

(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2012-249073

(P2012-249073A)

(43) 公開日 平成24年12月13日(2012.12.13)

(51) Int.Cl.			F I			テーマコード (参考)
H04N	7/167	(2011.01)	H04N	7/167	Z	5C159
H04N	7/32	(2006.01)	H04N	7/137	Z	5C164
H04K	1/04	(2006.01)	H04K	1/04		5J104
H04L	9/08	(2006.01)	H04L	9/00	6O1C	

審査請求 未請求 請求項の数 18 O L (全 29 頁)

(21) 出願番号	特願2011-119143 (P2011-119143)	(71) 出願人	302062931
(22) 出願日	平成23年5月27日 (2011.5.27)		ルネサスエレクトロニクス株式会社
		(74) 代理人	100103894
			弁理士 冢入 健
		(72) 発明者	白浜 伸祐
			神奈川県横浜市神奈川区金港町3番地1
			ルネサスマイクロシステム株式会社内
		Fターム(参考)	5C159 KK43 PP05 PP06 PP07 RB02
			RC11 RC35 SS02 UA05
			5C164 FA04 MB31S PA23 UC22P
			5J104 AA01 AA16 AA32 BA03 EA04
			EA16 NA02 NA37 PA05

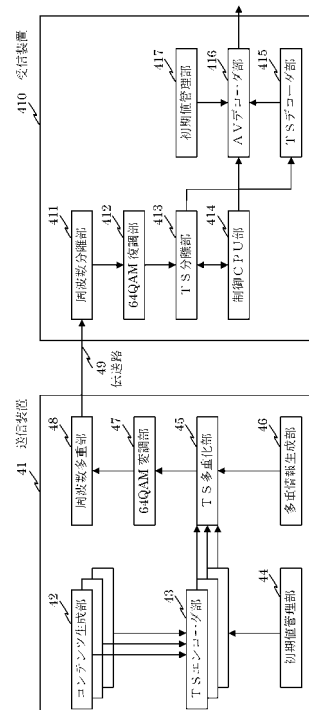
(54) 【発明の名称】 復号化装置、符号化装置、符号化復号化システム、デスクランブラ、スクランブラ、及びそれらの方法

(57) 【要約】

【課題】 チャンネル切り替え時間を短縮することができる復号化装置、符号化装置、符号化復号化システム、デスクランブラ、スクランブラ、及びそれらの方法を提供すること。

【解決手段】 本発明の実施の形態にかかる符号化装置は、Iピクチャと、それぞれ当該Iピクチャを参照するBピクチャ及びPピクチャと、がスクランブルされて含まれるストリームデータを復号する。符号化装置は、Iピクチャに基づいて、当該Iピクチャを参照するピクチャのデスクランブル鍵を生成する鍵生成部と、予め用意されたIピクチャのデスクランブル鍵によって、Iピクチャをデスクランブルするとともに、鍵生成部によって生成されたデスクランブル鍵によって、当該Iピクチャを参照するピクチャをデスクランブルするデスクランブラと、を備える。

【選択図】 図1



【特許請求の範囲】**【請求項 1】**

I ピクチャと、それぞれ当該 I ピクチャを参照する B ピクチャ及び P ピクチャと、がスクランブルされて含まれるストリームデータを復号する復号化装置であって、

前記 I ピクチャに基づいて、当該 I ピクチャを参照するピクチャのデスクランブル鍵を生成する鍵生成部と、

予め用意された前記 I ピクチャのデスクランブル鍵によって、前記 I ピクチャをデスクランブルするとともに、前記鍵生成部によって生成されたデスクランブル鍵によって、当該 I ピクチャを参照するピクチャをデスクランブルするデスクランブラと、

を備えた復号化装置。

10

【請求項 2】

前記鍵生成部は、前記 I ピクチャに続く第 1 のピクチャについて、前記 I ピクチャに基づいて、前記デスクランブル鍵を生成するものであって、前記 I ピクチャを参照する、前記第 1 のピクチャよりも後の第 2 のピクチャについては、当該第 2 のピクチャよりも前の前記第 1 のピクチャ又は前記第 2 のピクチャに基づいて、デスクランブル鍵を生成する、請求項 1 に記載の復号化装置。

【請求項 3】

前記鍵生成部は、前記第 2 のピクチャのデスクランブル鍵を、当該第 2 のピクチャの 1 つ前の前記第 1 のピクチャ又は前記第 2 のピクチャに基づいて生成する、

請求項 2 に記載の復号化装置。

20

【請求項 4】

前記鍵生成部は、前記ピクチャのハッシュ値を生成し、生成したハッシュ値に基づいて、前記デスクランブル鍵を生成する、

請求項 1 乃至 3 のいずれか 1 項に記載の復号化装置。

【請求項 5】

前記復号化装置は、前記デスクランブラによってデスクランブルされたピクチャを復号する復号部を備え、

前記鍵生成部は、前記復号部によって復号されたピクチャに基づいて、前記デスクランブル鍵を生成する、

請求項 1 乃至 4 のいずれか 1 項に記載の復号化装置。

30

【請求項 6】

動画像データを符号化して、I ピクチャと、それぞれ当該 I ピクチャを参照する B ピクチャ及び P ピクチャと、がスクランブルされて含まれるストリームデータを生成する符号化装置であって、

前記 I ピクチャに基づいて、前記 I ピクチャを参照するピクチャのスクランブル鍵を生成する鍵生成部と、

予め用意された前記 I ピクチャのスクランブル鍵によって、前記 I ピクチャをスクランブルするとともに、前記鍵生成部によって生成されたスクランブル鍵によって、前記 I ピクチャを参照するピクチャをスクランブルするスクランブラと、

を備えた符号化装置。

40

【請求項 7】

前記鍵生成部は、前記 I ピクチャに続く第 1 のピクチャについて、前記 I ピクチャに基づいて、前記スクランブル鍵を生成するものであって、前記 I ピクチャを参照する、前記第 1 のピクチャよりも後の第 2 のピクチャについては、当該第 2 のピクチャよりも前の前記第 1 のピクチャ又は前記第 2 のピクチャに基づいて、スクランブル鍵を生成する、

請求項 6 に記載の符号化装置。

【請求項 8】

前記鍵生成部は、前記第 2 のピクチャのスクランブル鍵を、当該第 2 のピクチャの 1 つ前の前記第 1 のピクチャ又は前記第 2 のピクチャに基づいて生成する、

請求項 7 に記載の符号化装置。

50

【請求項 9】

前記鍵生成部は、前記ピクチャのハッシュ値を生成し、生成したハッシュ値に基づいて、前記スクランブル鍵を生成する、

請求項 6 乃至 8 のいずれか 1 項に記載の符号化装置。

【請求項 10】

前記符号化装置は、前記スクランブラによってスクランブルされる前のピクチャを復号する復号部を備え、

前記鍵生成部は、前記復号部によって復号されたピクチャに基づいて、前記スクランブル鍵を生成する、

請求項 6 乃至 9 のいずれか 1 項に記載の符号化装置。

10

【請求項 11】

動画像データを符号化して、I ピクチャと、それぞれ当該 I ピクチャを参照する B ピクチャ及び P ピクチャと、がスクランブルされて含まれるストリームデータを生成する符号化装置と、前記符号化装置によって生成されたストリームデータを復号する復号化装置と、を備えた符号化復号化システムであって、

前記符号化装置は、

前記 I ピクチャに基づいて、前記 I ピクチャを参照するピクチャのスクランブル鍵を生成するスクランブル鍵生成部と、

予め用意された前記 I ピクチャのスクランブル鍵によって、前記 I ピクチャをスクランブルするとともに、前記スクランブル鍵生成部によって生成されたスクランブル鍵によって、前記 I ピクチャを参照するピクチャをスクランブルするスクランブラと、を有し、

20

前記復号化装置は、

前記 I ピクチャに基づいて、前記スクランブル鍵と同一のデスクランブル鍵を生成するデスクランブル鍵生成部と、

予め用意された前記 I ピクチャのスクランブル鍵と同一のデスクランブル鍵によって、前記 I ピクチャをデスクランブルするとともに、前記デスクランブル鍵生成部によって生成されたデスクランブル鍵によって、前記 I ピクチャを参照するピクチャをデスクランブルするデスクランブラと、を有する、

符号化復号化システム。

【請求項 12】

30

I ピクチャと、それぞれ当該 I ピクチャを参照する B ピクチャ及び P ピクチャと、がスクランブルされて含まれるストリームデータをデスクランブルするデスクランブラであって、

予め用意された前記 I ピクチャのデスクランブル鍵によって、前記 I ピクチャをデスクランブルするとともに、前記 I ピクチャに基づいて生成されたデスクランブル鍵によって、前記 I ピクチャを参照するピクチャをデスクランブルする、

デスクランブラ。

【請求項 13】

I ピクチャと、それぞれ当該 I ピクチャを参照する B ピクチャ及び P ピクチャと、をスクランブルするスクランブラであって、

40

予め用意された前記 I ピクチャのスクランブル鍵によって、前記 I ピクチャをスクランブルするとともに、前記 I ピクチャに基づいて生成されたスクランブル鍵によって、前記 I ピクチャを参照するピクチャをスクランブルする、

スクランブラ。

【請求項 14】

I ピクチャと、それぞれ当該 I ピクチャを参照する B ピクチャ及び P ピクチャと、がスクランブルされて含まれるストリームデータを復号する復号化方法であって、

予め用意された前記 I ピクチャのデスクランブル鍵によって、前記 I ピクチャをデスクランブルし、

前記 I ピクチャに基づいて、当該 I ピクチャを参照するピクチャのデスクランブル鍵を

50

生成し、

前記生成されたデスクランブル鍵によって、当該 I ピクチャを参照するピクチャをデスクランブルする、

復号化方法。

【請求項 15】

動画像データを符号化して、I ピクチャと、それぞれ当該 I ピクチャを参照する B ピクチャ及び P ピクチャと、がスクランブルされて含まれるストリームデータを生成する符号化方法であって、

予め用意された前記 I ピクチャのスクランブル鍵によって、前記 I ピクチャをスクランブルし、

前記 I ピクチャに基づいて、前記 I ピクチャを参照するピクチャのスクランブル鍵を生成し、

前記生成されたスクランブル鍵によって、前記 I ピクチャを参照するピクチャをスクランブルする、

符号化方法。

【請求項 16】

動画像データを符号化して、I ピクチャと、それぞれ当該 I ピクチャを参照する B ピクチャ及び P ピクチャと、がスクランブルされて含まれるストリームデータを生成して、生成したストリームデータを復号する符号化復号化方法であって、

予め用意された前記 I ピクチャのスクランブル鍵によって、前記 I ピクチャをスクランブルし、

前記 I ピクチャに基づいて、前記 I ピクチャを参照するピクチャのスクランブル鍵を生成し、

前記生成されたスクランブル鍵によって、前記 I ピクチャを参照するピクチャをスクランブルし、

予め用意された前記 I ピクチャのスクランブル鍵と同一のデスクランブル鍵によって、前記 I ピクチャをデスクランブルし、

前記 I ピクチャに基づいて、前記スクランブル鍵と同一のデスクランブル鍵を生成し、

前記生成されたデスクランブル鍵によって、前記 I ピクチャを参照するピクチャをデスクランブルする、

符号化復号化方法。

【請求項 17】

I ピクチャと、それぞれ当該 I ピクチャを参照する B ピクチャ及び P ピクチャと、がスクランブルされて含まれるストリームデータをデスクランブルするデスクランブル方法であって、

