(19)日本国特許庁(JP)　(12)特　許　公　報(B2)　(11)特許番号

特許第4322695号
(P4322695)

(45)発行日　平成21年9月2日(2009.9.2)　(24)登録日　平成21年6月12日(2009.6.12)

(51)Int.Cl.		F I		
G11B 20/10	(2006.01)	G11B	20/10	301Z
H04L 9/08	(2006.01)	H04L	9/00	601A
H04N 5/91	(2006.01)	H04N	5/91	Z

請求項の数 3　(全 16 頁)

(21)出願番号　特願2004-33668(P2004-33668)
(22)出願日　平成16年2月10日(2004.2.10)
(65)公開番号　特開2004-247036(P2004-247036A)
(43)公開日　平成16年9月2日(2004.9.2)
審査請求日　平成19年2月7日(2007.2.7)
(31)優先権主張番号　0301857
(32)優先日　平成15年2月11日(2003.2.11)
(33)優先権主張国　フランス(FR)

(73)特許権者　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】スクランブルデジタルデータを記録する方法、記録媒体及びかかるデータの読み取り方法

(57)【特許請求の範囲】
【請求項１】
データ記録媒体に記録されるスクランブルされたデジタルデータを読取る方法であって、
前記データ記録媒体は、
データパケットと多重化されるコントロールパケットであって、デジタルデータの一部をデスクランブルするための少なくとも１つのキーをそれぞれが含むコントロールパケットを備えるスクランブルされたデジタルデータストリームと、
前記データストリームとは別に記憶されるテーブルであって、少なくとも１つのコントロールパケットと、それぞれのコントロールパケットについて、前記データストリームにおける前記コントロールパケットの位置を示すインデックスであって、前記データストリームにおける前記コントロールパケットの直前及び前記コントロールパケットの直後に送信されるクロック基準値に関して前記データストリームにおける前記コントロールパケットの位置を定義するタイムスタンプを含むインデックスとを含むテーブルとを有し、
当該方法は、
（ｉ）記録されたデータのストリームからデータのブロックを選択するステップと、
（ｊ）前記データブロックから、少なくとも１つのクロック基準値を抽出するステップと、
（ｋ）抽出されたクロック基準値の関数として、前記ステップ（ｉ）で選択された前記データブロックに含まれる最初のパケットと最後のパケットに関連するタイムスタンプを

推定するステップと、
（ｌ）前記ステップ（ｋ）で推定されたタイムスタンプを使用して、このデータブロックに対応する少なくとも１つのコントロールパケットを前記データと記録されるテーブルから抽出するステップと、
（ｍ）前記コントロールパケットから、デスクランブルキーを抽出するステップと、
（ｎ）前記デスクランブルキーを使用して、前記データブロックをデスクランブルして、その内容を明確な表示でユーザに供給するステップと、
を備える方法。
【請求項２】
前記ステップ（ｉ）は、
前記データブロックの最初のパケットに関連するタイムスタンプよりも小さな最も大きなインデックスを有するコントロールパケットと、前記データブロックの最後のパケットに関連するタイムスタンプよりも小さな最も大きなインデックスを有するコントロールパケットとの間にあるコントロールパケットであって、前記データブロックの最初のパケットに関連するタイムスタンプよりも小さな最も大きなインデックスを有するコントロールパケットと、前記データブロックの最後のパケットに関連するタイムスタンプよりも小さな最も大きなインデックスを有するコントロールパケットを含むコントロールパケットを抽出するステップを含む、
請求項１記載の方法。
【請求項３】
前記コントロールパケットからデスクランブルキーを抽出する前記ステップ（ｍ）は、前記コントロールパケット又は前記デスクランブルキーを暗号解読するステップを備える、
請求項１記載の方法。

【発明の詳細な説明】
【技術分野】
【０００１】
本発明は、圧縮及びスクランブルされたデジタルデータの記録の分野に関する。本発明は、より詳細には、スクランブルデジタルデータの記録方法、及びかかるデータの読み取り方法に関する。
【背景技術】
【０００２】
圧縮されたデジタルデータストリーム、特にデジタルテレビ信号を記録するための装置は、現在ではあちこちに見られる。このタイプの装置は、たとえばハードディスクの形態を採用し、アナログテレビ番組についてビデオレコーダで予めリードバックするために使用したように、続いてリードバックすることができるデジタルテレビ番組を記録するための機能をユーザに対して提供する。
【０００３】
データ、特にテレビ番組が記録されるとき、魅力的な機能は、「巻き戻し再生」又は「順方向早送り」、或いは加速された巻き戻し再生のような、用語「トリックプレイモード」としばしば呼ばれる特定の読み取りモードに従って、これらのデータを読取りすることからなる。別の魅力的なモードは、番組の特定の部分に直接アクセスすること、すなわちデータにおいて「ジャンプ」することができることからなる。
【０００４】
これらの読取りモードは、たとえばＭＰＥＧ－２標準に従って圧縮及び符号化されたデジタルデータに関して実現することは常に容易ではない。特に、圧縮及び符号化技術は、デジタルデータの転送向けに本質的に使用されるように設計されている。結果的に、データの復号化は、通常のスピードでの「早送り再生」モードで行われることが意図されている。ＭＰＥＧ－２標準に従って圧縮及び符号化されたデジタルオーディオ／ビデオデータ

が、たとえば巻き戻し再生モードで読み取られるとき、ある複数の画像を表示するために、該複数の画像のうちの１つを表示可能となる前に、幾つかの画像をデコードすることが必要な場合がある。

【０００５】

記録されたデジタルデータがスクランブルされたとき（又は「暗号化“ｅｎｃｉｐｈｅｒｅｄ”“ｅｎｃｒｙｐｔｅｄ”」と呼ぶ）、「トリックプレイモード」を実現することはさらに困難である。実際、デスクランブルすることができる前に、デスクランブルのキーを取り戻し、次いでデータを復号することが必要である。デジタルペイテレビの分野で使用されている最も通常的なスクランブル方法によれば、データのスクランブルキーは、デジタルデータストリームにおけるＥＣＭ（Ｅｎｔｉｔｌｅｍｅｎｔ　Ｃｏｎｔｒｏｌ　Ｍｅｓｓａｇｅ：共通情報）と示されるデータパケットで転送される。データをスクランブルするために使用される（また、データをデスクランブルするために利用される）キーは、ＣＷ（「コントロールワード“ｃｏｎｔｒｏｌ　ｗｏｒｄ”」を意味する）と示され、典型的には１０秒毎に周期的に変化する。ＥＣＭは、たとえば１００ｍｓごとに繰り返すことによりデータストリームで転送され、その内容は約１０秒ごとに変化する。デジタルデータパケットをデスクランブルするために、このデータパケットをデスクランブルするためのＣＷキーを含むＥＣＭを最初に取り戻すことが必要である。

