBY JEFFREY W ET AL) 3 August 1999 (1999-08-03) abstract	17-22
X	US 6 466 671 B1 (BENARDEAU CHRISTIAN ET AL) 15 October 2002 (2002-10-15) column 21, line 12 - column 23, line 30 abstract column 1, line 33 - column 2, line 4 figures 2,element3020 figures 18,19	1-16
-/--		
<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 : *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 9 June 2004		Date of mailing of the international search report 19/07/2004
Name and mailing address of the ISA European Patent Office, P. B. 5518 Patentlaan 2 NL - 2280 HV Rijswijk Tel: (+31-70) 340-2040, Tx. 31 851 epo nl, Fax: (+31-70) 340-3010		Authorized officer Marzal-Abarca, X

INTERNATIONAL SEARCH REPORT

International Application No PCT/US2004/001573

C.(Continuation) DOCUMENTS CONSIDERED TO BE RELEVANT		
Category *	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	US 2002/152459 A1 (BATES CARY LEE ET AL) 17 October 2002 (2002-10-17) abstract paragraphs '0003!, '0004! paragraph '0022! claims 1,2	17-22
A	US 6 591 013 B1 (TAUNTON MARK) 8 July 2003 (2003-07-08) abstract column 1, lines 57-63 column 5, lines 22-58 figures 4,6a,6b,6c	17-22

INTERNATIONAL SEARCH REPORT

Information on patent family members

International Application No

PCT/US2004/001573

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
US 5594492	A	US 5477263 A	19-12-1995
US 5933192	A	NONE	
US 6466671	B1	WO 9843425 A1	01-10-1998
		AT 227492 T	15-11-2002
		AT 228746 T	15-12-2002
		AT 232670 T	15-02-2003
		AT 228747 T	15-12-2002
		AT 233415 T	15-03-2003
		AT 247297 T	15-08-2003
		AT 225108 T	15-10-2002
		AT 226003 T	15-10-2002
		AT 228289 T	15-12-2002
		AT 226378 T	15-11-2002
		AU 742213 B2	20-12-2001
		AU 746305 B2	18-04-2002
		AU 745783 B2	28-03-2002
		AU 741114 B2	22-11-2001
		AU 754166 B2	07-11-2002
		AU 746178 B2	18-04-2002
		AU 744517 B2	28-02-2002
		AU 2770697 A	20-10-1998
		AU 742956 B2	17-01-2002
		AU 742067 B2	13-12-2001
		AU 740740 B2	15-11-2001
		AU 744977 B2	07-03-2002
		AU 739663 B2	18-10-2001
		AU 745672 B2	28-03-2002
		AU 740887 B2	15-11-2001
		AU 7038198 A	20-10-1998
		AU 740632 B2	08-11-2001
		AU 740224 B2	01-11-2001
		BR 9714590 A	17-09-2002
		BR 9714591 A	17-09-2002
		BR 9714598 A	06-08-2002
		BR 9714599 A	10-09-2002
		BR 9714600 A	10-09-2002
		BR 9714601 A	10-09-2002
		BR 9714602 A	17-09-2002
		BR 9714603 A	16-05-2000
		BR 9714604 A	06-08-2002
		BR 9714627 A	06-08-2002
		BR 9714649 A	06-08-2002
		BR 9808283 A	16-05-2000
		BR 9808288 A	16-05-2000
		BR 9808385 A	22-04-2003
		BR 9808386 A	22-04-2003
		CA 2284011 A1	01-10-1998
		CA 2284014 A1	01-10-1998
		CA 2284016 A1	01-10-1998
		CA 2284018 A1	01-10-1998
		CA 2284022 A1	01-10-1998
		CA 2284023 A1	01-10-1998
US 2002152459	A1	NONE	
US 6591013	B1	WO 0057646 A1	28-09-2000

INTERNATIONAL SEARCH REPORT
Information on patent family members

International Application No
PCT/US2004/001573

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
US 6591013	B1	GB 2363276 A ,B US 2003194139 A1	12-12-2001 16-10-2003

フロントページの続き

(81) 指定国 AP(BW, GH, GM, KE, LS, MW, MZ, 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, IT, LU, MC, NL, 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 グライムス, ケヴィン

アメリカ合衆国, ミネソタ州 5 5 3 1 1, メイプル・グローブ, リウエルウッド・プレイス 8
2 7 6

Fターム(参考) 5C164 MB31S PA21 UB10S UB21 UB21P UB36S UB41 UB41S UC22 UC22P
UD51 UD51S YA04 YA21
5J104 EA17 EA18 PA05

【要約の続き】

クランブル解除鍵をスクランブル解除し、更に、Nビット・スクランブル解除鍵を記憶することによって、通常、チャンネル変更時間を削減するうえでの最大の利得をもたらす。