予め用意された前記 I ピクチャのデスクランブル鍵によって、前記 I ピクチャをデスクランブルし、

前記 I ピクチャに基づいて生成されたデスクランブル鍵によって、前記 I ピクチャを参照するピクチャをデスクランブルする、

デスクランブル方法。

【請求項 18】

I ピクチャと、それぞれ当該 I ピクチャを参照する B ピクチャ及び P ピクチャと、をスクランブルするスクランブル方法であって、

予め用意された前記 I ピクチャのスクランブル鍵によって、前記 I ピクチャをスクランブルし、

前記 I ピクチャに基づいて生成されたスクランブル鍵によって、前記 I ピクチャを参照するピクチャをスクランブルする、

スクランブル方法。

【発明の詳細な説明】

【技術分野】

10

20

30

40

50

【 0 0 0 1 】

本発明は、復号化装置、符号化装置、符号化復号化システム、デスクランブラ、スクランブラ、及びそれらの方法に関する。

【 背景技術 】

【 0 0 0 2 】

近年、デジタル放送の普及により、著作権保護を必要とする動画像などのデジタルコンテンツが、放送波やIP (Internet Protocol) 網といった伝送手段で配信されている。また、一般に、不正な視聴やコピーを防ぐために、デジタルコンテンツが暗号化 (スクランブル) されて配信されている。その一例として、日本のデジタル放送においては、デジタルコンテンツに対してMulti2と呼ばれるスクランブルが施され、正当な受信機以外による視聴や録画を防いでいる。

10

【 0 0 0 3 】

このようにして暗号化されたデジタルコンテンツの復号化 (デスクランブル) に用いる鍵情報は、デジタルコンテンツを含むストリームに関連データとして一定間隔で多重化されている。しかし、そのようにすることで、チャンネルの切り替え時に、鍵情報を取得してから鍵の生成処理を行なっているため、画像及び音声の出力までの時間が遅くなっている。そのため、起動時の待ち時間や、チャンネルの切り替え時の待ち時間を短縮して、ストレス無く視聴できるようにすることが望まれている。

【 0 0 0 4 】

特許文献1～4には、チャンネルの切り替え時の待ち時間を短縮する技術が開示されている。その中で、特許文献1は、受信装置において複数のスクランブルされたチャンネルの選択を切り替える時に選択したチャンネルのストリームを短時間でデスクランブルすることを目的としている。

20

【 0 0 0 5 】

図10を参照して、特許文献4にかかる限定受信システムの送信装置128及び受信装置110について説明する。図10は、特許文献4にかかる限定受信システムの送信装置128及び受信装置110の構成を示すブロック図である。

【 0 0 0 6 】

送信装置128は、鍵管理装置11、Kw暗号化部12、TS多重化部13、Ks暗号化部14、スクランブラ15、コンテンツ生成部16、TSエンコーダ17、64QAM変調部18、多重情報生成部125、及び周波数多重部126を備えている。

30

【 0 0 0 7 】

鍵管理装置11は、スクランブル鍵Ks、ワーク鍵Kw及び個別鍵Kmiを生成管理する。Kw暗号化部12は、ワーク鍵Kwを格納した個別情報EMMをKmiで暗号化する。TS多重化部13は、個別情報EMM、共通情報ECM、トランスポートストリーム及びPSI (Program Specific Information) をMPEG2 SYSTEMS (ISO / IEC 13818 - 1) の規定通りに多重化する。Ks暗号化部14は、スクランブル鍵Ksを格納した共通情報ECMをKwで暗号化する。スクランブラ15は、TS多重化部13で多重化されたデータの中からコンテンツストリームのみをスクランブル鍵Ksでスクランブルする。コンテンツ生成部16は、映像、データ等のコンテンツを生成する。TSエンコーダ17は、コンテンツをMPEG2 SYSTEMSのTSパケット (Transport Stream Packet) のデータフォーマットに変換する。64QAM変調部18は、送信データを64Q変調する。多重情報生成部125は、MPEG2 SYSTEMSのPSIをチャンネル、番組の情報に合わせて生成する。周波数多重部126は、変調した信号を周波数多重する。

40

【 0 0 0 8 】

受信装置110は、64QAM復調部111、TS分離部112、制御CPU113、デスクランブラ114、特殊鍵復号モジュール115、汎用鍵復号モジュール116、TSデコーダ123、AVデコーダ124、及び周波数分離部127を備えている。

【 0 0 0 9 】

50

64QAM復調部111は、受信信号を64QAM復調する。TS分離部112は、受信信号からPSI、映像ストリーム、共通情報ECM、個別情報EMM等を分離する。制御CPU113は、PSI情報に基づいてフィルタリングすべきProgram-IDをTS分離部112やデスクランブラ114等に伝える。デスクランブラ114は、選局されたチャンネルの映像ストリームを、Ksを用いてデスクランブルする。特殊鍵復号モジュール115は、Ksを復号化する。汎用鍵復号モジュール116は、ICカードで構成される。汎用鍵復号モジュール116は、Ksを復号化する。TSデコーダ123は、デスクランブルされたストリームをコンテンツストリームの形式に変換する。AVデコーダ124は、コンテンツストリームを視聴可能なアナログ信号に変換する。周波数分離部127は、伝送路19より受信した信号を周波数分離する。

10

【0010】

特殊鍵復号モジュール115は、送信側が複数のチャンネルに共通のKsを用いる場合に、そのKsの復号化を行う。特殊鍵復号モジュール115は、Kw復号化部118及びKs復号化部119を備えている。Kw復号化部118は、EMMを、あらかじめ持っている個別鍵Kmi117で復号化してKwを取り出す。Ks復号化部119は、ECMをKwで復号化してKsを取り出す。Ks復号化部119には、制御CPU113から選局したチャンネルが伝えられる。

【0011】

ICカードで構成される汎用鍵復号モジュール116は、送信側が複数のチャンネルに共通のKsを用いない場合に、そのKsの復号化を行う。ICカードで構成される汎用鍵復号モジュール116は、Kw復号化部121及びKs復号化部122を備えている。Kw復号化部121は、特殊鍵復号モジュール115と同様に、EMMを個別鍵Kmi120で復号化してKwを取り出す。Ks復号化部122は、ECMをKwで復号化してKsを取り出す。

20

【0012】

以下、このシステムでの送受信に関して説明する。

【0013】

送出側では、鍵管理装置11が、ワーク鍵Kwを生成し、これを個別情報EMMに格納する。その後、Kw暗号化部12は、個別情報EMMをあらかじめ鍵管理装置11から受け取っているKmiを用いて暗号化し、暗号化された個別情報としてTS多重化部13

30

【0014】

また、鍵管理装置11が、スクランブル鍵Ksを生成し、共通情報ECMに格納する。その後、Ks暗号化部14は、共通情報ECMをあらかじめ鍵管理装置11から受け取っているKwを用いて暗号化し、暗号化された共通情報としてTS多重化部13に送出する。

【0015】

また、映像、データ等のコンテンツは、コンテンツ生成部16よりTSエンコーダ17に送られ、MPEG2SYSTEMSにおけるTSパケットのデータフォーマットに変換される。TS化された映像情報等のコンテンツデータは、TS多重化部13に送られる。また、マルチプログラム構成の場合、コンテンツデータは、複数のコンテンツ生成部からそれぞれのTSエンコーダに送られる。そして、TSエンコーダ17は、コンテンツデータをTSパケット化してTS多重化部13に送る。

40

【0016】

また、多重情報生成部125では、MPEG2SYSTEMSのPSIをチャンネル、番組の情報に合わせて生成して、TS多重化部13に送る。

【0017】

TS多重化部13に送られた個別情報EMM、共通情報ECM、コンテンツストリーム及びPSIは、MPEG2SYSTEMSでの規定通り多重化され、スクランブラ15に送られる。スクランブラ15は、Ks暗号化部14から渡されたスクランブル鍵Ksを用

50

いてコンテンツストリームのみをスクランブルする。スクランブラ 15 では、スクランブルされたトランスポートストリームを 64 QAM 変調部 18 に送る。64 QAM 変調部 18 は、トランスポートストリームを 64 QAM 変調する。さらに、周波数多重部 126 は、他に 64 QAM 変調された信号と周波数多重を行い、伝送路 19 に送出する。

【0018】

一方、受信装置 110 では、伝送路 19 より受信した信号を、周波数分離部 127 で周波数分離し、64 QAM 復調部 111 で復調し、復調された信号が TS 分離部 112 で分離される。

【0019】

制御 CPU 113 は、受信装置操作部で選局したチャンネルの PSI 情報を基に、フィルタリングすべき Program-ID を取得して TS 分離部 112 に伝達する。それによって、TS 分離部 112 は、該当チャンネルの復調されたトランスポートストリームを関連情報（以下、共通情報 ECM、個別情報 EMM の総称とする）と、映像ストリーム等とに分離することが可能になる。また、制御 CPU 113 は、デスクランブルする Program-ID をデスクランブラ 114 に設定し、選局したチャンネルを Ks 復号化部 119 に設定する。

【0020】

TS 分離部 112 により分離された関連情報は、特殊鍵復号モジュール 115 または汎用鍵復号モジュール 116 のいずれかに送られ、そこで、コンテンツをデスクランブルするためのスクランブル鍵 Ks が取り出される。特殊鍵復号モジュール 115 または汎用鍵復号モジュール 116 のいずれかへの振り分けは、関連情報のモジュール識別フラグに応じて行われる。関連情報が、特殊鍵復号モジュール 115 に振り分けられた場合、特殊鍵復号モジュール 115 が用いられる。

【0021】

例えば、特殊鍵復号モジュール 115 を用いた場合、TS 分離部 112 により分離された個別情報 EMM は、Kw 復号化部 118 で、あらかじめ持っている個別鍵 Kmi 117 を使って復号される。個別情報 EMM 内に格納されたワーク鍵 Kw は、取り出されて Ks 復号化部 119 に設定される。また、TS 分離部 112 により分離された共通情報 ECM は、Ks 復号化部 119 で、先に取り出されたワーク鍵 Kw を使って復号される。共通情報 ECM 内に格納された Ks は、取り出されてデスクランブラ 114 に設定される。

【0022】

TS 分離部 112 で分離された映像などのコンテンツストリームは、デスクランブラ 114 において、セットされたスクランブル鍵 Ks を使ってデスクランブルされ、TS デコーダ 123 に送られてコンテンツストリームの形式に変換される。さらに、映像は、AV デコーダ 124 により視聴可能なアナログ信号に変換される。

【0023】

ここで、図 11 を参照して、MPEG2-TS のフォーマットについて説明する。図 11 は、MPEG2-TS のフォーマットを示す図である。

【0024】

MPEG2-TS では、映像、音声、及び、その他のデータを多重化して伝送する。ビデオカメラなどで撮影された映像（ビデオ）及び音声（オーディオ）のデータは、エンコーダと呼ばれる符号装置によってエレメンタリストリーム（ES: Elementary Stream）と呼ばれる圧縮符号化されたデジタルデータに変換される。それらのビデオ ES 及びオーディオ ES は、PES（Packetized Elementary Stream）パケットと呼ばれる、適当な大きさに分割される。さらに、MPEG2-TS の場合、PES パケットがさらに分割されて、188 バイトの TS（Transport Stream）パケットが生成される（例えば、非特許文献 1、非特許文献 2）。

【0025】

また、映像、音声、及び、その他のデータ等のコンテンツのデスクランブルするための

10

20

30

40

50

鍵情報のそれぞれは、PSI (Program Specific Information)、又は、PSIを拡張したSI (Service Information)と呼ばれるデータに含められる。PSI又はSIは、ビデオやオーディオとは別のMPEG2-TSパケットに格納されて送出される。

【0026】

図11は、ビデオ及びオーディオのエレメンタリストリームと、PSIの1つであるECM (Entitlement Control Message)と、をMPEG2-TSパケットへ変換して、MPEG2-TSストリームとして多重化するまでの過程を示したものである。ECMは、著作権が必要なコンテンツに対してスクランブルを行うための鍵情報が格納されている。

10

【0027】

ビデオES200は、PES化されてビデオPESパケット202、203に変換され、オーディオES201は、PES化されてオーディオPESパケット204、205に変換される。さらに、ビデオPESパケット202は、TS化されてビデオTSパケット206、207、208、209に変換され、オーディオPESパケット204は、TS化されてオーディオTSパケット210、211、212、213に変換される。なお、ビデオPESパケット203及びオーディオPESパケット205のTSパケットについては、図示を省略している。また、ECM219は、TS化されてECMパケット215、216、217、218に変換される。ビデオTSパケット206～209、オーディオTSパケット210～213、及びECMパケット215～218は、MPEG2-TSストリーム214に多重化されて送出される。