【０００６】

ＥＣＭは、偶数キー（ｅｖｅｎ　ｋｅｙ）と奇数キー（ｏｄｄ　ｋｅｙ）という２つのＣＷキーを通常含んでいる。デジタルデータ転送パケットは、特にＤＶＢ規格（Ｄｉｇｉｔａｌ　Ｖｉｄｅｏ　Ｂｒｏａｄｃａｓｔｉｎｇを意味する）に従い符号化されるか、ＡＴＳＣ規格（Ａｄｖａｎｃｅｄ　Ｔｅｌｅｖｉｓｉｏｎ　Ｓｙｓｔｅｍｓ　Ｃｏｍｍｉｔｔｅｅを意味する）に従い符号化されており、パケットがスクランブルされているか否か、スクランブルされている場合に偶数キーでスクランブルされているか、或いは奇数キーでスクランブルされているかを示すスクランブル指標（すなわち「フラグ」）をヘッダに含んでいる。したがって、ＥＣＭは、ストリームで転送される次のデータパケットをデスクランブルするために必要なＣＷキーを常に含んでいる。ＣＷキーに含まれる第二のＣＷキーは、データストリームにおけるＥＣＭの前に転送される所定のデータパケットをデスクランブルするか、又はストリームにおけるＥＣＭの後に転送される所定のデータパケットをデスクランブルするために役立つ。

【０００７】

図１は、この原理を図解的に例示している。様々なＣＷキーでスクランブルされたデータストリーム１０が表されている。周期ｎ－１に対応するデータパケット１００は、キーCW_{n-1}でスクランブルされており、周期ｎに対応するデータパケット１０１は、キーCW_{n}でスクランブルされており、及び周期ｎ＋１に対応するデータパケット１０２は、キーCW_{n+1}でスクランブルされることが想定されている。それぞれの「キー周期」は、データの最後をスクランブルするためにキーが使用される周期に対応しており、図１の例に従えば１０秒である。

【０００８】

図１では、データストリームで転送されるＥＣＭが表されている。より明確にするために、これらのＥＣＭは、データストリームから分離して表されているが、勿論、実際にＥＣＭはデータストリームで転送される。図１に表される例では、これらのＥＣＭは１００ｍｓごとに転送され、図１の下に明確にされるように、２つのＣＷキーをそれぞれ含んでいる。これらのキーは、データストリーム１０をスクランブルするために使用される期間に対応するクロスハッチング又はスクエアハッチングにより図解的に表されている。図１では、周期ｎ－１の終了と周期ｎ＋１の開始とを伴って、周期ｎのみが詳しく示されている。

【０００９】

図１に例示されるように、周期ｎの間、データストリームで転送されるＥＣＭの内容は変化する。開始では、ＥＣＭは、前の周期に対応するキーCW_{n-1}、及び現在の周期に

対応するキーＣＷ$_n$を含んでいる。次いで、その内容は変わり、ＥＣＭは、現在の周期に対応するキーＣＷ$_n$、及び次の周期に対応するキーＣ$_{n+1}$を含んでいる。あるキーＣＷでスクランブルされたデータストリームが転送される前に、このキーＣＷがＥＣＭで転送される周期は、「ＥＣＭアドバンス」と呼ばれる。このＥＣＭアドバンスは、０とキー周期（１０秒）の間に持続する。

【発明の開示】

【発明が解決しようとする課題】

【００１０】

それゆえ、データストリームの読取り方向に従うと共に、読取り速度に従って、あるケースでは、データを受信する前にデータをデスクランブルするために必要なＣＷキーを取り戻すことが困難な場合があることを注目すべきである。特に、ＣＷキーは暗号化されることでＥＣＭにおいて転送され、データのデスクランブルのためのデータストリーム受信装置により利用可能となる前に、該受信装置に接続されるスマートカードで一般に暗号解読（ｄｅｃｒｙｐｔｅｄ）される必要があることが指摘されるべきである。

【００１１】

欧州特許ＥＰ１１４３７２２Ａ１は、このタイプのデータストリームの巻き戻し再生の読取りを容易にするためのソリューションを提案する。このソリューションは、現在の周期のキー、前の周期のキー及び次の周期のキーである３つのＣＷキーをそれぞれのＥＣＭに挿入することからなる。しかしながら、このソリューションは、加速された読取りモード（順方向早送り、加速された巻き戻し再生）向けに満足されるものではなく、また、デジタルデータストリームにおけるあるデータブロックから別のデータブロックへの高速な「ジャンプ」を実行することが可能にするものでもない。

【課題を解決するための手段】

【００１２】

本発明は、スクランブルデジタルデータを記録する方法を提案することで、これらの課題を解決する。本方法は、以下のステップを備える。（ａ）スクランブルされたデジタルデータストリームを受信するステップ、（ｂ）該データストリームにおいて、該ストリームのデータの少なくとも１部をデスクランブルするための少なくとも１つのキーを含んだコントロールパケットを識別するステップ、（ｃ）該コントロールパケットをテーブルに記憶するステップ、及び（ｄ）該データストリームと該テーブルをデータ記録媒体に記録するステップ。

【００１３】

本発明の特定の機能によれば、上記ステップ（ａ）で受信されたデータストリームが、少なくとも１つのデスクランブルキーを含んだ複数のコントロールパケットを備えている場合、上記記憶するステップ（ｃ）は、上記ステップ（ｂ）で識別されたコントロールパケットがテーブルに既に記憶されていない場合にのみ実行される。ステップ（ｃ）では、データストリームにおけるコントロールパケットの位置を示すインデックスが該テーブルに更に記憶され、該インデックスは、該記録されたデータストリームの最初のパケットに関して該コントロールパケットのシリアル番号を備えているか、代替的に、該インデックスは、該コントロールパケットに関連し、該データストリームで転送されるクロック基準参照値に関して該データストリームにおけるその位置を定義するタイムスタンプを備える。

【００１４】

また、本発明は、データ記録媒体に関する。この記録媒体は、デジタルデータの一部をデスクランブルするための少なくとも１つのキーをそれぞれ含むコントロールパケットを備えるスクランブルされたデジタルデータストリームを含んでいる。該コントロールパケットは、該データパケットと多重化されている。本発明は、該データストリームとは別々に記憶され、少なくとも１つのコントロールパケットを含んだテーブルをさらに含むことを特徴とする。

