(19)日本国特許庁(JP)　(12)特　許　公　報(B2)　(11)特許番号
特許第3754847号
(P3754847)
(45)発行日　平成18年3月15日(2006.3.15)　(24)登録日　平成17年12月22日(2005.12.22)

(51)Int.Cl.			F I		
H04N	1/387	(2006.01)	H04N	1/387	
G09C	5/00	(2006.01)	G09C	5/00	
H04L	9/08	(2006.01)	H04L	9/00	601D
H04L	9/32	(2006.01)	H04L	9/00	601E
H04N	5/91	(2006.01)	H04L	9/00	673B

請求項の数 11　(全 14 頁)　最終頁に続く

(21)出願番号　特願平11-246723
(22)出願日　平成11年8月31日(1999.8.31)
(65)公開番号　特開2001-78007(P2001-78007A)
(43)公開日　平成13年3月23日(2001.3.23)
審査請求日　平成15年11月27日(2003.11.27)

(73)特許権者　000001007
キヤノン株式会社
東京都大田区下丸子３丁目３０番２号
(74)代理人　100076428
弁理士　大塚　康徳
(74)代理人　100093908
弁理士　松本　研一
(74)代理人　100101306
弁理士　丸山　幸雄
(72)発明者　若尾　聡
東京都大田区下丸子３丁目３０番２号　キヤノン株式会社内
(72)発明者　岩村　恵市
東京都大田区下丸子３丁目３０番２号　キヤノン株式会社内
最終頁に続く

(54)【発明の名称】データ処理方法、データ処理装置およびその記憶媒体

(57)【特許請求の範囲】
【請求項１】
夫々所定の情報を有するオブジェクトストリームを含むデータストリームから前記オブジェクトストリームを分離して再生するデータ処理方法であって、
前記データストリームに含まれる著作権管理情報を抽出し、
前記オブジェクトストリームに含まれる透かし情報を抽出し、
前記データストリームを受信して再生するユーザ又は装置に固有のＩＤ情報と前記著作権管理情報と前記透かし情報とを用いて鍵情報を生成し、
前記オブジェクトストリームを、前記鍵情報に基づいてデスクランブルするように制御することを特徴とするデータ処理方法。
【請求項２】
前記著作権管理情報と前記ＩＤ情報とに基づいて認証情報を生成し、前記認証情報と前記透かし情報とを基に前記鍵情報が生成されることを特徴とする請求項１に記載のデータ処理方法。
【請求項３】
前記著作権管理情報は、著作権を保護、管理するためのストリームに含まれることを特徴とする請求項１又は２に記載のデータ処理方法。
【請求項４】
前記ＩＤ情報は、前記オブジェクトストリームを分離、デスクランブル、再生を行うデータ処理装置に設定されていることを特徴とする請求項１乃至３のいずれか１項に記載の

データ処理方法。
【請求項５】
前記ＩＤ情報は、前記データ処理装置に接続可能な記憶媒体に組み込まれていることを特徴とする請求項４に記載のデータ処理方法。
【請求項６】
前記オブジェクトストリームの情報は高能率符号化されていることを特徴とする請求項１乃至５のいずれか１項に記載のデータ処理方法。
【請求項７】
前記データストリームは、音声オブジェクトストリーム、静止画像オブジェクトストリーム、動画像ストリーム、コンピュータグラフィックストリームのうち少なくとも１つのストリームと、オブジェクトを合成するためのシーン記述情報ストリームとを少なくとも含むことを特徴とする請求項１乃至６のいずれか１項に記載のデータ処理方法。
【請求項８】
オブジェクトストリームを含むデータストリームから前記オブジェクトストリームを分離して再生するデータ処理装置であって、
夫々所定の情報を有する暗号化された少なくとも１つのオブジェクトストリームを含むデータストリームを入力する入力手段と、
前記入力手段により入力された前記データストリームから前記オブジェクトストリームを分離する分離手段と、
前記データストリームに含まれる著作権管理情報を抽出する著作権管理情報抽出手段と、
前記オブジェクトストリームに含まれる透かし情報を抽出する透かし情報抽出手段と、
前記データ処理装置或いは前記データ処理装置に接続可能な記憶媒体に組み込まれたＩＤ情報を収得する収得手段と、
前記著作権管理情報と前記透かし情報及び前記ＩＤ情報とを用いて鍵情報を生成する鍵情報生成手段と、
前記分離手段で分離された前記オブジェクトストリームを、前記鍵情報に基づいてデスクランブルするデスクランブル手段と、
前記デスクランブル手段でデスクランブルされた前記オブジェクトストリームから前記所定の情報を復号化する復号化手段とを有することを特徴とするデータ処理装置。
【請求項９】
更に、前記著作権管理情報と前記ＩＤ情報とに基づいて認証情報を生成する認証情報処理手段を有し、前記鍵情報生成手段は、前記認証情報と前記透かし情報とを基に前記鍵情報生成することを特徴とする請求項８に記載のデータ処理装置。
【請求項１０】
前記著作権管理情報は、著作権を保護、管理するためのストリームに含まれることを特徴とする請求項８又は９に記載のデータ処理装置。
【請求項１１】
請求項１乃至７のいずれか１項に記載のデータ処理方法を実行するコンピュータプログラムを格納し、コンピュータが読取り可能なコンピュータ可読記憶媒体。
【発明の詳細な説明】
【０００１】
【発明の属する技術分野】
本発明はデータ処理方法、データ処理装置、データ処理システムおよびその記憶媒体とコンピュータプログラムに関し、特に複数のオブジェクトストリームから情報を再生するデータ処理方法、データ処理装置およびその記憶媒体に関するものである。
【０００２】
【従来の技術】
近年、動画像や音声などのデータを符号化し、それぞれの符号化データをオブジェクトとして扱い、これら所謂マルチメディアデータを組み合わせて単一のビットストリームとし