20

【0028】

続いて、図12を参照して、ビデオESにおけるピクチャの関係の一例について説明する。図12は、MPEGにより圧縮符号化されたビデオESにおいて時間軸上に並んでいるピクチャの関係の一例を図示している。

【0029】

MPEGでは、映像信号は、複数の圧縮画像データにより構成されている。圧縮画像データは、フレームと呼ばれる。フレームは、Iピクチャ、Pピクチャ、及びBピクチャの3種類に分類される。

【0030】

30

Iピクチャ (Intra-picture) は、前後のフレームとは関係なく、独立して一枚の画像を得ることができる。また、Pピクチャ (Predictive-picture) は、自身よりも時間軸上で過去に存在するIピクチャやPピクチャからフレーム間予測を行うことにより一枚の画像を得ることができる。さらに、Bピクチャ (Bidirectional Predictive-picture) は、時間軸上過去または未来、もしくは両方に存在するピクチャからフレーム間予測を行うことにより一枚の画像を得ることができる (例えば、非特許文献3)。

【0031】

図12について説明すると、Bピクチャ300は、時間軸上未来に存在するIピクチャ302からフレーム間予測を行うことで、一枚の画像を得ることができる。Bピクチャ301は、時間軸上未来に存在するIピクチャ302からフレーム間予測を行うことで、一枚の画像を得ることができる。

40

【0032】

Iピクチャ302は、自身単体で一枚の画像を得ることができる。Bピクチャ303は、時間軸上過去に存在するIピクチャ302と時間軸上未来に存在するPピクチャ304からフレーム間予測を行うことで、一枚の画像を得ることができる。Pピクチャ304は、時間軸上過去に存在するIピクチャ302からフレーム間予測を行うことで、一枚の画像を得ることができる。Bピクチャ305及びBピクチャ306のそれぞれは、時間軸上過去に存在するPピクチャ304と時間軸上未来に存在するPピクチャ307からフレーム間予測を行うことで、一枚の画像を得る。Pピクチャ307は、時間軸上過去に存在す

50

る P ピクチャ 3 0 4 からフレーム間予測を行うことで、一枚の画像を得ることができる。

【 0 0 3 3 】

この例では、B ピクチャ 3 0 0 及び B ピクチャ 3 0 1 のそれぞれは、時間軸上 I ピクチャ 3 0 2 よりも前に存在することになるが、一枚の画像を得るためには、時間軸上未来に存在する I ピクチャ 3 0 2 が必要となる。

【 0 0 3 4 】

続いて、図 1 3 を参照して、一般的な M P E G 2 - T S パケットの構成について説明する。図 1 3 は、一般的な M P E G 2 - T S パケットの構成図である。

【 0 0 3 5 】

M P E G 2 - T S パケット F 1 は、T S ヘッダ F 2 と、アダプテーション・フィールド F 3 と、データ・バイト F 4 と、を有する。一般的に、全ての M P E G 2 - T S パケットには、T S ヘッダ F 2 が存在する。

【 0 0 3 6 】

T S ヘッダ F 2 は、アダプテーション・フィールド・コントロールと呼ばれる 2 ビットのデータが含まれる。アダプテーション・フィールド・コントロールの値が、" 1 0 " もしくは " 1 1 " である場合、アダプテーション・フィールド F 3 が、M P E G 2 - T S パケット F 1 に含まれる。

【 0 0 3 7 】

アダプテーション・フィールド・コントロールの値が、" 0 1 " もしくは " 1 1 " である場合、データ・バイト F 4 が、M P E G 2 - T S パケット F 1 に含まれる。データ・バイト F 4 には、ビデオやオーディオの P E S データ、又は、P S I / S I データが格納されている。

【 先行技術文献 】

【 特許文献 】

【 0 0 3 8 】

【 特許文献 1 】 特開 2 0 0 0 - 2 9 5 2 0 2 号公報

【 特許文献 2 】 特開 2 0 1 0 - 1 5 4 3 4 9 号公報

【 特許文献 3 】 特開 2 0 0 7 - 2 1 5 0 6 9 号公報

【 特許文献 4 】 特開 2 0 0 9 - 2 8 4 2 8 3 号公報

【 非特許文献 】

【 0 0 3 9 】

【 非特許文献 1 】 ソニー株式会社、"ブルーレイディスクの特色"、[online]、ソニー株式会社ホームページ、[平成 2 3 年 2 月 1 4 日検索]、インターネット<URL: http://www.sony.jp/bd/products_archive/BDZ-S77/technology/blu.html>

【 非特許文献 2 】 日経 B P 社、"ワンセグ利用の V O D 連携や大量データの配信など新技術を紹介"、[online]、I T p r o、[平成 2 3 年 2 月 1 8 日検索]、<URL: <http://itpro.nikkeibp.co.jp/article/COLUMN/20080417/299449/>>

【 非特許文献 3 】 特許庁、"デジタル動画圧縮技術"、[online]、特許庁ホームページ、[平成 2 3 年 2 月 1 6 日検索]、インターネット<URL: http://www.jpo.go.jp/shiryou/s_sonota/map/denki14/4/4-3-6.htm>

【 発明の概要 】

【 発明が解決しようとする課題 】

【 0 0 4 0 】

上述した特許文献 1 に開示の技術は、正常な画像を得るためには、E C M を受信した後に到着する I ピクチャを待たなければならず、E C M の受信後に到着する I ピクチャを待つ時間だけチャンネルの切り替えが遅くなるという問題がある。

【 0 0 4 1 】

その理由としては、チャンネルに依存しない共通な鍵で復号可能な特殊鍵復号モジュールと呼ばれるモジュールを用いることで、チャンネルの切り替えの高速化を実現しているが、共通な鍵でデスクランブル可能かどうかを判断するためには E C M の受信を待たなく

10

20

30

40

50

てはならないからである。それは、上述したように、特殊復号モジュールを用いるか否かを、ECMのモジュール識別フラグによって判定しているからである。

【0042】

具体的には、特許文献1に開示の技術では、チャンネルの切り替え後に、ECMよりもIピクチャが早く到着した場合、Iピクチャを共通な鍵でデスクランブル可能かどうかを判断ができない。そのため、この場合は、Iピクチャをデスクランブルすることができない。

【0043】

また、正常な画像を出力するためには、Bピクチャ及びPピクチャの復号を開始するまでに、Iピクチャをデスクランブル及び復号して、Bピクチャ及びPピクチャのフレーム間予測に使用可能としておく必要がある。しかし、上述したように、チャンネルの切り替え後に、ECMよりもIピクチャが早く到着した場合、Iピクチャがデスクランブルできないため、Iピクチャを使用してBピクチャ及びPピクチャのフレーム間予測を行うこともできなくなってしまう。

【0044】

図14を参照して、その問題が発生するメカニズムについてより詳細に説明する。図14は、時間軸上においてMPEG2-TSパケットの受信タイミングと、それらのMPEG2-TSパケットから得られるピクチャとの関係を示す図である。

【0045】

図14は、チャンネル切り替え後のストリームに含まれるMPEG2-TSパケット605～633の受信が、時刻600から開始される様子を示している。最初にMPEG2-TSパケット605が受信される。その後は、MPEG2-TSパケット606～633が順次受信される。

【0046】

図14では、MPEG2-TSパケット611、614、615、620、628、630のそれぞれは、オーディオTSパケットを示し、MPEG2-TSパケット610、617、626のそれぞれは、ECMパケットを示す。それら以外のMPEG2-TSパケットのそれぞれは、ビデオTSパケットを示す。

【0047】

各ビデオTSパケットを受信することによって、ピクチャ634～642に示す各種ピクチャを得ることができる。各種ピクチャは、複数のMPEG2-TSパケットにより構成される。

【0048】

具体的には、図14に示すMPEG2-TSストリームには、ピクチャとして、MPEG2-TSパケット604、605により構成されるBピクチャ634と、MPEG2-TSパケット609、612により構成されるBピクチャ636と、MPEG2-TSパケット613、616により構成されるBピクチャ637と、MPEG2-TSパケット624、625により構成されるBピクチャ640と、MPEG2-TSパケット627、629により構成されるBピクチャ641と、MPEG2-TSパケット606、607、608により構成されるIピクチャ635と、MPEG2-TSパケット621、622、623により構成されるIピクチャ639と、MPEG2-TSパケット618、619により構成されるPピクチャ638と、MPEG2-TSパケット631、632、633により構成されるPピクチャ642と、が含まれている。

【0049】

時刻601で、Iピクチャ635を構成するMPEG2-TSパケット606、607、608の全てが受信される。つまり、時刻601で、スクランブルされたIピクチャ635を得ることができる。しかし、時刻601の時点では、ECMパケット610は得られていない。そのため、Iピクチャ635をデスクランブルすることができず、Iピクチャ635から正常な画像を得ることができない。

【0050】

10

20

30

40

50

一方で、ストリームの受信を開始してから最初にECMパケット610が受信される時刻602においてECMパケットを取得した後は、Bピクチャ636、Bピクチャ637、及びPピクチャ638のデスクランブルは可能となる。しかし、Bピクチャ636、Bピクチャ637、及びPピクチャ638のそれぞれは、Iピクチャ635との間でフレーム間予測という依存関係がある。しかし、デスクランブルされていないIピクチャ635を使用して、Bピクチャ636、Bピクチャ637、及びPピクチャ638を復号することはできない。したがって、Bピクチャ636、Bピクチャ637、及びPピクチャ638からも、Iピクチャ635と同様に、正常な画像を得ることができない。

【0051】

以上に説明した通り、図14に示すようなストリームの受信関係においては、チャンネル切り替え後にストリームの受信を開始した後に、全てのピクチャが正しく画像を得ることができるのは、ECMパケットの受信後に、最初にIピクチャ639が得られる時刻603以降となる。言い換えると、受信側が、チャンネルを切り替えてから正常な画像を得ることができるようになる時刻が、時刻600のストリーム受信開始から時刻603にまで大幅に遅延してしまっている。

【0052】

このように、特許文献1に開示の技術では、チャンネルを切り替えてから正常な画像を得ることができるようになるまでのチャンネル切り替え時間が長くなってしまっている、という問題がある。

【課題を解決するための手段】

【0053】

本発明の第1の態様にかかる復号化装置は、Iピクチャと、それぞれ当該Iピクチャを参照するBピクチャ及びPピクチャと、がスクランブルされて含まれるストリームデータを復号する復号化装置であって、前記Iピクチャに基づいて、当該Iピクチャを参照するピクチャのデスクランブル鍵を生成する鍵生成部と、予め用意された前記Iピクチャのデスクランブル鍵によって、前記Iピクチャをデスクランブルするとともに、前記鍵生成部によって生成されたデスクランブル鍵によって、当該Iピクチャを参照するピクチャをデスクランブルするデスクランブラと、を備えたものである。

【0054】

本発明の第2の態様にかかる符号化装置は、動画像データを符号化して、Iピクチャと、それぞれ当該Iピクチャを参照するBピクチャ及びPピクチャと、がスクランブルされて含まれるストリームデータを生成する符号化装置であって、前記Iピクチャに基づいて、前記Iピクチャを参照するピクチャのスクランブル鍵を生成する鍵生成部と、予め用意された前記Iピクチャのスクランブル鍵によって、前記Iピクチャをスクランブルするとともに、前記鍵生成部によって生成されたスクランブル鍵によって、前記Iピクチャを参照するピクチャをスクランブルするスクランブラと、を備えたものである。