【００１５】

本発明によるデータ記録媒体は、１つ以上の特徴をさらに備えている。テーブルは、それぞれのコントロールパケットについて、データストリームにおけるコントロールパケットの位置を示すインデックスを含んでいる。インデックスは、記録されたデータパケットの最初のパケットに関するコントロールパケットのシリアル番号を備えている。インデックスは、該コントロールパケットに関連し、データストリームで転送されるクロック基準参照値に関してデータストリームにおけるその位置を定義するタイムスタンプを備えている。

【００１６】

また、本発明は、先の方法に従い記録されたスクランブルデジタルデータを読み取るための方法に関し、以下のステップを備えている。（ｉ）記録されたデータのストリームからデータのブロックを選択するステップ、（ｊ）このデータのブロックに対応するコントロールパケットをテーブルから抽出するステップ、（ｋ）デスクランブルキーをコントロールパケットから抽出するステップ、及び（ｌ）デスクランブルキーを使用して、データブロックをデスクランブルして、その内容を明確な表示でユーザに供給するステップ。

【００１７】

本発明によるデータ読取り方法は、１つ以上の以下の特徴をさらに備えている。コントロールパケットからのデスクランブルキーを抽出する上記ステップ（ｋ）は、コントロールパケット又はデスクランブルキーを暗号化するステップを備えている。本方法は、上記ステップ（ｉ）で選択されたデータブロックに含まれる最初のパケットと最後のパケットのシリアル番号を選択するステップをさらに備えており、ステップ（ｊ）において、データブロックの最初のパケットのシリアル番号よりも小さい最も大きなインデックスを有するコントロールパケットと、該データブロックの最後のパケットのシリアル番号よりも小さい最も大きなインデックスを有するコントロールパケットとの間にあって、これら２つのコントロールパケットを含むコントロールパケットが該テーブルから抽出される。

【００１８】

本方法は、データブロックから少なくとも１つのクロック基準参照値を抽出すること、該抽出された１つ以上のクロック基準参照値の関数として、上記ステップ（ｉ）で選択されたデータブロックに含まれる最初のパケットと最後のパケットに関連するタイムスタンプを推定すること、及び、ステップ（ｊ）において、データブロックの最初のパケットに関連するタイムスタンプよりも小さい最も大きなインデックスを有するコントロールパケットと、データブロックの最後のパケットに関連するタイムスタンプよりも小さい最も大きなインデックスを有するコントロールパケットとの間にあって、これら２つのコントロールパケットを含むコントロールパケットをテーブルから抽出することをさらに備えている。

【００１９】

本発明は、添付図面を参照して、例示により与えられる以下の発明の実施の形態を良好に理解される。

【発明を実施するための最良の形態】

【００２０】

本発明の基本的な概念は、データ記録の間に、記録されたデータの読み取りの間に適切なＣＷキーを含んでいるＥＣＭを非常に迅速に取り戻すように、ＥＣＭのテーブルを作成することである。これにより、有利なことに、ＣＷキーを取り戻すために、データをデスクランブルするために必要であって、したがってＥＣＭを暗号解読することができるために必要な短い時間に関して、事前にＥＣＭへのアクセスを得ることが可能となる。

【００２１】

したがって、本発明は、有利なことに、記録されるときにスクランブルされるデジタルデータに関する変化する「トリックプレイ」モードを実行することができる。

【００２２】

この原理は、記録されるそれぞれの番組についてＥＣＭテーブルを記録することからなり、このテーブルは、番組をデスクランブルするために必要な全てのＥＣＭを含んでいる

。特に、番組がデジタルオーディオ及びビデオデータ、並びに考えられる他のデータストリームを備えている場合、これら様々なストリームをデスクランブルするために必要な全てのＥＣＭは、この番組についてのＥＣＭテーブルに記録される。

【００２３】

また、その内容がデータストリームで前に転送された内容に関して異なるＥＣＭのみがＥＣＭテーブルに記録される。したがって、図１に表されているデータストリームのその一部について、キーＣＷ$_{n-1}$及びＣＷ$_{n}$を含んでいるＥＣＭ、キーＣＷ$_{n}$及びＣＷ$_{n+1}$を含んでいるＥＣＭ、並びにＣＷ$_{n+1}$及びＣＷ$_{n+2}$を含んでいるＥＣＭは、ＥＣＭテーブルに記録される。ＥＣＭの内容が「キー周期“ｋｅｙ　ｐｅｒｉｏｄ”」あたり一回おおよそ変化するので、「キー周期」あたりＥＣＭのうちの１つを記録することが必要なだけである。

【００２４】

本発明の別の観点によれば、記録されるＥＣＭのそれぞれについて、特定のデータパケットをデスクランブルするために必要なＥＣＭを非常に迅速に取り戻すことが続いてできるように、ＥＣＭインデックスがＥＣＭテーブルに記録される。

【００２５】

好適な実施の形態によれば、このＥＣＭインデックスは、データストリームにおけるＥＣＭの位置を示しているＥＣＭパケットのシリアル番号を生成することにより作成される。第二の実施の形態によれば、ＥＣＭインデックスは、スタンプ、すなわち、データストリームで転送されるクロックの値に関してデータストリームにおけるその位置を定義するＥＣＭに関連するタイムスタンプを計算することにより作成される。

【００２６】

図２では、本発明の実施例が示されている。記録装置１は、記録される入力データのストリームを受信する。このデジタルデータのストリームは、コントロールワード、すなわちキーＣＷにより、デジタルペイＴＶの原理に従って一般的にスクランブルされている。このキーＣＷは、所定の周期（たとえば、１０秒毎）で更新され、既に説明された図１において例示されるＥＣＭと示されているコントロールメッセージに挿入される。

【００２７】

記録装置は、たとえばハードディスクのような記録されたデータを蓄積するための手段を備えており、デジタルバス３を介して表示装置２に接続されている。また、記録装置は、カセットのような磁気メディアにデータを記録するデジタルビデオレコーダ、又は光メディア（「コンパクトディスク」を意味するＣＤ、又は「デジタル多用途ディスク」を意味するＤＶＤ）にデータを記録する光ディスクライタとすることができる。

【００２８】

表示装置２は、たとえば、デジタルテレビ受信機であり、この受信機は、ＥＣＭを暗号解読し、受信されたデータをデスクランブルし、及び該デスクランブルされたデータをデコードしてユーザに提供するための要素を少なくとも含んでいる。記録されたデータは、典型的にはオーディオ／ビデオデータであり、そのユーザへの提供は、ビデオデータに関してはスクリーンへの表示により実行され、オーディオデータに関してはスピーカへの転送により実行される。また、表示装置２は、ユーザインタフェースを備えている。このインタフェースにより、ユーザは、順方向早送り、巻き戻し再生、スローモーション、ある番組から別の番組へのジャンプ等のような「トリックプレイ」に従い記録されたデータをリードバックすることができる。