て伝送する手法として、ＩＳＯにてＭＰＥＧ－４(Moving Picture Experts Group Phase 4)が標準化されつつある。このＭＰＥＧ－４の受信側（再生側）においては、例えば音声と動画シーンとを関連付けて再生する。このようなＭＰＥＧ－４システムにおいては、データがオブジェクトとして扱われるという特性のために、受信したビットストリームをオブジェクト毎に１つ１つバラバラにして容易に再編成することができる。ここで、各オブジェクトに著作権が存在する場合、その著作権保護を行うために、データの全体又はその一部に対して使用制限を行う必要がある。

【０００３】

上述したようなＭＰＥＧ－４のデータストリームにおいては、これまでの一般的なマルチメディアストリームとは異なり、いくつものビデオシーンやビデオオブジェクトを単一のストリーム上で独立して送受信する機能を有している。また音声についても同様に、いくつものオブジェクトを単一のストリーム上で独立して送受信する機能をも有する。

【０００４】

これらのオブジェクトを合成し、あるシーンを合成するための情報としてＶＲＭＬを修正したＢＩＦＳ(Binary Format For Scenes)が存在する。このＢＩＦＳは、シーンが２値で記述されているもので、このＢＩＦＳに従ってシーンが合成される。

【０００５】

このような、シーンの合成に必要な個々のオブジェクトは夫々、個別に最適な符号化が行われて送信されることになるので、復号（受信）側でも、各オブジェクトは個別に復号される。こうして復号された各オブジェクトは、ＢＩＦＳの記述に従って個々のデータの持つ時間軸を再生機内部の時間軸に同期させてシーンを合成して出力することになる。

【０００６】

このように、ＭＰＧＥ－４再生機では、複数のオブジェクトを合成するので、いずれかのオブジェクトに著作権が存在する場合には、そのオブジェクトの使用制限を行う必要が生じる。

【０００７】

一般的に、著作権保護のためには、送信側において送信データに暗号処理を行うか、又は電子透かしを挿入するといった処理を実行し、受信側、即ち、再生機において、その著作権に対して正当な対価を支払った場合にのみ、その暗号化されたデータを復号するために必要となる情報等を入手して受信したデータを復号し、動画像、音声等のデータを再生することが行われている。

【０００８】

また、電子透かしを用いたＭＰＥＧ－４における著作権保護の方法として以下の方式が考えられる。この方法では、それぞれ所定の情報を有する複数のオブジェクトストリームを含むデータストリームから各オブジェクトストリームを分離し、動画データを復号するためのビデオデコーダを起動する。次に、このビデオデコーダにより動画データが復号されるとともに、電子透かしとして埋め込まれている著作権情報が抽出されて、知的財産を保護するための管理ストリーム中のデータとの間で認証作業を行う。この認証作業の結果、“再生許可”の場合にはそのビデオデコーダに対して動作開始／継続の命令が発行される。これにより、復号された動画像データがシーン合成回路に供給されて動画像データの視聴が可能になる。