【0055】

本発明の第3の態様にかかる符号化復号化システムは、動画像データを符号化して、Iピクチャと、それぞれ当該Iピクチャを参照するBピクチャ及びPピクチャと、がスクランブルされて含まれるストリームデータを生成する符号化装置と、前記符号化装置によって生成されたストリームデータを復号する復号化装置と、を備えた符号化復号化システムであって、前記符号化装置は、前記Iピクチャに基づいて、前記Iピクチャを参照するピクチャのスクランブル鍵を生成するスクランブル鍵生成部と、予め用意された前記Iピクチャのスクランブル鍵によって、前記Iピクチャをスクランブルするとともに、前記スクランブル鍵生成部によって生成されたスクランブル鍵によって、前記Iピクチャを参照するピクチャをスクランブルするスクランブラと、を有し、前記復号化装置は、前記Iピクチャに基づいて、前記スクランブル鍵と同一のデスクランブル鍵を生成するデスクランブル鍵生成部と、予め用意された前記Iピクチャのスクランブル鍵と同一のデスクランブル鍵によって、前記Iピクチャをデスクランブルするとともに、前記デスクランブル鍵生成部によって生成されたデスクランブル鍵によって、前記Iピクチャを参照するピクチャを

10

20

30

40

50

デスクランブルするデスクランブラと、を有するものである。

【 0 0 5 6 】

本発明の第 4 の態様にかかるデスクランブラは、I ピクチャと、それぞれ当該 I ピクチャを参照する B ピクチャ及び P ピクチャと、がスクランブルされて含まれるストリームデータをデスクランブルするデスクランブラであって、予め用意された前記 I ピクチャのデスクランブル鍵によって、前記 I ピクチャをデスクランブルするとともに、前記 I ピクチャに基づいて生成されたデスクランブル鍵によって、前記 I ピクチャを参照するピクチャをデスクランブルするものである。

【 0 0 5 7 】

本発明の第 5 の態様にかかるスクランブラは、I ピクチャと、それぞれ当該 I ピクチャを参照する B ピクチャ及び P ピクチャと、をスクランブルするスクランブラであって、予め用意された前記 I ピクチャのスクランブル鍵によって、前記 I ピクチャをスクランブルするとともに、前記 I ピクチャに基づいて生成されたスクランブル鍵によって、前記 I ピクチャを参照するピクチャをスクランブルするものである。

10

【 0 0 5 8 】

本発明の第 6 の態様にかかる復号化方法は、I ピクチャと、それぞれ当該 I ピクチャを参照する B ピクチャ及び P ピクチャと、がスクランブルされて含まれるストリームデータを復号する復号化方法であって、予め用意された前記 I ピクチャのデスクランブル鍵によって、前記 I ピクチャをデスクランブルし、前記 I ピクチャに基づいて、当該 I ピクチャを参照するピクチャのデスクランブル鍵を生成し、前記生成されたデスクランブル鍵によって、当該 I ピクチャを参照するピクチャをデスクランブルするものである。

20

【 0 0 5 9 】

本発明の第 7 の態様にかかる符号化方法は、動画像データを符号化して、I ピクチャと、それぞれ当該 I ピクチャを参照する B ピクチャ及び P ピクチャと、がスクランブルされて含まれるストリームデータを生成する符号化方法であって、予め用意された前記 I ピクチャのスクランブル鍵によって、前記 I ピクチャをスクランブルし、前記 I ピクチャに基づいて、前記 I ピクチャを参照するピクチャのスクランブル鍵を生成し、前記生成されたスクランブル鍵によって、前記 I ピクチャを参照するピクチャをスクランブルするものである。

【 0 0 6 0 】

30

本発明の第 8 の態様にかかる符号化復号化方法は、動画像データを符号化して、I ピクチャと、それぞれ当該 I ピクチャを参照する B ピクチャ及び P ピクチャと、がスクランブルされて含まれるストリームデータを生成して、生成したストリームデータを復号する符号化復号化方法であって、予め用意された前記 I ピクチャのスクランブル鍵によって、前記 I ピクチャをスクランブルし、前記 I ピクチャに基づいて、前記 I ピクチャを参照するピクチャのスクランブル鍵を生成し、前記生成されたスクランブル鍵によって、前記 I ピクチャを参照するピクチャをスクランブルし、予め用意された前記 I ピクチャのスクランブル鍵と同一のデスクランブル鍵によって、前記 I ピクチャをデスクランブルし、前記 I ピクチャに基づいて、前記スクランブル鍵と同一のデスクランブル鍵を生成し、前記生成されたデスクランブル鍵によって、前記 I ピクチャを参照するピクチャをデスクランブルするものである。

40

【 0 0 6 1 】

本発明の第 9 の態様にかかるデスクランブル方法は、I ピクチャと、それぞれ当該 I ピクチャを参照する B ピクチャ及び P ピクチャと、がスクランブルされて含まれるストリームデータをデスクランブルするデスクランブル方法であって、予め用意された前記 I ピクチャのデスクランブル鍵によって、前記 I ピクチャをデスクランブルし、前記 I ピクチャに基づいて生成されたデスクランブル鍵によって、前記 I ピクチャを参照するピクチャをデスクランブルするものである。

【 0 0 6 2 】

本発明の第 10 の態様にかかるスクランブル方法は、I ピクチャと、それぞれ当該 I ピ

50

クチャを参照する B ピクチャ及び P ピクチャと、をスクランブルするスクランブル方法であって、予め用意された前記 I ピクチャのスクランブル鍵によって、前記 I ピクチャをスクランブルし、前記 I ピクチャに基づいて生成されたスクランブル鍵によって、前記 I ピクチャを参照するピクチャをスクランブルするものである。

【 0 0 6 3 】

上述した本発明の各態様によれば、例えば、E C M のような他のデータの受信タイミングに関係なく、I ピクチャを受信した時点から、正常な画像を出力することができる。

【発明の効果】

【 0 0 6 4 】

上述した本発明の各態様によれば、チャンネル切り替え時間を短縮することができる復号化装置、符号化装置、符号化復号化システム、デスクランブラ、スクランブラ、及びそれらの方法を提供することができる。

【図面の簡単な説明】

【 0 0 6 5 】

【図 1】本発明の実施の形態にかかる送信装置及び受信装置を含むシステム構成図である。

【図 2】本発明の実施の形態にかかる T S エンコーダ部のブロック図である。

【図 3】本発明の実施の形態にかかる M P E G 2 - T S のパケット構成図である。

【図 4】本発明の実施の形態にかかる A V デコーダ部のブロック図である。

【図 5】本発明の実施の形態にかかる送信装置の制御フローチャートである。

【図 6】本発明の実施の形態にかかる T S エンコーダ部の制御フローチャートである。

【図 7】本発明の実施の形態にかかる受信装置の制御フローチャートである。

【図 8】本発明の実施の形態にかかる A V デコーダ部の制御フローチャートである。

【図 9】本発明の実施の形態にかかるチャンネル切り替え時の受信関係図である。

【図 10】特許文献 1 にかかる限定受信システムの送信装置及び受信装置の構成を示すブロック図である。

【図 11】M P E G 2 - T S のフォーマットを示す図である。

【図 12】M P E G 2 におけるピクチャの関係を示す図である。

【図 13】一般的な M P E G 2 - T S のパケット構成図である。

【図 14】特許文献 1 にかかるチャンネル切り替え時の受信関係図である。

【発明を実施するための形態】

【 0 0 6 6 】

図 1 を参照して、本発明の実施の形態にかかる送受信システムの構成について説明する。図 1 は、本発明の実施の形態にかかる送信装置及び受信装置を含むシステム構成図である。

【 0 0 6 7 】

送受信システムは、送信装置 4 1 及び受信装置 4 1 0 を有する。送信装置 4 1 及び受信装置 4 1 0 は、伝送路 4 9 によって相互に接続されている。送信装置 4 1 は、動画像データを M P E G 2 - T S ストリームに変換して受信装置 4 1 0 に送信する。受信装置 4 1 0 は、送信装置 4 1 から伝送路 4 9 を経由して受信した M P E G 2 - T S ストリームを再生可能な形式のデータに変換して出力装置（図示せず）に出力する。ここで、本実施の形態では、動画像データが、テレビ番組データである場合について例示する。したがって、送信装置 4 1 は、例えば、デジタル放送送信装置であり、受信装置 4 1 0 及び出力装置は、デジタルテレビ受像機に含まれる装置となる。

【 0 0 6 8 】

送信装置 4 1 は、コンテンツ生成部 4 2、T S エンコーダ部 4 3、初期値管理部 4 4、T S 多重化部 4 5、多重情報生成部 4 6、6 4 Q A M 変調部 4 7、及び周波数多重部 4 8 を有する。

【 0 0 6 9 】

コンテンツ生成部 4 2 は、画像データ、音声データ、字幕データ、及び B M L (B r o

10

20

30

40

50

adcast Markup Language)データ等のコンテンツを生成する。テレビ番組データは、これらのコンテンツのそれぞれが複数含まれて構成される。なお、動画像データは、このようなテレビ番組データに限られず、これらのコンテンツのうち、少なくとも画像データが複数含まれて構成されるものであればよい。コンテンツ生成部42は、生成したコンテンツから構成される動画像データを蓄積・管理する。つまり、コンテンツ生成部42は、動画像データが格納される任意の記憶装置を有する。記憶装置は、例えば、メモリ又はハードディスク等である。コンテンツ生成部42は、動画像データをTSエンコーダ部43に出力する。

【0070】

ここで、送信装置41がマルチチャンネルのデジタル放送送信装置である場合、送信装置41が複数のコンテンツ生成部42を有するようにし、コンテンツ生成部42のそれぞれが、別々のチャンネルのテレビ番組データのコンテンツを生成するようにする。

【0071】

TSエンコーダ部43は、コンテンツ生成部42から動画像データが入力され、初期値管理部44から初期値が入力される。TSエンコーダ部43は、動画像データに含まれるコンテンツのうち、画像データ及び音声データのそれぞれをエンコード(符号化)及びスクランブルしてMPEG2-TSパケット形式に変換する。なお、初期値は、画像データのスクランブル鍵の初期鍵として機能する。TSエンコーダ部43は、生成したMPEG2-TSパケットをTS多重化部45に出力する。以下、画像データのMPEG2-TSパケットを「ビデオTSパケット」とも言い、音声データのMPEG2-TSパケットを「オーディオTSパケット」とも言う。

【0072】

ここで、送信装置41がマルチチャンネルのデジタル放送送信装置である場合、送信装置41が複数のTSエンコーダ部43を有するようにし、それぞれのTSエンコーダ部43が、複数のコンテンツ生成部42のそれぞれで生成されたテレビ番組データのコンテンツをMPEG2-TSパケット形式に変換するようにする。

【0073】

初期値管理部44は、画像データをスクランブルする際に使用される初期値を管理する。つまり、初期値管理部44は、初期値が格納される任意の記憶装置を有する。ここで、本実施の形態では、初期値が格納される記憶装置として、ICカードを使用した場合について例示する。したがって、初期値管理部44は、IC(Integrated Circuit)カードが挿入されて、挿入されたICカードに格納された初期値を読み取るICカードリーダーを含むものとする。後述する初期値管理部417についても、同様であるものとする。初期値管理部44は、初期値をTSエンコーダ部43に出力する。

【0074】

TS多重化部45は、TSエンコーダ部43からコンテンツのMPEG2-TSパケットが入力され、多重情報生成部46からPSI/SI(Service Information)パケットが入力される。TS多重化部45は、コンテンツのMPEG2-TSパケット及びPSIパケットを多重化して、MPEG2-TSストリームを生成する。TS多重化部45は、生成したMPEG2-TSストリームを64QAM変調部47に出力する。

【0075】

多重情報生成部46は、MPEG2システムにおけるPSI/SIパケットをテレビ番組のデータ及びそのデータのチャンネルに合わせて生成する。多重情報生成部46は、生成したPSI/SIパケットをTS多重化部45に出力する。

【0076】

64QAM変調部47は、TS多重化部45から出力されたMPEG2-TSストリームを64Q変調する。64QAM変調部47は、64QAM変調したMPEG2-TSストリームを周波数多重部48に出力する。

【0077】

10

20

30

40

50

周波数多重部 4 8 は、6 4 Q A M 変調部 4 7 から出力された M P E G 2 - T S ストリームを周波数多重して伝送波を生成する。周波数多重部 4 8 は、伝送路 4 9 を経由して、生成した伝送波を受信装置 4 1 0 に送信する。