【００２９】

デジタルバス３は、たとえば、ＩＥＥＥ１３９４規格に準拠するバスである。

【００３０】

本発明は、当然、この構成に限定されるものではない。特に、記録装置１及び表示装置所定の要素（ＥＣＭの暗号解読、データのデスクランブル及びデコード）を１つの同じ機器に含めることも可能である。この機器は、この場合、ユーザへのデータの提供のための一般のテレビジョンに接続される。

【００３１】
データストリームを記録するとき、記録装置１は、ＥＣＭを抽出して、データストリームの記録された部分をデスクランブルするために必要な全てのＥＣＭを含んでいるＥＣＭテーブルを同時に作成するために、ストリームを分析する。以下、ＤＶＢデジタルテレビ伝送規格に準拠して伝送され、ＭＰＥＧ－２規格（ＩＴＵ－Ｔ　Ｒｅｃ．Ｈ．２２２．０｜ＩＳＯ／ＩＥＣ　１３８１８－１）に準拠して符号化される、オーディオビジュアルプログラムをユーザが記録することを想定している。しかし、本発明は、勿論、ＭＰＥＧ－２規格以外の圧縮規格に従ってエンコードされていようとなかろうと、ＤＶＢ規格以外の特定の放送規格に従ってブロードキャストされていようとなかろうと、特定の読み取りモード（「トリックプレイ」モード）を実行するために有効な場合がある任意のタイプのデジタルデータに適用される。

【００３２】
記録される特定の番組に対応するＥＣＭは、ＰＩＤを含むデータトランスポートパケットのＰＩＤ（「パケット識別子」を意味する）により、データストリームにおいて識別される。このＰＩＤは、伝送される番組のそれぞれに関連するＰＭＴ（「プログラムマップテーブル」を意味する）において、それ自身が示される。記録装置１は、このＰＩＤを使用して、該記録装置が記録する番組のＥＣＭを抽出する。

【００３３】
テーブルにＥＣＭを記録するための処理が以下に説明される。記録装置１が記録されたデータストリームの最初のＥＣＭを受信したとき、該最初のＥＣＭをＥＣＭテーブルに記憶する。記録装置１が次のＥＣＭを受信したとき、該受信装置は、該次のＥＣＭを前に記録したＥＣＭと比較し、その内容が同一である場合には該次のＥＣＭを無視し、その内容が同一ではない場合には該次のＥＣＭも記憶する。このように、全ての受信されたＥＣＭについて処理が継続される。

【００３４】
例として、２．５時間（すなわち、９０００秒）続く映画について、１つのＥＣＭストリームがオーディオ及びビデオについて必要な場合、（その内容は約１０秒毎に更新されるため）約９００の異なるＥＣＭが存在する。それぞれのＥＣＭは、（前述のＭＰＥＧ規格では）１８８バイトのデータトランスポートパケットに記憶され、したがって、ＥＣＭテーブルは、１８８×９００バイト、すなわち１６９２００バイトを含む必要がある。

【００３５】
また、記録装置１は、テーブルに記憶されるＥＣＭのそれぞれについて、データストリームにおけるＥＣＭの位置を記憶することを可能にするインデックスを作成する。このインデックスは、テーブルに記憶されるものであって、その後、表示装置２により使用されて、データの特定部分をデスクランブルするために必要なＥＣＭを容易に取り戻すことができる。

【００３６】
図３及び図４と共に、ＥＣＭをインデックス処理する第一の方法を説明する。

【００３７】
本発明の好適な実施の形態によれば、ＥＣＭテーブルに記憶されるＥＣＭインデックスは、記録される番組の開始に関して記録されるデータストリームにおけるＥＣＭを含んでいるデータパケットのそれぞれのシリアル番号を計算することにより作成される。このシリアル番号は、番組開始以降、データパケットの数をカウントすることにより計算される。

【００３８】
図３では、３１個のデータパケットを含んでいる、記録されるデータストリームが簡略化された方法で示されている。最初のパケット（Ｎｏ．１）はＥＣＭ、すなわちＥＣＭ１を含んでいる。したがって、後者は、ＥＣＭテーブルに記録され、その内容がインデックス１で図４に示されている。データストリームにおける（パケットＮｏ．８での）次のＥＣＭは、同じであり（ＥＣＭ１）、記録されない。（パケットＮｏ．１５での）次のＥＣ

Mは、異なるので（ＥＣＭ２）、インデックス１５でＥＣＭテーブルに記録される。この方法は、同様にして、（パケットＮｏ．２９での）ＥＣＭ３まで続き、このＥＣＭ３は、インデックス２９でＥＣＭテーブルに記録される。

【００３９】

図５及び図６と共に、ＥＣＭをインデックス処理する第二の方法が説明される。

【００４０】

この方法によれば、ＥＣＭテーブルに記憶されるＥＣＭを含むパケットのそれぞれにタイムスタンプを割り当てる。このインデックスは、ＥＴＳ（「ＥＣＭタイムスタンプ」を意味する）と表され、データストリームで転送され、前述のＭＰＥＧ－２規格ではＰＣＲ（「プログラム・クロック・リファレンス」を意味する）で表されるクロック基準参照値の値から計算される。

【００４１】

ＰＣＲ値は、所定のデータパケットのヘッダのアダプテーションフィールドに位置している。パケットに含まれる（たとえばビデオ）データがスクランブルされるときでさえ、トランスポートパケットのヘッダは、特にＰＣＲ値を含むアダプテーションフィールドを選択的に備えており、スクランブルされない。したがって、ＰＣＲ値は、明らかにアクセス可能である。

【００４２】

ＰＣＲ値は、２７ＭＨｚのクロックチックカウンタ（ｃｌｏｃｋ　ｔｉｃｋ　ｃｏｕｎｔｅｒ）の値を表し、所定の周期でデータパケットにより転送される。

【００４３】

第二の実施の形態のインデックス処理方法は、図５及び図６に例示されるものであり、以下に説明されるように実行される。記録されたデータストリームから抽出されたＥＣＭ$_n$のインデックスＥＴＳ$_n$を計算する。ＥＣＭ$_n$の直前であるＰＣＲ１$_n$の値と、ＥＣＭ$_n$の直後であるＰＣＲ２$_n$の値とを取り出す。次いで、ＰＣＲ１$_n$の値とＰＣＲ２$_n$の値との間の転送されたパケットＰ$_n$の数をカウントし、ＰＣＲ１$_n$の値とＥＣＭ$_n$の値とのパケットＥ$_n$の数をカウントする。したがって、ＥＣＭ$_n$を含んでいるパケットに対応するＰＣＲの値を補間することが可能である。