【０００９】

一方、その認証作業の結果が“再生不許可”の場合には、そのビデオデコーダに対して動作停止、又はビデオデコーダへのデータの転送停止命令が発行されるので、復号された動画像データがシーン合成回路に供給されなくなり、その動画像の視聴ができなくなる。

【００１０】

【発明が解決しようとする課題】

しかしながら、上記従来の方式では、オブジェクトストリームのデータに電子透かしとして埋め込まれた著作権情報は、一旦、そのストリームのデータが復号されてしまった後に抽出されるという問題がある。これは一旦復号されることにより、画像や音声などのデー

タが再生機のメモリに、暗号等により保護されない状態で存在することを意味している。従って、もし悪意を持った第三者が、このメモリに記憶されているデータをコピーできる環境にあると、この復号されたデータが不法にコピーされて望ましくない。しかしながら、ＭＰＥＧ－４システムにおいては、このような状況に対処するための具体的な方法については何等提案されていなかった。

【００１２】

本発明は上記従来例に鑑みてなされたもので、著作権を有するオブジェクトデータを、第三者による不正な再生から守ることができるデータ処理方法及び装置およびその記憶媒体を提供することにある。

【００１３】

【課題を解決するための手段】

上記目的を達成するために本発明のデータ処理装置は以下のような構成を備える。即ち、

オブジェクトストリームを含むデータストリームから前記オブジェクトストリームを分離して再生するデータ処理装置であって、

夫々所定の情報を有する暗号化された少なくとも１つのオブジェクトストリームを含むデータストリームを入力する入力手段と、

前記入力手段により入力された前記データストリームから前記オブジェクトストリームを分離する分離手段と、

前記データストリームに含まれる著作権管理情報を抽出する著作権管理情報抽出手段と、

前記オブジェクトストリームに含まれる透かし情報を抽出する透かし情報抽出手段と、

前記データ処理装置或いは前記データ処理装置に接続可能な記憶媒体に組み込まれたＩＤ情報を収得する収得手段と、

前記著作権管理情報と前記透かし情報及び前記ＩＤ情報とを用いて鍵情報を生成する鍵情報生成手段と、

前記分離手段で分離された前記オブジェクトストリームを、前記鍵情報に基づいてデスクランブルするデスクランブル手段と、

前記デスクランブル手段でデスクランブルされた前記オブジェクトストリームから前記所定の情報を復号化する復号化手段とを有することを特徴とする。

【００１４】

上記目的を達成するために本発明のデータ処理方法は以下のような工程を備える。即ち、

夫々所定の情報を有するオブジェクトストリームを含むデータストリームから前記オブジェクトストリームを分離して再生するデータ処理方法であって、

前記データストリームに含まれる著作権管理情報を抽出し、

前記オブジェクトストリームに含まれる透かし情報を抽出し、

前記データストリームを受信して再生するユーザ又は装置に固有のＩＤ情報と前記著作権管理情報と前記透かし情報とを用いて鍵情報を生成し、

前記オブジェクトストリームを、前記鍵情報に基づいてデスクランブルするように制御することを特徴とする。

【００１５】

【発明の実施の形態】

以下、添付図面を参照して本発明の好適な実施の形態を詳細に説明する。

【００１６】

本実施の形態では、まず図１に示す一般的なＭＰＥＧ－４再生機の概略構成を説明し、次に本実施の形態に係る再生機のデスクランブル処理の一例を説明する。更に、本実施の形態に係る再生機の動作の一例を示すフローチャートを参照して説明し、そして最後に送信側装置を含むシステム全体の一例を説明する。

【００１７】

図１は、本実施の形態に係るＭＰＥＧ－４再生機の概略基本構成を示すブロック図である。

【００１８】

図１において、伝送路１０１は各種ネットワーク、コンピュータバス等のデータの伝送路であり、本実施の形態では、ＭＰＥＧ－４ストリームが入力されるネットワークを示している。また、本実施の形態における伝送路１０１は、通信路の意味の他に、ＣＤ－ＲＯＭ、ＤＶＤ－ＲＯＭ、ＤＶＤ－ＲＡＭといった記憶媒体の再生装置とのインターフェースも意味している。