【 0 0 7 8 】

受信装置 4 1 0 は、周波数分離部 4 1 1、6 4 Q A M 復調部 4 1 2、T S 分離部 4 1 3、制御 C P U 部 4 1 4、T S デコーダ部 4 1 5、A V デコーダ部 4 1 6、及び初期値管理部 4 1 7 を有する。

【 0 0 7 9 】

周波数分離部 4 1 1 は、伝送路 4 9 を経由して、送信装置 4 1 から受信した伝送波から、M P E G 2 - T S ストリームを周波数分離する。周波数分離部 4 1 1 は、分離した M P E G 2 - T S ストリームを 6 4 Q A M 復調部 4 1 2 に出力する。

10

【 0 0 8 0 】

6 4 Q A M 復調部 4 1 2 は、周波数分離部 4 1 1 から出力された M P E G 2 - T S パケットを 6 4 Q A M 復調する。6 4 Q A M 復調部 4 1 2 は、6 4 Q A M 復調した M P E G 2 - T S パケットを T S 分離部 4 1 3 に出力する。

【 0 0 8 1 】

T S 分離部 4 1 3 は、6 4 Q A M 復調部 4 1 2 から出力された M P E G 2 - T S パケットに分離する。T S 分離部 4 1 3 は、制御 C P U 部 4 1 4 から M P E G 2 - T S パケットのフィルタリング制御情報を取得する。フィルタリング制御情報については、後述する。そして、T S 分離部 4 1 3 は、取得したフィルタリング制御情報に応じて、分離した M P E G 2 - T S パケットを種類別に分類して T S デコーダ部 4 1 5 に出力する。

20

【 0 0 8 2 】

制御 C P U 部 4 1 4 は、M P E G 2 - T S パケットのフィルタリング及びデスクランブルの制御をする。制御 C P U 部 4 1 4 は、T S 分離部 4 1 3 から取得した M P E G 2 - T S パケットからフィルタリング制御情報及びデスクランブル制御情報を取得する。制御 C P U 部 4 1 4 は、取得したフィルタリング制御情報を T S 分離部 4 1 3 に出力する。また、制御 C P U 部 4 1 4 は、取得したデスクランブル制御情報を A V デコーダ部 4 1 6 に出力する。なお、デスクランブル制御情報については、後述する。

【 0 0 8 3 】

T S デコーダ部 4 1 5 は、T S 分離部 4 1 3 から出力された M P E G 2 - T S パケットのうち、ビデオ T S パケット及びオーディオ T S パケットを、A V デコーダ部 4 1 6 で処理可能なエレメンタリストリーム形式に変換する。T S デコーダ部 4 1 5 は、生成したエレメンタリストリームを A V デコーダ部 4 1 6 に出力する。以下、ビデオ T S パケットのエレメンタリストリームを「ビデオ E S」とも言い、オーディオ T S パケットのエレメンタリストリームを「オーディオ E S」とも言う。

30

【 0 0 8 4 】

A V デコーダ部 4 1 6 は、制御 C P U 部 4 1 4 からデスクランブル制御情報が入力され、初期値管理部 4 1 7 から初期値が入力され、T S デコーダ部 4 1 5 からエレメンタリストリームが入力される。A V デコーダ部 4 1 6 は、エレメンタリストリームをデスクランブル及びデコード（復号）する。なお、初期値は、ビデオ E S のデスクランブル鍵である初期鍵として機能する。A V デコーダ部 4 1 6 は、ビデオ E S をデコードして、画像を表示可能な形式のピクチャデータを生成する。また、A V デコーダ部 4 1 6 は、オーディオ E S をデコードして、音声を出力可能な形式のオーディオデータを生成する。A V デコーダ部 4 1 6 は、生成したピクチャデータ及びオーディオデータを、受信装置 4 1 0 の外部に接続された出力装置に出力する。

40

【 0 0 8 5 】

ここで、出力装置は、表示装置（図示せず）及び出音装置（図示せず）を含む。表示装置は、例えば、C R T（Cathode Ray Tube）ディスプレイ、プラズマディスプレイ、液晶ディスプレイ及び有機 E L（Electro Luminescence）ディスプレイ等である。出音装置は、例えば、スピーカーである。表示装置は、受信装置 4 1 0 から出力されたピクチャデー

50

タに基づいて、画像を表示する。出音装置は、受信装置 4 1 0 から出力されたオーディオデータに基づいて、音声を出音する。

【0086】

初期値管理部 4 1 7 は、エレメンタリストリームのデスクランブルする際に使用される初期値を管理する。つまり、初期値管理部 4 1 7 は、初期値が格納される任意の記憶装置を有する。なお、初期値管理部 4 1 7 は、送信装置 4 1 と共有された初期値を管理する。つまり、初期値管理部 4 1 7 は、初期値管理部 4 4 に格納される初期値と同一の初期値が格納される。初期値管理部 4 1 7 は、初期値を A V デコーダ部 4 1 6 に出力する。

【0087】

続いて、図 2 を参照して、本発明の実施の形態にかかる T S エンコーダ部 4 3 の構成について説明する。図 2 は、本発明の実施の形態にかかる T S エンコーダ部 4 3 のブロック図である。

【0088】

T S エンコーダ部 4 3 は、ビデオエンコーダ 2 2、ビデオデコーダ 2 3、ハッシュ生成器 2 4、バッファ 2 5、スクランブラ 2 6、及び T S 処理部 2 7 を有する。

【0089】

ビデオエンコーダ 2 2 は、コンテンツ生成部 4 2 から出力された画像データをエレメンタリストリーム形式に変換をする。エレメンタリストリームは、画像データがエンコードされたデータである。よって、エレメンタリストリームは、I ピクチャ、B ピクチャ、及び P ピクチャのうちのいずれかのデータとなる。ビデオエンコーダ 2 2 は、生成したエレメンタリストリームをビデオデコーダ 2 3 及びスクランブラ 2 6 に出力する。

【0090】

ビデオデコーダ 2 3 は、ビデオエンコーダ 2 2 から出力されたエレメンタリストリームをデコードする。ビデオデコーダ 2 3 は、エレメンタリストリームをデコードして生成したピクチャデータをハッシュ生成器 2 4 に出力する。また、ビデオデコーダ 2 3 は、デスクランブル制御情報であるリセットフラグを生成して T S 処理部 2 7 に出力する。

【0091】

ハッシュ生成器 2 4 は、ビデオデコーダ 2 3 から出力されたピクチャデータをハッシュ演算して、一意の値のハッシュを生成する。ハッシュ生成器 2 4 は、生成したハッシュをバッファ 2 5 に出力する。

【0092】

バッファ 2 5 は、ハッシュ生成器 2 4 から出力されたハッシュ、又は、初期値管理部 4 4 から出力された初期値を保持する。つまり、バッファ 2 5 は、ハッシュ又は初期値が格納される任意の記憶装置である。バッファ 2 5 は、保持しているハッシュ又は初期値を、スクランブル鍵としてスクランブラ 2 6 に出力する。

【0093】

スクランブラ 2 6 は、バッファ 2 5 から出力されたスクランブル鍵を使用して、ビデオエンコーダ 2 2 から出力されたエレメンタリストリームをスクランブルする。スクランブラ 2 6 は、スクランブルしたエレメンタリストリームを T S 処理部 2 7 に出力する。

【0094】

T S 処理部 2 7 は、スクランブラ 2 6 から出力されたエレメンタリストリームを M P E G 2 - T S パケット形式へ変換する。T S 処理部 2 7 は、ビデオデコーダ 2 3 から出力されたリセットフラグを、M P E G 2 - T S パケットに含まれるアダプテーション・フィールドに埋め込む。そして、T S 処理部 2 7 は、生成した M P E G 2 - T S パケットを T S 多重化部 4 5 に出力する。

【0095】

なお、本実施の形態では、このように M P E G 2 - T S フォーマットに変換する場合について例示しているが、リセットフラグのように、受信装置 4 1 0 でのデスクランブルに必要な情報を埋め込むことできるフォーマットであれば、このフォーマットに限定されない。

10

20

30

40

50

【 0 0 9 6 】

続いて、本発明の実施の形態にかかる M P E G 2 - T S パケットの構成について説明する。図 3 は、本発明の実施の形態にかかる M P E G 2 - T S パケットの構成図である。ここでは、図 1 3 を参照して説明した M P E G 2 - T S パケットと異なる点について説明する。

【 0 0 9 7 】

本実施の形態にかかる M P E G 2 - T S パケットは、アダプテーション・フィールド F 3 にリセットフラグ F 6 が格納されるエリアを設けられている。なお、リセットフラグ F 6 が格納されるエリアは、アダプテーション・フィールド F 3 のうち、任意のビット位置に設けられるようにしてよい。

10

【 0 0 9 8 】

続いて、図 4 を参照して、本発明の実施の形態にかかる A V デコーダ部 4 1 6 の構成について説明する。図 4 は、本発明の実施の形態にかかる A V デコーダ部 4 1 6 のブロック図である。

【 0 0 9 9 】

A V デコーダ部 4 1 6 は、ビデオデコーダ 3 7、デスクランブラ 3 8、バッファ 3 9、及びハッシュ生成器 3 1 0 を有する。

【 0 1 0 0 】

ビデオデコーダ 3 7 は、デスクランブラ 3 8 から出力されたエレメンタリストリームをデコードする。ビデオデコーダ 3 7 は、エレメンタリストリームをデコードして生成したピクチャデータを、受信装置 4 1 0 の外部及びハッシュ生成器 3 1 0 に出力する。ここで、ビデオデコーダ 3 7 は、送信装置 4 1 のビデオデコーダ 2 3 と同一のデコード規則によってエレメンタリストリームをデコードする。つまり、ビデオデコーダ 2 3 及びビデオデコーダ 3 7 は、同一のエレメンタリストリームをデコードした場合、同一のピクチャデータを生成する。

20

【 0 1 0 1 】

デスクランブラ 3 8 は、バッファ 3 9 から出力されたデスクランブル鍵を使用して、T S デコーダ部 4 1 5 から出力されたエレメンタリストリームをデスクランブルする。デスクランブラ 3 8 は、デスクランブルしたエレメンタリストリームをビデオデコーダ 3 7 に出力する。

30

【 0 1 0 2 】

バッファ 3 9 は、初期値管理部 4 1 7 から出力された初期値、又は、ハッシュ生成器 3 1 0 から出力されたハッシュを保持する。つまり、バッファ 3 9 は、ハッシュ又は初期値が格納される任意の記憶装置である。バッファ 3 9 は、保持している初期値又はハッシュをデスクランブル鍵としてデスクランブラ 3 8 に出力する。

【 0 1 0 3 】

ハッシュ生成器 3 1 0 は、ビデオデコーダ 3 7 から出力されたピクチャデータをハッシュ演算して、一意の値のハッシュを生成する。ハッシュ生成器 3 1 0 は、生成したハッシュをバッファ 3 9 に出力する。ここで、ハッシュ生成器 3 1 0 は、送信装置 4 1 のハッシュ生成器 2 4 と同一の演算規則でハッシュを生成する。つまり、ハッシュ生成器 2 4 及びハッシュ生成器 3 1 0 は、同一のピクチャデータを演算した場合、同一のハッシュを生成する。

40

【 0 1 0 4 】

続いて、図 5 を参照して、本発明の実施の形態にかかる送信装置 4 1 の動作について説明する。図 5 は、本発明の実施の形態にかかる送信装置 4 1 の制御フローチャートである。

【 0 1 0 5 】

コンテンツ生成部 4 2 は、画像データ、音声データ、字幕データ、B M L データ等のコンテンツを生成する。つまり、各コンテンツによって構成される動画像データが生成される。コンテンツ生成部 4 2 は、生成した動画像データを T S エンコーダ部 4 3 に出力する

50

(S 1 0 1)。

【 0 1 0 6 】

T S エンコーダ部 4 3 は、コンテンツ生成部 4 2 から出力された動画像データのうち、画像データ及び音声データのようにスクランブルによる保護が必要なデータを、エレメンタリストリームに変換してから、バッファ 2 5 のスクランブル鍵を利用してスクランブルして M P E G 2 - T S パケットに変換する (S 1 0 2)。T S エンコーダ部 4 3 は、生成した M P E G 2 - T S パケットを T S 多重化部 4 5 に出力する。