【００４４】

この値ＥＴＳ$_n$は、図６に示されるＥＣＭテーブルにおけるＥＣＭ$_n$のインデックスを構成しており、以下のように計算される。

【００４５】

【数１】

$$ETS_n = PCR1_n + \frac{E_n(PCR2_n - PCR1_n)}{P_n}$$

ＭＰＥＧ－２規格におけるＰＣＲの値に要求される精度、及びデータストリームにおけるその繰り返し周期（データストリームは少なくとも０．１秒毎に伝送される必要がある）が与えられると、この計算方法により、ＥＣＭテーブルに記憶される必要があるＥＣＭのそれぞれは、異なるインデックスＥＴＳを有することを保証することができる（１つのＥＣＭは１０秒毎であり、異なるＥＣＭが１秒毎に転送される場合であってもこの状態のままである）。

【００４６】

ＥＣＭテーブルが、記憶されるＥＣＭのそれぞれのインデックスで一旦テーブルに構築されると、インデックスは、適切な媒体にまさに記録されている番組を構成するデータと記録される。好ましくは、ＥＣＭテーブルは、たとえば、ファイルの開始で、番組のオーディオ／ビデオデータを含んでいるファイルと同じファイルに記憶される。また、ＥＣＭ

テーブルは、変形例として、記録された番組を含んでいるファイルとは異なるファイルに記憶される。

【００４７】

また、ＥＣＭテーブルは、番組を構成するデータと多重化することができる。たとえば、記憶されたデータは、ＭＰＥＧ－２フォーマットであるとき、特定のＰＩＮ番号でＭＰＥＧ－２に従い「プライベートセクション」を作成して、ＥＣＭテーブルを形成している全てのデータパケットをこのＰＩＤとそのヘッダに記憶することが可能である。

【００４８】

番組がカセットに記録される別の変形例では、ＥＣＭテーブルは、カセットの開始で記録されることが好ましい。

【００４９】

なお、記録される番組は、「トリックプレイ」モードを管理するための手段を備えていない場合であっても、任意の装置がデータの通常の読取りを常に実行することができるように、データストリームにおいてＥＣＭパケットを常に含んでいる。

【００５０】

ここで、特に、「順方向早送り」、「巻き戻し再生」又は「番組の特定の位置にジャンプ」のような「トリックプレイ」モードに従って、データが読み取られるとき、先に見られるような方法のうちの１つに従う、記録装置１により記録される番組のデータは表示装置２によりリードバックされるような方式を説明する。

【００５１】

これを行うために、表示装置２は、その概念がＭＰＥＧ－２規格に定義されるＧＯＰ（「グループ・オブ・ピクチャ」を意味する）を大体表す幾つかのデータパケットを含むデータブロックとして番組のデータを取り出す。データがスクランブルされたとき、このデータは、任意の後続の処理の前にデスクランブルされる必要がある。したがって、取り出されたデータブロックをデスクランブルするためのＣＷキーは、迅速に取り戻される必要があり、該データブロックのデスクランブルのために必要なＣＷキーを含んでいる１つ以上のＥＣＭが取り戻される必要がある。

【００５２】

これを行うために、データが記憶されるＥＣＭテーブルが使用される。ＥＣＭテーブルを作成するために使用されるインデックス処理の方法によれば、異なる方法を使用して、正しいＣＷキーを含んでいるＥＣＭを取り戻すことができる。

【００５３】

ＥＣＭが第一の方法に従ってインデックス処理されるとき（ＥＣＭインデックスはパケットのシリアル番号から形成される）、表示装置により取り出されるデータブロックの（記録される番組の最初のパケットに関して）パケットのシリアル番号を取り戻すことが必要である。

【００５４】

デジタルデータを読取る任意のシステムは、一般に、ファイルの開始と、該ファイルから抽出されるデータのパケットｎとの間の「距離」Ｎをバイトで示すことができる。このデータパケットの数Ｎとサイズ Ｔを知ることは（たとえば、ＭＰＥＧ規格に従いトランスポートパケットにとって、サイズはパケットあたり１８８バイトである）、データパケットｎのインデックスI_nが計算される。

【００５５】

【数２】

$$I_n = \frac{N}{T}$$

このインデックスI_nが一旦計算されると、表示装置は、I_nよりも小さい最も大きな

インデックスを有するＥＣＭについて、現在読取られている番組に対応するＥＣＭテーブルをサーチする必要がある。このＥＣＭが偶数キー及び奇数キーという２つのＣＷキーを含んでいる場合、パケットが偶数キーでスクランブルされているか、又は奇数キーでスクランブルされているかを示している、デスクランブルすべきデータパケットのそれぞれのヘッダに位置される指標を見て、発見されたＥＣＭの対応するキーを使用してパケットをデスクランブルすることが必要である。

【００５６】

あるケースでは、表示装置により取り出されるデータブロックは、データブロックをデスクランブルするために幾つかのＥＣＭを取り戻すことが必要であることが生じる場合がある。これは、たとえば、データブロックが幾つかのキー周期をオーバラップする場合に生じる可能性がある。図１を参照して、これは、取り出されたデータブロックが周期ｎ－１，ｎ及びｎ＋１をオーバラップする場合である。このケースでは、CW_{n-1}及びCW_nを含むＥＣＭと、CW_n及びCW_{n+1}を含むＥＣＭを取り出すことが必要である。

【００５７】

これを行うために、実際には、データブロックの最初のパケットのインデックスI_{n1}、及びデータブロックの最後のパケットのインデックスI_{n2}を計算する。次いで、I_{n1}よりも小さい最も大きなインデックスを有するECM_1、及びI_{n2}よりも小さな最も大きなインデックスを有するECM_2について、ＥＣＭテーブルがサーチされ、ECM_1とECM_2の間の全てのＥＣＭができる限り取り出される。しかし、殆どのケースでは、インデックスI_{n1}及びI_{n2}について、ＥＣＭテーブルにおいて１つ及び同じＥＣＭが発見される。

【００５８】

それぞれのＥＣＭについて、スタンプ計算（ＥＴＳ）を使用した第二の方法に従ってＥＣＭがインデックス処理されるとき、表示装置２により取り出されるデータブロックに属するデータパケットのＰＣＲの値を取り戻すことが必要である。

【００５９】

先に説明されたように、ＰＣＲ値は、定期的に、少なくとも０．１秒毎にデータストリームで送信されている。更に、ＧＯＰのデータ量は、約０．５秒続く。おおよそＧＯＰのサイズのデータブロックが取り出されるとき、ＰＣＲ値を含むデータブロックにおいて少なくとも１つのパケットが常に存在する。