【００１９】

本実施の形態の装置において、伝送路１０１、即ち、ネットワークから配信されたＭＰＥＧ－４ストリームや、或は記憶媒体装置から伝送されたＭＰＥＧ－４ストリームは、デマルチプレクサ１０２に入力される。ここでＭＰＥＧ－４ストリームは、シーン記述データ、動画オブジェクトデータ、音声オブジェクトデータ、オブジェクト記述データ等に分離された後、それぞれ対応するメモリ部１０３～１０６に入力されて保存される。即ち、メモリ部１０３にはシーン記述データが、メモリ１０４には音声オブジェクトデータが、メモリ部１０５には動画オブジェクトデータが、メモリ部１０６にはオブジェクト記述データがそれぞれ記憶される。

【００２０】

ここで、音声オブジェクトデータは例えば、周知のＣＥＬＰ(Code Excited Linear Prediction)符号化や、変換領域重み付けインターリーブ・ベクトル量子化(TWINVQ)符号化等の高効率符号化が施されたデータであり、動画像オブジェクトデータは、例えば、周知のＭＰＥＧ－２やIII　Ｈ－２６３方式にて高効率符号化が施されたデータである。

【００２１】

メモリ部１０４～１０６の各オブジェクトデータのそれぞれは、対応する復号部１０７～１１０へ入力される。これらシーン記述復号部１０７、音声復号部１０８、動画像復号部１０９、オブジェクト記述復号部１１０のそれぞれにおいて、上述のような高効率符号化された、シーン記述データ、音声オブジェクトデータ、動画像オブジェクトデータ、オブジェクト記述データのそれぞれが復号される。

【００２２】

尚、本実施の形態においては、音声オブジェクト、動画像オブジェクト、オブジェクト記述データについて夫々複数の互いに異なる種類のオブジェクトがＭＰＥＧ－４ストリームに内に存在しても復号可能な装置を仮定しているため、メモリ部１０４～１０６や復号部１０８～１１０は音声用、動画像用、オブジェクト記述データ用に夫々複数用意されているものとする。

【００２３】

そして、復号部１０８～１１０において夫々復号された音声オブジェクト、動画像オブジェクト、オブジェクト記述データは、シーン記述復号部１０７で復号されたシーン記述データに基づいて、シーン合成部１１２にて合成／グラフィック処理が行われる。このようにして得られた最終的なデータ列は、ディスプレイやプリンタ装置といった出力機器１１３に供給されて可視化されて出力されることになる。

【００２４】

ここで、本実施の形態における受信データストリームには、音声或は動画像などのシーンを構成する個々のオブジェクトデータに対して、著作権などの保護のために再生を実行させたり、再生を停止させたりする制御が必要となる場合には、ＩＰＭＰ情報を用いて制御を行う。このＩＰＭＰ情報は、受信データストリームの構成要素であるＩＰＭＰストリームにて伝送される。

【００２５】

ＩＰＭＰ制御部１１１は、デマルチプレクサ１０２からのＩＰＭＰストリームに含まれるＩＰＭＰ情報１２０に基づき、必要に応じて制御ポイントにおいてストリームを遮断したり、復号部１０８～１１０にアクセスして、復号動作の停止を命令する。