【 0 1 0 7 】

T S 多重化部 4 5 は、T S エンコーダ部 4 3 から出力された M P E G 2 - T S パケットと、多重情報生成部 4 6 から出力された P S I / S I パケットと、ストリーム全体のビットレートを調整するための N U L L パケットと、を 1 つの M P E G 2 - T S ストリームに多重化する (S 1 0 3)。T S 多重化部 4 5 は、生成した P E G 2 - T S ストリームを 6 4 Q A M 変調部 4 7 に出力する。

10

【 0 1 0 8 】

ここで、日本の地上デジタル放送は、放送波を伝送するために 6 4 Q A M (Q u a d r a t u r e A m p l i t u d e M o d u l a t i o n) 方式で変調されている。また、日本のデジタル放送においては、携帯機器などの移動体に向けてワンセグメント放送と呼ばれる放送も行っている。ワンセグメント放送は、地上デジタル放送とは異なり、Q P S K (Q u a d r a t u r e P h a s e S h i f t K e y i n g) 方式で変調されている。6 4 Q A M 変調方式で変調された地上デジタル放送の電波、及び、Q P S K 変調方式で変調されたワンセグメント放送の電波は、O F D M (O r t h o g o n a l F r e q u e n c y - D i v i s i o n M u l t i p l e x i n g) と呼ばれる方式で多重化され、送信されている。

20

【 0 1 0 9 】

6 4 Q A M 変調部 4 7 は、T S 多重化部 4 5 から出力された M P E G 2 - T S ストリームを 6 4 Q A M 変調する (S 1 0 4)。6 4 Q A M 変調部 4 7 は、6 4 Q A M 変調した M P E G 2 - T S ストリームを周波数多重部 4 8 に出力する。

【 0 1 1 0 】

周波数多重部 4 8 は、6 4 Q A M 変調部 4 7 から出力された M P E G 2 - T S ストリームを O F D M のサブキャリアとして多重化する (S 1 0 5)。送信装置 4 1 は、M P E G 2 - T S ストリームを多重化して生成した O F D M 波を、受信装置 4 1 0 に向けて送信する (S 1 0 6)。つまり、本実施の形態では、伝送路 4 9 が、電波である O F D M 波を伝送する自由空間である場合について例示している。

30

【 0 1 1 1 】

なお、本発明では、送信装置 4 1 と受信装置 4 1 0 の間でのストリームの送受信方法については、上述した方法に限定されない。例えば、伝送路 4 9 は、自由空間のような無線のものに限定されず、I P 網のように有線のものであってもよい。また、変調の有無及びその方法についても、上述したものに限定されない。つまり、6 4 Q A M 変調を行わずに、M P E G 2 - T S ストリームを送信するようにしてもよい。また、例えば、M P E G 2 - T S ストリームを Q P S K 方式によって変調して送信するようにしてもよい。つまり、動画像データは、地上デジタル放送におけるテレビ番組データに限られず、ワンセグメント放送におけるテレビ番組データであってもよい。

40

【 0 1 1 2 】

続いて、図 6 を参照して、本発明の実施の形態にかかる T S エンコーダ部 4 3 の動作について説明する。図 6 は、本発明の実施の形態にかかる T S エンコーダ部 4 3 の制御フローチャートである。

【 0 1 1 3 】

ビデオエンコーダ 2 2 は、T S エンコーダ部 4 3 から出力された画像データをエレメンタリストリームにエンコードする (S 2 0 1)。ここで、画像データのエンコード方式は、例えば、H . 2 6 4 / A V C のように、送信装置側と受信装置側のそれぞれにおけるビ

50

デオデコーダでのデコード結果が等しくなるエンコード方式であれば、どのようなエンコード方式であってもよい。例えば、現在の日本のデジタル放送で採用されている M P E G 2 形式では、デコード演算に小数演算が必要なため、デコーダの小数演算の精度や実装方法によって、デコード演算結果が異なってしまうことがある。つまり、このようなエンコード方式を採用すると、送信装置 4 1 でのデコード演算結果と、受信装置 4 1 0 でのデコード演算結果とが異なってしまう場合がある。この場合、それぞれのデコード演算結果から生成されるスクランブル鍵及びデスクランブル鍵が異なるものとなるため、受信装置 4 1 0 で正常にデスクランブルすることができなくなってしまう。

【 0 1 1 4 】

それに対して、H . 2 6 4 / A V C では、整数のみでデコード演算をできるようになっているため、デコーダの小数演算の精度や実装方法に関わらずデコード演算結果が一致する。そのため、エンコード方式として、H . 2 6 4 / A V C を採用することによって、送信装置 4 1 でのデコード演算結果と、受信装置 4 1 0 でのデコード演算結果のそれぞれから、同一のスクランブル鍵及びデスクランブル鍵を生成することができ、正常にデスクランブルをすることが可能となる。

【 0 1 1 5 】

ビデオデコーダ 2 3 は、ビデオエンコーダ 2 2 から出力されたエレメンタリストリームをデコードする (S 2 0 2)。ビデオデコーダ 2 3 は、エレメンタリストリームをデコードして生成したピクチャデータをハッシュ生成器 2 4 及び T S 処理部 2 7 に出力する。ここで、一般的な画像のデコード方式では、I ピクチャがデコードできなければ、I ピクチャの前後に存在する B ピクチャや、I ピクチャの後に存在する P ピクチャのデコードが不可能となる。そこで、本実施の形態では、I ピクチャをスクランブル / デスクランブル鍵のリセットタイミングとすることにより、受信装置 4 1 0 によるデスクランブル及びデコードを行うまでの時間を最短化する。よって、I ピクチャをスクランブル / デスクランブル鍵のリセットタイミングとするために、送信装置 4 1 がスクランブル対象となるエレメンタリストリームのピクチャの種類を判定する必要がある。

【 0 1 1 6 】

そのため、ビデオデコーダ 2 3 は、デコードにおいて、デコードしたエレメンタリストリームが I ピクチャか否かを判定する (S 2 0 3)。I ピクチャか否かは、例えば、エレメンタリストリームに含まれる P C T (P i c t u r e S t a r t C o d e) によって判定する。

【 0 1 1 7 】

デコードしたエレメンタリストリームが I ピクチャであると判定した場合 (S 2 0 3 : Y e s)、T S エンコーダ部 4 3 は、初期値管理部 4 4 から初期値を取得して、バッファ 2 5 に格納する。また、ビデオデコーダ 2 3 は、リセットフラグを " 1 " として、T S 処理部 2 7 に出力する (S 2 0 5)。そして、処理は、ステップ S 2 0 7 に進む。

【 0 1 1 8 】

デコードしたエレメンタリストリームが I ピクチャでないと判定された場合 (S 2 0 3 : N o)、ビデオデコーダ 2 3 は、リセットフラグを " 0 " として、T S 処理部 2 7 に出力する (S 2 0 6)。そして、処理は、ステップ S 2 0 7 に進む。なお、この場合は、バッファ 2 5 には、ビデオデコーダ 2 3 によって前回デコードされたピクチャデータをハッシュ演算して生成されたハッシュが格納されていることになる。このハッシュは、後述するステップ S 2 0 9 で格納されることになる。

【 0 1 1 9 】

スクランブラ 2 6 は、バッファ 2 5 に格納された値をスクランブル鍵として利用して、ビデオエンコーダ 2 2 から出力されたエレメンタリストリームをスクランブルする。よって、スクランブラ 2 6 は、I ピクチャのエレメンタリストリームについては、初期値によってデスクランブルを行い、その I ピクチャを参照する B ピクチャ及び P ピクチャのエレメンタリストリームについては、前回デコードされたピクチャのハッシュによってデスクランブルを行うことになる。スクランブラ 2 6 は、スクランブルしたエレメンタリストリ

10

20

30

40

50

ームをTS処理部27に出力する(S207)。ここで、スクランブラ26におけるスクランブルのアルゴリズムとして、どのようなアルゴリズムを採用するようにしてよい。

【0120】

TS処理部27は、スクランブラ26から出力されたエレメンタリストリームをMPEG2-TSパケット化する。そして、TS処理部27は、MPEG2-TSパケットのアダプテーション・フィールドF3に、ビデオデコーダ23から出力されたりセットフラグF6を格納する。これによって、Iピクチャのエレメンタリストリームから生成されたMPEG2-TSパケットのアダプテーション・フィールドF3には、リセットフラグが"1"で格納され、Bピクチャ及びPピクチャのエレメンタリストリームから生成されたMPEG2-TSパケットのアダプテーション・フィールドF3には、リセットフラグが"0"で格納される。

10

【0121】

ハッシュ生成器24は、ビデオデコーダ23によってデコードされたピクチャデータから、ハッシュを生成する(ステップS208)。ここで、ハッシュ生成器24において、ハッシュを生成するアルゴリズムとして、どのようなアルゴリズムを採用するようにしてもよい。例えば、SHA-1又はMD5等のアルゴリズムを採用する。また、ピクチャから生成することができる一意な値であれば、ハッシュ以外の値を生成するようにしてもよい。ハッシュ生成器24は、生成したハッシュをバッファ25に格納する(S209)。バッファ25に格納されたハッシュは、次にデコードするエレメンタリストリームがBピクチャ又はPピクチャである場合に、ステップS207においてスクランブル鍵として使用される。

20

【0122】

続いて、図7を参照して、本発明の実施の形態にかかる受信装置410の動作について説明する。図7は、本発明の実施の形態にかかる受信装置410の制御フローチャートである。

【0123】

受信装置410は、送信装置41から伝送路49を通じてOFDM波を受信する(S301)。受信装置410が受信したOFDM波は、周波数分離部411に入力される。周波数分離部411は、入力されたOFDM波からMPEG2-TSストリームを分離する(S302)。周波数分離部411は、分離したMPEG2-TSストリームを64QAM復調部412に出力する。なお、この時点では、MPEG2-TSストリームは、64QAM変調された状態となっている。

30

【0124】

64QAM復調部412は、周波数分離部411によって分離されたMPEG2-TSストリームを64QAM復調する(S303)。64QAM復調部412は、64QAM復調したMPEG2-TSストリームをTS分離部413に出力する。

【0125】

TS分離部413は、64QAM復調部412から出力されたMPEG2-TSストリームを、MPEG2-TSパケットに分離する(S304)。TS分離部413は、分離したMPEG2-TSパケットのコピーを制御CPU部414に出力する。ここで、MPEG2-TSパケットのTSヘッダ部分には、MPEG2-TSパケットにどのような種類のデータが格納されているかを識別するための識別子が含まれている。この識別子は、PID(Packet Identifier)と呼ばれる。制御CPU部414は、TS分離部413から出力されたMPEG2-TSパケットからPIDを取得して、取得したPIDをフィルタリング制御情報としてTS分離部413に出力する。TS分離部413は、制御CPU部414から出力されたPIDに基づいて、コピー元のMPEG2-TSパケットの種類を判別する。TS分離部413は、判別結果に応じて、画像、音声、及びPSI/SI等の種類別にMPEG2-TSパケットを分類する。TS分離部413は、分類したMPEG2-TSパケットをTSデコーダ部415に出力する。

40

【0126】

50

また、制御CPU部414は、TS分離部413から出力されたMPEG2-TSパケットを解析して、解析したMPEG2-TSパケットからデスクランブル制御情報であるリセットフラグを取得する(S305)。制御CPU部414は、TS分離部413から出力された制御CPU部414は、取得したリセットフラグをAVデコーダ部416に出力する。

【0127】

TSデコーダ部415は、TS分離部413によって分離されたMPEG2-TSパケットのうち、ビデオTSパケット及びオーディオTSパケットをエレメンタリストリームに変換するとともに、PSI/SIパケットをセクション形式に変換する(S306)。TSデコーダ部415は、エレメンタリストリーム及びセクション形式に変換したPSI/SIをAVデコーダ部416に出力する。なお、この時点では、エレメンタリストリームは、スクランブルされた状態となっている。