【００６０】

データブロックに存在するＰＣＲ値の数に従って、データブロックのパケットのスタンプの値を決定する２つの方法を有する。

【００６１】

［１／全体のデータブロックにおける単一のＰＣＲ値］

（このパケットについて事実上のＰＣＲ値に対応する）データブロックのデータパケットｎのスタンプ$STAMP_n$を決定するものと想定し、ＰＣＲの値はデータブロックのパケットにおいて発見されるものと想定する。このとき、スタンプの値は以下のように計算される。

【００６２】

【数３】

$$STAMP_n = PCR + \frac{D_n x T_n x F}{R_n} \quad :$$

D_nは、パケットｎと、ＰＣＲ値を含むパケットとの間のパケット数に関する距離に対応する（D_nは正又は負とする）。ＰＣＲは、データブロックにおいて発見されるＰＣＲの値、R_nは、データブロックのビット／秒でのビットレートに対応する。Ｆは、システム基準参照クロックの周波数（ＭＰＥＧ－２規格によれば、一般に２７ＭＨｚ＋／－８１０

Ｈｚ）、Ｔ$_n$は、ビットでのパケットのサイズに対応する（ＭＰＥＧ－２規格によれば、一般に１８８×８）。

【００６３】

［２／全体のデータブロックに含まれる２つ以上のＰＣＲ値］

少なくとも２つのＰＣＲ値を含むデータブロックのパケットｎのスタンプＳＴＡＭＰ$_n$の値を決定するために、以下の計算を実行する。

【００６４】

【数４】

$$STAMP_n = PCR1_n + \frac{D(PCR2_n - PCR1_n)}{P_n} \quad :$$

ＰＣＲ１$_n$は、パケットｎに最も近い第一のＰＣＲの値であり、ＰＣＲ２$_n$は、パケットｎに最も近い第二のＰＣＲの値であり、Ｐ$_n$は、ＰＣＲ１$_n$を含むパケットと、ＰＣＲ２$_n$を含むパケットとの間のパケット数に対応し、Ｄ$_n$は、パケットｎと、ＰＣＲ１$_n$を含むパケットとの間のパケット数に関する距離に対応する（Ｄ$_n$は、正又は負とする）。

【００６５】

このスタンプＳＴＡＭＰ$_n$が上述した方法のうちの１つに従い一旦計算されると、表示装置は、ちょうど下にあるが、かつ計算された値ＳＴＡＭＰ$_n$に最も近いＥＣＭテーブルをサーチする。このインデックスＥＴＳ$_n$で記憶されたＥＣＭは、原理的に、データブロックのパケットをデスクランブルするために必要なキーを含んでいる。

【００６６】

先の実施の形態に関してわかるように、あるケースでは、データブロックをデスクランブルするために、複数のＥＣＭを取り戻す必要がある。

【００６７】

これは、実際に、データブロックの最初のパケットについてスタンプ値ＳＴＡＭＰ$_{n\,1}$の計算、及びデータブロックの最後のパケットについてスタンプ値ＳＴＡＭＰ$_{n\,2}$の計算に進む。次いで、ＥＣＭテーブルは、インデックスＥＴＳ$_1$及びＥＴＳ$_2$で記憶されているＥＣＭ$_1$及びＥＣＭ$_2$についてサーチされる。インデックスＥＴＳ$_1$及びＥＴＳ$_2$の値は、値ＳＴＡＭＰ$_{n\,1}$及びＳＴＡＭＰ$_{n\,2}$よりも小さく、該値ＳＴＡＭＰ$_{n\,1}$及びＳＴＡＭＰ$_{n\,2}$に最も近い。ＥＣＭ$_1$とＥＣＭ$_2$の間の全てのＥＣＭは、できる限り取り戻される。しかし、殆どのケースでは、１つ及び同じＥＣＭは、スタンプ値ＳＴＡＭＰ$_{n\,1}$及びＳＴＡＭＰ$_{n\,2}$についてＥＣＭテーブルにおいて発見される。

【００６８】

ここで、記録装置又は表示装置の典型的な実施の形態を説明する。これらは、ＥＣＭをインデックス処理する第一の方法を使用するか、第二の方法を使用するかに依存して僅かに異なる。

【００６９】

図７では、第一の実施の形態による記録装置４が示されている。記録装置４は、たとえば、オーディオビジュアルプログラムを表している記録すべきスクランブルデータストリームを受信するための入力４１を備えている。また、記録装置４は、ＥＣＭ４２を検出するためのモジュールを備えている。このモジュールは、それ自身公知のやり方で、（たとえば、ＰＩＤに基づいて）受信されたデータストリームからＥＣＭを抽出する。また、記録装置４は、パケットカウンタ４４を備えており、このカウンタは、データストリームのそれぞれのパケットのシリアル番号を、ＥＣＭテーブルを作成するためのモジュール４３に供給する。また、ＥＣＭテーブルを作成するためのモジュール４３は、検出モジュール４２からＥＣＭを受信し、その値が互いに異なるＥＣＭをＥＣＭテーブルに記憶する。また、モジュール４３は、これらＥＣＭのそれぞれと関連するパケットのシリアル番号をＥ

ＣＭテーブルに記憶する。これらのパケットシリアル番号は、ＥＣＭのインデックスを構成している。このＥＣＭテーブルは、ストレージモジュール４５に転送され、該モジュール４５は、ＥＣＭテーブルと入力４１で受信されたデータストリームと記録する。ストレージモジュール４５は、好ましくはデジタルバスに接続される出力４６に、記録されたデータを供給する。

【００７０】

図８では、本発明の第一の実施の形態による表示装置５を示している。この装置は、番組に対応する記録されたデータストリームを入力５１で受信する。データブロックを選択するためのモジュール５２は、番組における特定のデータブロック、及び記録されたデータストリームにおけるこのブロックのパケットのシリアル番号について記録装置に求める。データパケットのシリアル番号は、モジュール５４に転送され、モジュール５４は、データブロックの最初のパケット及び最後のパケットのシリアル番号を選択する。モジュール５４は、最初と最後のパケットのこれらシリアル番号を記録して、該シリアル番号をＥＣＭサーチモジュール５５に転送する。このＥＣＭサーチモジュール５５は、該モジュール５５に、現在読取られている番組のＥＣＭテーブルを送ることを記録装置に求め、該ＥＣＭテーブルから、これらのパケットシリアル番号に基づいて及び上述した方法に従って、受信されたデータブロックのパケットをデスクランブルするために必要なキーを含んでいるＥＣＭを抽出する。次いで、ＥＣＭは暗号解読モジュール５７に転送され、該モジュール５７は、該ＥＣＭから暗号解読キーＣＷ（すなわちコントロールワード）を抽出する。