【００２６】
このためＩＰＭＰ情報１２０等によりオブジェクトデータの視聴の権利が無いと判断された場合には、そのオブジェクトデータが復号されなくなるため、その再生が行われなくなる。このような制御を行うことで著作権を有するデータが、第三者により不法に視聴されるなどの事態の発生を防止することができる。
【００２７】
図２は、本実施の形態に係る再生機におけるデスクランブル処理の一例を説明するための図で、前述の図１と共通する部分は同じ番号で示し、それらの説明を省略する。
【００２８】
ここではＩＰＭＰ制御部１１１から出力される著作権管理情報２２１と、記憶媒体Ｉ／Ｆ２０６からの再生機情報２２２とを用いて、認証情報処理部２０５において認証情報２２３が生成されてデスクランブル制御部２０４に送られる。デスクランブル制御部２０４は、この認証情報２２３と、透かし抽出部２０２で抽出された透かし情報２２４とを用いて鍵情報２２５を生成してデスクランブル部２０７に出力する。こうして暗号化されたデータのデスクランブルが行われる。以下、詳しく説明する。
【００２９】
尚、ここで著作権管理情報２２１とは、ＩＰＭＰ情報１２０に記述されている情報であり、再生機情報２２２とは、その再生機の記憶媒体に予め組み込まれている、又はこの再生機に接続可能な外部記憶媒体に組み込まれている情報であり、透かし情報２２４とは、オブジェクトデータに電子透かしとして埋め込まれている情報である。
【００３０】
シーン記述データ、音声オブジェクトデータ、動画像オブジェクトデータ、ＣＧオブジェクトデータ、オブジェクト記述データ、ＩＰＭＰ情報等を含むＭＰＥＧ－４ストリームは、デマルチプレクサ１０２にて各オブジェクトデータに分離された後、音声オブジェクトデータ、動画像オブジェクトデータ、ＣＧオブジェクトデータ等は透かし抽出部２０２に、ＩＰＭＰ情報１２０はＩＰＭＰ制御部１１１に、オブジェクト記述データは復号部１０７～１１０へ夫々送られる。透かし抽出部２０２は、音声、動画及びオブジェクト記述データのそれぞれに対して設けられており、それぞれメモリと抽出部とを備えている。そして、このデマルチプレクサ１０２で分離された各オブジェクトデータのそれぞれは、透かし抽出部２０２の夫々対応するメモリに格納される。尚、ここでは、著作権を有するオブジェクトデータは予め暗号化が施されている。
【００３１】
この暗号化はオブジェクトデータの送信側にて行われ、この暗号化には暗号鍵が必要となる。ここでは正当なユーザの再生機でデスクランブルする時に限り、デスクランブル制御部２０４で生成される鍵情報２２５が、この暗号鍵と同一のデータとなるように制御される。即ち、送信側の装置は、透かし情報、ＩＰＭＰ情報１２０、再生機情報２２２を生成する。そして透かし情報をオブジェクトデータに埋め込み、またＩＰＭＰ情報１２０をＩＰＭＰストリームに組込んで送信する。また再生機情報２２２は、何らかの方法で再生機の記憶媒体に予め組み込むか、又は再生機に接続可能な外部記憶媒体に組み込んでおく。
【００３２】
本実施の形態に係る再生機では、著作権管理情報２２１と再生機情報２２２と透かし情報とを用いて鍵情報２２５が生成されるが、送信側の装置において暗号鍵（つまり鍵情報）の生成を行う時にどの情報を使用するか、及びそれらの情報の組み合わせ方は多数存在する。従って、使用する情報の選択、それらの組み合わせは、そのデータの著作権者、或はサービス提供者により決定される。そのため、この選択、組み合わせの情報を再生機に伝える仕組みが必要になる。ここでは、その選択、組み合わせに関する情報は、ＩＰＭＰ情報１２０によって再生機に伝えられるものとする。
【００３３】
このようにして本実施の形態の再生機では、まずＩＰＭＰ情報１２０を解析する。ＩＰＭＰ制御部１１１のメモリに記憶されたＩＰＭＰ情報１２０は、ＩＰＭＰ制御部１１１の制

御部により解析される。このＩＰＭＰ情報１２０は、ヘッダ部と情報部で構成されており、情報部は更にフラグ部と実データ部とで構成されている。また、この実データ部には、著作権管理情報２２１が記述されている。ＭＰＥＧ－４システムでは、ＩＰＭＰ情報１２０のヘッダ部の構成は規定しているが、実データ部の構成は規定していない。そのため、上記のような構成とすることはＭＰＥＧ－４システムの規格に沿ったものである。

【００３４】

このＩＰＭＰ情報１２０のヘッダ部には、透かし抽出部２０２のメモリに格納されているオブジェクトデータが暗号化されているか否かを示す情報が存在する。具体的には、ＩＰＭＰ情報１２０のヘッダ部のＩＰＭＰ＿Ｔｙｐｅが“１”の場合には、そのオブジェクトデータが暗号化されていることを示す。また、このＩＰＭＰ情報１２０の情報部のフラグ部には、透かしフラグ、認証情報フラグ、再生機情報フラグ、著作権管理情報フラグが存在し、それぞれオブジェクトデータに透かし情報が埋め込まれているか、認証情報２２３が鍵情報２２５を生成する際に必要となるか、再生機情報２２２が認証情報２２３を生成する際に必要となるか、著作権管理情報２２１が認証情報２２３を生成する際に必要となるか、等を示している。ここで著作権管理情報２２１が「必要」となっている場合には、ＩＰＭＰ情報１２０の実データ部に著作権管理情報２２１が記述されていることになる。