10

【0128】

AVデコーダ部416は、TSデコーダ部415から出力されたエレメンタリストリームと、制御CPU部414から出力されたリセットフラグF6と、初期値管理部417から出力された初期値とに基づいて、エレメンタリストリームをデスクランブルする(S307)。さらに、AVデコーダ部416は、デスクランブルされたエレメンタリストリームをデコードして、ピクチャデータ及びオーディオデータを生成する。AVデコーダ部416は、生成したピクチャデータ及びオーディオデータを、受信装置410外部に接続された出力装置に出力する(S308)。

20

【0129】

続いて、図8を参照して、本発明の実施の形態にかかるAVデコーダ部416の動作について説明する。図8は、本発明の実施の形態にかかるAVデコーダ部416の制御フローチャートである。

【0130】

制御CPU部414は、TS分離部413から出力されたMPEG2-TSパケットから、ビデオTSパケットをサーチする。制御CPU部414は、ビデオTSパケットとしてサーチされたMPEG2-TSパケットのアダプテーション・フィールドF3を解析してリセットフラグF6を取得する(S401)。制御CPU部414は、取得したリセットフラグF6をAVデコーダ部416に出力する。また、TSデコーダ部415は、TS分離部413から出力されたMPEG2-TSパケットをエレメンタリストリーム形式に変換する。TSデコーダ部415は、生成したエレメンタリストリームをAVデコーダ部416に出力する。

30

【0131】

AVデコーダ部416は、制御CPU部414から出力されたリセットフラグF6を取得する(S402)。ここで、TSデコーダ部415からAVデコーダ部416にビデオTSパケットが出力されるときに、そのビデオTSパケットのアダプテーション・フィールドF3中のリセットフラグF6が、制御CPU部414からAVデコーダ部416に出力されるように、それぞれの出力タイミングを同期するものとする。

【0132】

AVデコーダ部416は、取得したリセットフラグF6が"1"であるか否かを判定する(S403)。つまり、AVデコーダ部416は、TSデコーダ部415から出力されたビデオTSパケットが、Iピクチャであるか否かを判定することになる。

40

【0133】

リセットフラグF6が"1"である場合、AVデコーダ部416は、初期値管理部417のICカードリーダーに挿入されているICカードに格納されている初期値を読み出してバッファ39に格納する(S404)。そして、処理は、ステップS405に進む。

【0134】

リセットフラグF6が"1"でない場合、処理は、ステップS405に進む。なお、この場合は、バッファ39には、ビデオデコーダ37によって前回デコードされたピクチャデ

50

ータから生成されたハッシュが格納されていることになる。このハッシュは、後述するステップ S 4 0 8 で格納されることになる。

【 0 1 3 5 】

このように、本実施の形態では、送信装置 4 1 と受信装置 4 1 0 の間でスクランブル / デスクランブル鍵の初期値を共有する手段の一例として I C カードを利用した共有を行っている。具体的には、コンテンツ管理者は、初期値が記録された I C カードを受信装置 4 1 0 のユーザに配布して、ユーザが配布された I C カードを受信装置 4 1 0 に挿入することで、初期値の共有が行われる。

【 0 1 3 6 】

しかし、初期値を共有する方法は、これに限られない。例えば、I C カード以外の外部記憶媒体によって共有するようにしてもよい。外部記憶媒体として、例えば、U S B (U n i v e r s a l S e r i a l B u s) メモリ、外付けハードディスク、又は光ディスク等を使用するようにして、初期値管理部 4 4、4 1 7 がこれらから初期値を読み取り可能としてもよい。また、送信装置 4 1 及び受信装置 4 1 0 に入力装置を有するようにして、コンテンツ管理者又はユーザが入力装置を介して、同一の初期値を初期値管理部 4 4、4 1 7 に対して入力するようにしてもよい。入力装置として、例えば、キーボード及びマウス等を使用するようにしてもよい。

【 0 1 3 7 】

デスクランブラ 3 8 は、バッファ 3 9 に格納された値をデスクランブル鍵として利用して、T S デコーダ部 4 1 5 から出力されたエレメンタリストリームをデスクランブルする (S 4 0 5)。よって、デスクランブラ 3 8 は、送信装置 4 1 のスクランブラ 2 6 と同様に、I ピクチャのエレメンタリストリームについては、初期値によってデスクランブルを行い、その I ピクチャを参照する B ピクチャ及び P ピクチャのエレメンタリストリームについては、前回デコードされたピクチャのハッシュによってデスクランブルを行うことになる。デスクランブラ 3 8 は、デスクランブルしたエレメンタリストリームをビデオデコーダ 3 7 に出力する。

【 0 1 3 8 】

ビデオデコーダ 3 7 は、デスクランブラ 3 8 から出力されたエレメンタリストリームをデコードして、ピクチャデータを生成する (S 4 0 6)。ビデオデコーダ 2 3 は、生成したピクチャデータをハッシュ生成器 3 1 0 に出力する。

【 0 1 3 9 】

ハッシュ生成器 3 1 0 は、ビデオデコーダ 3 7 から出力されたピクチャデータから、ハッシュを生成する (S 4 0 7)。ハッシュ生成器 2 4 は、生成したハッシュをバッファ 3 9 に格納する (S 4 0 8)。

【 0 1 4 0 】

また、ビデオデコーダ 3 7 は、エレメンタリストリームのデコード結果であるピクチャデータを、受信装置 4 1 0 の外部に接続された出力装置 (図示せず) に出力する (S 4 0 9)。

【 0 1 4 1 】

続いて、図 9 を参照して、本実施の形態にかかるメカニズム及び効果について説明する。図 9 は、時間軸上において M P E G 2 - T S パケットの受信タイミングと、それらの M P E G 2 - T S パケットから得られるピクチャとの関係を示す図である。

【 0 1 4 2 】

図 9 は、チャンネル切り替え後のストリームに含まれる M P E G 2 - T S パケット 7 0 4 ~ 7 3 3 の受信が、時刻 7 0 0 から開始される様子を示している。最初に M P E G 2 - T S パケット 7 0 4 受信される。その後は、M P E G 2 - T S パケット 7 0 5 ~ 6 3 3 が順次受信される。

【 0 1 4 3 】

図 9 では、M P E G 2 - T S パケット 7 1 0、7 1 3、7 1 4、7 1 9、7 2 7、7 2 9 のそれぞれは、オーディオ T S パケットを示し、M P E G 2 - T S パケット 7 0 9、7

10

20

30

40

50

16、725のそれぞれは、ECMパケットを示す。それら以外のMP EG 2 - TSパケットのそれぞれは、ビデオTSパケットを示す。

【0144】

各ビデオTSパケットを受信することによって、ピクチャ733～741に示す各種ピクチャを得ることができる。各種ピクチャは、複数のMP EG 2 - TSパケットにより構成される。

【0145】

具体的には、図9に示すMP EG 2 - TSストリームには、ピクチャとして、MP EG 2 - TSパケット703、704により構成されるBピクチャ733と、MP EG 2 - TSパケット708、711により構成されるBピクチャ735と、MP EG 2 - TSパケット712、715により構成されるBピクチャ737と、MP EG 2 - TSパケット723、724により構成されるBピクチャ739と、MP EG 2 - TSパケット726、728により構成されるBピクチャ740と、MP EG 2 - TSパケット705、706、707により構成されるIピクチャ734と、MP EG 2 - TSパケット720、721、722により構成されるIピクチャ738と、MP EG 2 - TSパケット717、718により構成されるPピクチャ737と、MP EG 2 - TSパケット730、731、732により構成されるPピクチャ741と、が含まれている。

【0146】

チャンネル切り替え後、ストリームの受信を開始した時刻700で、MP EG 2 - TSパケット704を得る。MP EG 2 - TSパケット704は、Bピクチャ733を構成するパケットであるが、受信開始時刻700では、MP EG 2 - TSパケット703を受信することができないため、Bピクチャ733は得ることができない。

【0147】

時刻701で、Iピクチャ734を構成するMP EG 2 - TSパケット705、706、707が全て受信される。ステップS401において、制御CPU部414は、MP EG 2 - TSパケット705のアダプテーション・フィールドF3を解析して、ステップS402においてリセットフラグF6を得る。また、ステップS306において、TSデコーダ部415は、Iピクチャ734が含まれるMP EG 2 - TSパケットをエレメンタリストリームに変換する。

【0148】

ステップS403において、AVデコーダ部416は、リセットフラグF6が"1"であるか、又は"0"であるかの判定を行う。ステップS203、S204、S205の処理によって、Iピクチャ734を構成するMP EG 2 - TSパケット705、706、707には、リセットフラグF6に"1"が格納されている。そのため、処理はステップS404に進み、AVデコーダ部416は、初期値管理部417から初期値を読み出してバッファ39に格納する。そして、ステップS405において、デスクランブラ38は、バッファ39に格納された初期値をデスクランブル鍵として、Iピクチャ734が格納されるエレメンタリストリームをデスクランブルすることにより、時刻701でデスクランブルされたIピクチャ734を得ることができる(S406)。

【0149】

また、ステップS407及びS408において、ハッシュ生成器310は、時刻701で得られたIピクチャ734からハッシュを生成し、生成されたハッシュをバッファ39に格納する。

【0150】

時刻701以降は、時刻702にてIピクチャ738を検出するまでに得られるMP EG 2 - TSパケットのアダプテーション・フィールドには"0"が格納されたりリセットフラグF6しか得ることがない。そのため、Bピクチャ735が格納されたエレメンタリストリームをデスクランブルする際は、ステップS408にてバッファ39に格納されたIピクチャ734のハッシュを用いてデスクランブルされる。同様に、Bピクチャ736が格納されたエレメンタリストリームは、ステップS408にてバッファ39に格納されたB

10

20

30

40

50

ピクチャ 7 3 5 のハッシュを用いてデスクランブルされ、P ピクチャ 7 3 7 が格納されたエレメンタリストリームは、ステップ S 4 0 8 にてバッファ 3 9 に格納された B ピクチャ 7 3 6 のハッシュを用いてデスクランブルされる。

【0151】

以上より、本実施の形態では、正常な画像を出力することができる時刻を、図 1 4 に示す時刻 6 0 3 に対応する時刻 7 0 2 から、時刻 7 0 1 にまで短縮することが可能となる。つまり、本実施の形態では、E C M を受信する前に受信した I ピクチャであってもデスクランブルすることができ、正常な画像を得ることができる。よって、E C M を受信した後に到着する I ピクチャを待たなくても良いため、特許文献 1 に開示の技術と比較して、チャンネル切り替え時間を短縮することができるという効果を奏する。

10

【0152】

以上に説明したように、本実施の形態では、予め用意された I ピクチャのデスクランブル鍵によって、I ピクチャをデスクランブルするようにしている。そして、I ピクチャに基づいて、I ピクチャを参照するピクチャのデスクランブル鍵を生成して、生成したデスクランブル鍵によって、I ピクチャを参照するピクチャをデスクランブルする。

【0153】

これによれば、例えば、E C M のような他のデータの受信タイミングに関係なく、I ピクチャを受信した時点から、正常な画像を出力することができる。そのため、本実施の形態によれば、チャンネル切り替え時間を短縮することができる。

【0154】

20

なお、本発明は上記実施の形態に限られたものではなく、趣旨を逸脱しない範囲で適宜変更することが可能である。

【0155】

上述した本実施の形態では、送信装置 4 1 をデジタル放送送信装置に適用し、受信装置 4 1 0 をデジタルテレビ受像機に適用した場合について例示したが、これに限られない。例えば、送信装置 4 1 を、生成した M P E G 2 - T S ストリームを外部記憶媒体に格納するレコーダに適用し、受信装置 4 1 0 を、外部記憶媒体に格納された M P E G 2 - T S ストリームを再生するプレーヤに適用するようにしてもよい。

【0156】

上述した本実施の形態では、ビデオデコーダ 2 3 及びビデオデコーダ 3 7 が生成したピクチャデータに基づいて、ハッシュを生成する場合について例示したが、これに限られない。ピクチャデータにデコードする前のエレメンタリストリームに基づいて、ハッシュを生成するようにしてもよい。