【００７１】

なお、モジュール５７は、暗号解読を許可されたときにのみ、ＥＣＭの暗号解読を実行することができ、ＥＣＭを暗号解読するためのキーを所持している。

【００７２】

ＣＷキーは、デスクランブルモジュール５３により、最後に使用され、該モジュール５３は、データブロックのパケットをデスクランブルして、デスクランブルされたパケットをデコードモジュール５８に送出する。このモジュール５８は、（ビデオ向けにスクリーン、必要であればオーディオ向けにスピーカを有しており）番組を表示するために必要な信号を表示装置５９に供給する。

【００７３】

ここでは、モジュールは個別に表されているが、当然、１つ及び同じ集積回路に本質的に設けられる。ＥＣＭ暗号解読モジュール５７のような所定のモジュールは、表示装置に挿入されるスマートカードに設けられる場合もある。

【００７４】

なお、記録装置のＥＣＭテーブルを表示装置に送出するための幾つかの可能な変形例が存在する。ＥＣＭテーブルは、データの読取りの開始でその全体において送出される（すなわち、記録されたストリームの最初のデータブロックが表示装置により処理されたとき）。この変形例は、表示装置がデータの読取りの間にテーブルを記録するために利用することができる十分なメモリを有する場合に可能である。別のソリューションは、ストリームで転送されるデータブロックのパケットの位置の関数として、記録装置から表示装置にＥＣＭテーブルを部分的に送出することからなる。

【００７５】

図９では、本発明の第二の実施の形態による記録装置６を示している。

【００７６】

記録装置６は、たとえば、オーディオビジュアルプログラムを表している、記録すべきスクランブルデータストリームを受信するための入力６１を有している。また、受信装置６は、ＥＣＭを検出するためのモジュール６２を有しており、該モジュール６２は、受信されたデータストリームからＥＣＭを抽出する。また、記録装置６は、ＰＣＲ検出モジュール６４を有しており、該モジュール６４は、受信されたデータパケットのＰＣＲの値を抽出する。これらの値は、先に見られたように、モジュール６６において、ＥＣＭを含む

パケットについてＰＣＲ（ＥＴＳスタンプ）の推定された値を計算するために使用される。次いで、ＥＣＭテーブルを作成するためのモジュール６３は、その値が互いに異なるＥＣＭを、モジュール６６により計算されたＥＴＳスタンプと関連させ、記録されたスタンプのＥＣＭテーブルを形成する。

【００７７】

このＥＣＭテーブルは、ストレージモジュール６５に送出され、該モジュール６５は、該ＥＣＭテーブルを入力６１で受信されたデータストリームと記録する。ストレージモジュール６５は、好ましくはデジタルバスに接続される出力６７に、記録されたデータを供給する。

【００７８】

最後に、図１０には、本発明の第二の実施の形態による表示装置７を示している。

【００７９】

この装置は、番組に対応する記録されたデータストリームを入力７１で受信する。データブロックを選択するためのモジュール７２は、番組における特定のデータブロックを記録装置に求める。ＰＣＲ検出モジュール７３は、データブロックについて推定されたＰＣＲ値を計算するために、１つ以上のＰＣＲ値をモジュール７４に送出するように、該データブロックに含まれる該１つ以上のＰＣＲ値をこのデータブロックから抽出する。このモジュール７４は、先に発展された方法によれば、データブロックの最初のパケット及び最後のパケットの推定されたスタンプ値を計算し、これらの値をＥＣＭサーチモジュール７５に送出する。

【００８０】

このＥＣＭサーチモジュール７５は、現在読み取りされている番組のＥＣＭテーブルを該モジュール７５に送出することを記録装置に求め、推定されたスタンプ値に基づいて及び上述した方法に従って、該ＥＣＭテーブルから受信されたデータブロックのパケットをデスクランブルするために必要なキーを含むＥＣＭを抽出する。ついで、ＥＣＭは、暗号解読モジュール７７に送出され、該モジュール７７は、該ＥＣＭからデスクランブルキーＣＷ（すなわち、コントロールワード）を抽出する。なお、モジュール７７は、暗号解読を許可されたときにのみ、ＥＣＭの暗号解読を実行することができ、ＥＣＭを暗号解読するためのキーを有している。

【００８１】

ＣＷキーは、デスクランブルモジュール７８により最後に使用され、該モジュール７８は、データブロックのパケットをデスクランブルし、該デスクランブルされたパケットをデコードモジュール７９に送出する。デコードモジュール７９は、（ビデオ向けのスクリーン、及び必要であればオーディオ向けのスピーカを有しており）番組を表示するために必要な信号を表示装置８０に供給する。

【図面の簡単な説明】

【００８２】

【図１】スクランブルデータストリームの一部を図解的に例示する図である。

【図２】本発明の典型的な実現を例示する図である。

【図３】本発明の第一の実施の形態による、ＥＣＭテーブルを作成するためにＥＣＭをインデックス処理する第一の方法を例示する図である。

【図４】本発明の第一の実施の形態による、ＥＣＭテーブルを作成するためにＥＣＭをインデックス処理する第一の方法を例示する図である。

【図５】本発明の第二の実施の形態による、ＥＣＭテーブルを構築するためにＥＣＭをインデックス処理する第二の方法を例示する図である。

【図６】本発明の第二の実施の形態による、ＥＣＭテーブルを構築するためにＥＣＭをインデックス処理する第二の方法を例示する図である。

【図７】本発明の第一の実施の形態による図２に例示される装置の詳細を表す図である。

【図８】本発明の第一の実施の形態による図２に例示される装置の詳細を表す図である。

【図９】本発明の第二の実施の形態による図２に例示される装置の詳細を表す図である。

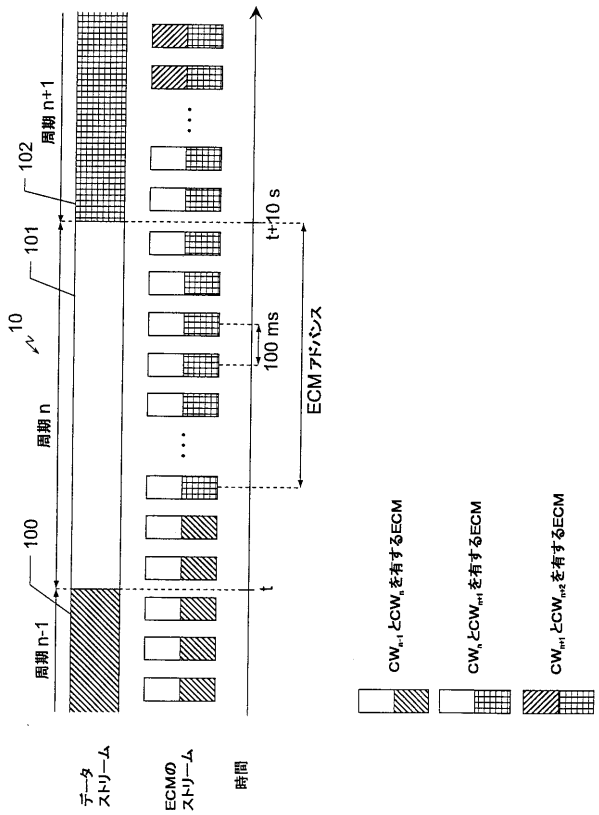
【図１０】本発明の第二の実施の形態による図２に例示される装置の詳細を表す図である。

【符号の説明】

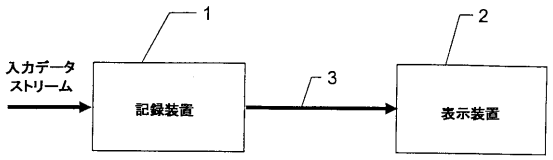
【００８３】

１：記録装置
２：表示装置
３：デジタルバス
４，６：記録装置
５，７：表示装置
４２，６２：ＥＣＭ検出モジュール
４３，６３：ＥＣＭテーブル作成モジュール
４４：パケットカウンタ
５２，７２：データブロック選択モジュール
５３，７８：データブロックデスクランブルモジュール
５４：最初と最後のパケット番号選択モジュール
５５，７５：ＥＣＭサーチモジュール
５７，７７：ＥＣＭ暗号解読モジュール
５８，７９：デコードモジュール
５９，８０：ディスプレイ
６４：ＰＣＲ検出モジュール
６６：ＥＴＳ計算モジュール
７３：ＰＣＲ検出モジュール
７４：ＰＣＲ値／データブロック計算モジュール

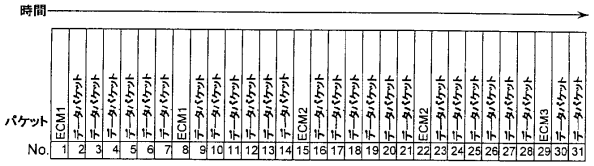
【図１】



【図２】



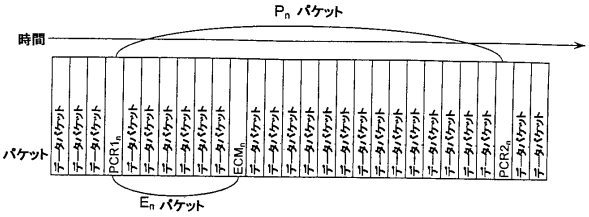
【図３】



【図４】

ECMインデックス	ECM パケット
1	ECM1
15	ECM2
29	ECM3
…	…

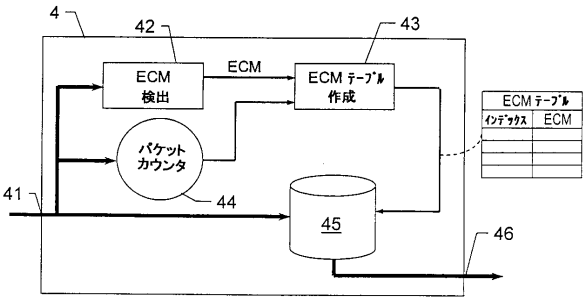
【図５】



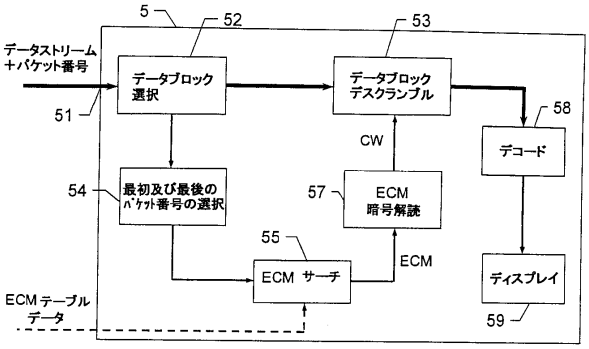
【図６】

ECMインデックス	ECM パケット
…	…
ETS_{n-1}	ECM_{n-1}
ETS_n	ECM_n
ETS_{n+1}	ECM_{n+1}
…	…

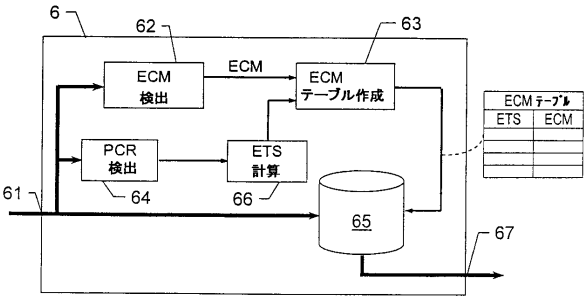
【図７】



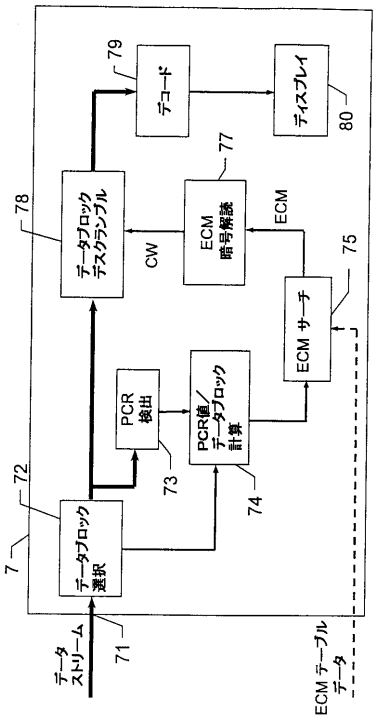
【図８】



【図９】



【図１０】



フロントページの続き

(72)発明者　フランク　アベラール
フランス国　３５２３０　サンタルメ　リュ・パティ・デ・ノエス　８
(72)発明者　ジャン－フランソワ　ヴィアル
フランス国　３５０００　レンヌ　リュ・サン・マロ　２９
(72)発明者　エリク　ディエール
フランス国　３５３４０　リフレ　ラ・ビュザールディエール（番地なし）
(72)発明者　ジャンールイ　ディアスコール
フランス国　３５８３０　ベトン　リュ・ド・ブロセリアンド　５－２

審査官　高野　美帆子

(56)参考文献　特開２００１－１８９９１４（ＪＰ，Ａ）
特開２０００－１５６８３８（ＪＰ，Ａ）
特開２０００－１７３１８１（ＪＰ，Ａ）

(58)調査した分野(Int.Cl.，ＤＢ名)
Ｇ１１Ｂ　２０／１０
Ｈ０４Ｌ　９／０８
Ｈ０４Ｎ　５／９１