30

【符号の説明】

【0157】

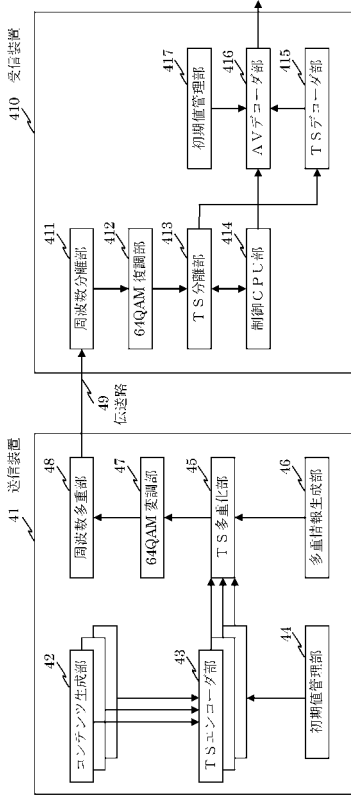
1 1 鍵管理装置
 1 2 K w 暗号化部
 1 3、4 5 T S 多重化部
 1 4 K s 暗号化部
 1 5、2 6 スランブラ
 1 6、4 2 コンテンツ生成部
 1 7 T S エンコーダ
 1 8、4 7 6 4 Q A M 変調部
 1 9、4 9 伝送路
 2 2 ビデオエンコーダ
 2 3、3 7 ビデオデコーダ
 2 4、3 1 0 ハッシュ生成器
 2 5、3 9 バッファ
 2 7 T S 処理部
 3 8、1 1 4 デスクランブラ

40

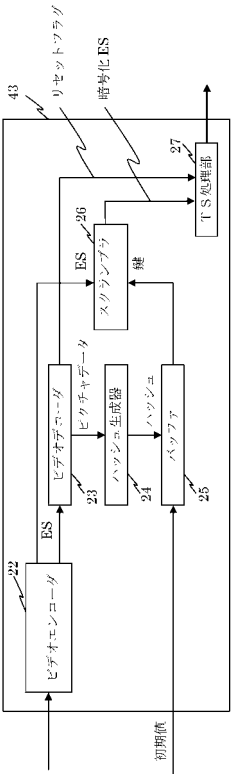
50

4 1、1 2 8	送信装置	
4 3	T S エンコーダ部	
4 4、4 1 7	初期値管理部	
4 6、1 2 5	多重情報生成部	
4 8、1 2 6	周波数多重部	
1 1 0、4 1 0	受信装置	
1 1 1、4 1 2	6 4 Q A M 復調部	
1 1 2、4 1 3	T S 分離部	
1 1 3	制御 C P U	
1 1 5	特殊鍵復号モジュール	10
1 1 6	汎用鍵復号モジュール	
1 1 7、1 2 0	個別鍵 K m i	
1 1 8、1 2 1	K w 復号化部	
1 1 9、1 2 2	K s 復号化部	
1 2 3	T S デコーダ	
1 2 4	A V デコーダ	
1 2 7、4 1 1	周波数分離部	
1 2 8、4 1 0	送信装置	
2 0 0	ビデオ E S	
2 0 1	オーディオ E S	20
2 0 2、2 0 3	ビデオ P E S	
2 0 4、2 0 5	オーディオ P E S	
2 0 6、2 0 7、2 0 8、2 0 9	ビデオ T S パケット	
2 1 0、2 1 1、2 1 2、2 1 3	オーディオ T S パケット	
2 1 4	M P E G 2 - T S ストリーム	
2 1 5、2 1 6、2 1 7、2 1 8	E C M パケット	
2 1 9	E C M	
3 0 0、3 0 1、3 0 3、3 0 5、3 0 6、6 3 4、6 3 6、6 3 7、6 4 0、6 4 1、 7 3 3、7 3 5、7 3 6、7 3 9、7 4 0	B ピクチャ	
3 0 2、6 3 5、6 3 9、7 3 4、7 3 8	I ピクチャ	30
3 0 4、3 0 7、6 3 8、6 4 2、7 3 7、7 4 1	P ピクチャ	
4 1 4	制御 C P U 部	
4 1 5	T S デコーダ部	
4 1 6	A V デコーダ部	
F 1	M P E G 2 - T S パケット	
F 2	T S ヘッダ	
F 3	アダプテーション・フィールド	
F 4	データ・バイト	
F 6	リセットフラグ	

【図 1】



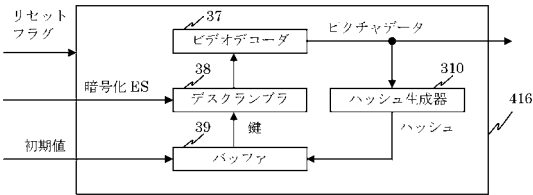
【図 2】



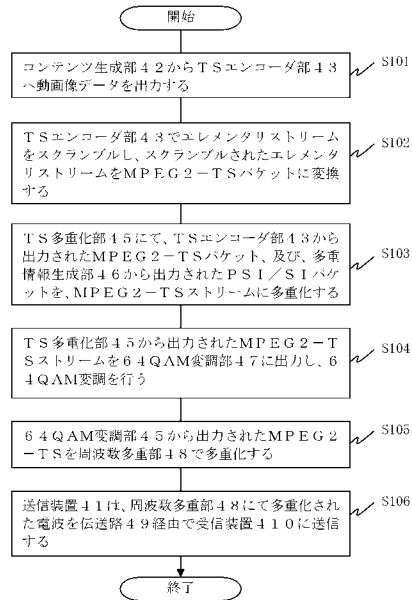
【図 3】



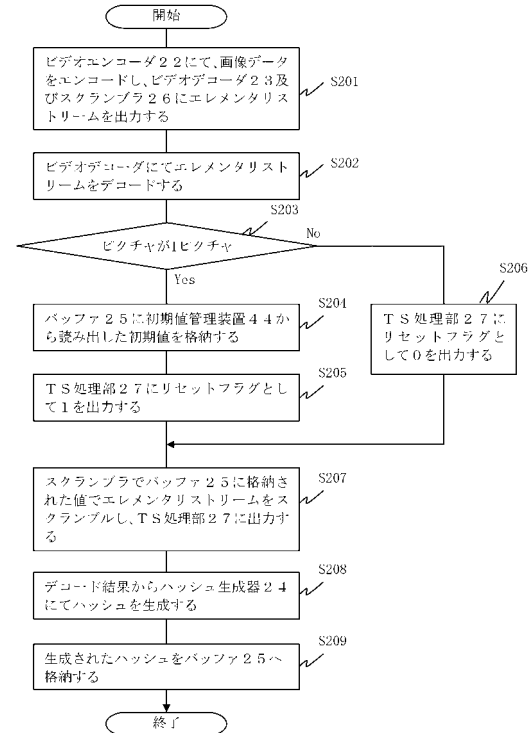
【図 4】



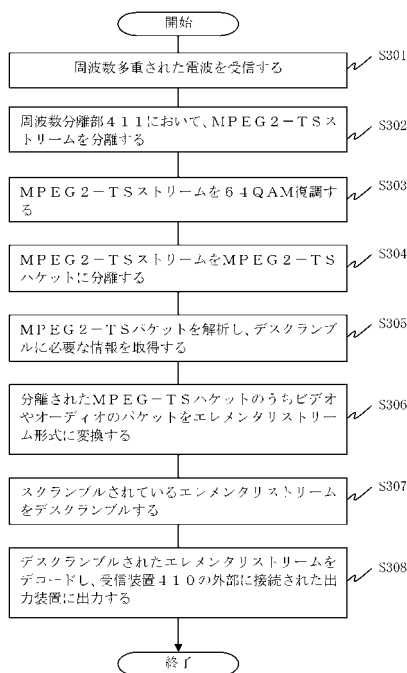
【図 5】



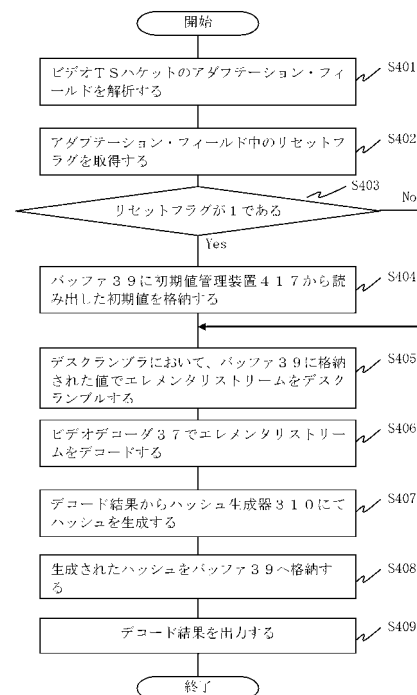
【図 6】



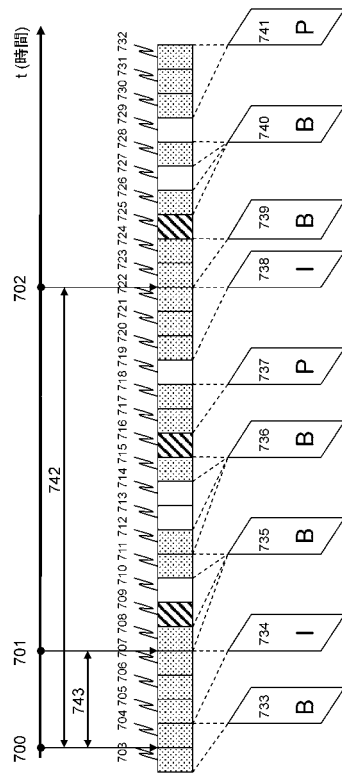
【図 7】



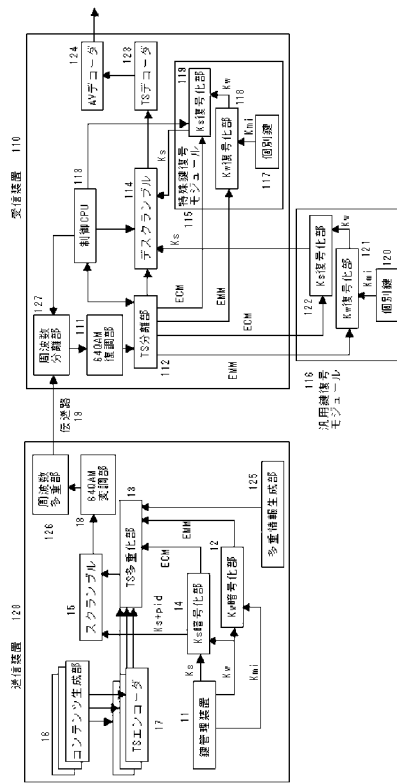
【図 8】



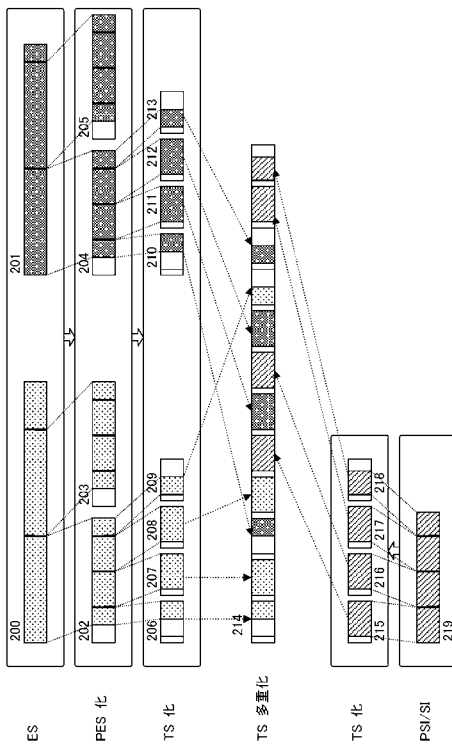
【 図 9 】



【 図 1 0 】



【 図 1 1 】



【 図 1 2 】