【００３５】

本実施の形態では、著作権管理情報２２１と再生機情報２２２とを用いて認証情報２２３が生成され、そしてこの認証情報２２３と透かし情報とを用いて鍵情報２２５が生成されて、この鍵情報２２５を用いて、暗号化されたデータのデスクランブルが行われる場合について説明する。従って、この実施の形態では、上記各フラグにおいて、透かし埋め込み及び認証情報２２３は「必要」、再生機情報２２２は「必要」、著作権管理情報２２１は「必要」であることを示すようにセットされている。

【００３６】

このＩＰＭＰ情報１２０に含まれる著作権管理情報２２１は、ＩＰＭＰ制御部１１１の制御部で取り出されて認証情報処理部２０５へ送られる。また暗号化され、透かし情報が埋め込まれたオブジェクトデータは、透かし抽出部２０２において透かし情報が抽出される。そして、この抽出された透かし情報がデスクランブル制御部２０４に送られた後、その透かし情報が抽出されたオブジェクトデータがデスクランブル部２０７へ送られる。

【００３７】

また、再生機の記憶媒体や再生機に接続されている外部記憶媒体に含まれている再生機情報２２２は記憶媒体Ｉ／Ｆ２０６にて取り出され、認証情報処理部２０５へ送られる。この再生機情報２２２とは、再生機ＩＤ、ユーザＩＤといった夫々の再生機、又はユーザに固有な情報であり、送信側の装置からオフラインで送られるか、或は予め再生機の記憶媒体、外部記憶媒体に組み込まれるものとする。この再生機情報２２２と著作権管理情報２２１とが認証情報処理部２０５において処理されて認証情報２２３が生成されてデスクランブル制御部２０４に送られる。デスクランブル制御部２０４では、透かし抽出部２０２で抽出された透かし情報２２４と、認証情報処理部２０５からの認証情報２２３を基にして鍵情報２２５を生成してデスクランブル部２０７に送る。ここで正当なユーザの再生機である場合には、この鍵情報２２５は送信側で暗号化の際に使用された暗号鍵と同一のデータとなるので、デスクランブル部２０７において、透かし抽出部２０２から送られてきた暗号化されたオブジェクトデータに対してデスクランブル処理を行うことにより、正常にデスクランブルが行われる。

【００３８】

一方で、正当でないユーザの再生機の場合には、デスクランブル制御部２０４で生成された鍵情報２２５が、送信側の装置で暗号化の際に使用された暗号鍵と同一ではないので、正常にデスクランブルが行われないことになる。

【００３９】

こうしてデスクランブル部２０７にてデスクランブルされたデータは、復号部１０７～１１０にて復号されて、動画像、静止画、ＣＧ等のデータが出力される。

【００４０】
このように本実施の形態によれば、データの再生が許可されていないユーザの再生機では、オブジェクトデータは暗号化されたままの状態でメモリ等に存在するので、第三者によるデータのコピー等の脅威から、著作権を有するデータを保護することができる。
【００４１】
更に、電子透かしをオブジェクトデータに埋め込んで伝送することにより、透かしとして埋め込むデータ量分だけ伝送効率が良くなる。更には、鍵情報の基になる重要な情報が埋め込まれることで、セキュリティーの面でも良い効果が得られる。
【００４２】
上記では、著作権管理情報２２１と再生機情報２２２とを用いて認証情報２２３が生成され、そして認証情報２２３と透かし情報２２４とを用いて鍵情報２２５が生成され、その鍵情報２２５を用いて、暗号化されたデータのデスクランブルを行う場合について説明したが、これら透かし情報２２４、再生機情報２２２、著作権管理情報２２１のうち少なくても１つを用いて鍵情報２２５が生成されて、この鍵情報２２５がデスクランブルに用いられるようにしてもよい。この場合には、ＩＰＭＰ情報１２０のヘッダ部、情報部の内容を再生機が解析して、透かし情報、再生機情報、著作権管理情報の中から必要な情報を取得し、それを処理することで最終的には鍵情報２２５が生成されてデスクランブル処理が行われることになる。
【００４３】
ここで、ＭＰＥＧストリームへある情報の埋め込みと暗号化を同時に行い、再生機側でデスクランブル前に、この埋め込まれた情報を抽出する方法に関しては、「圧縮動画像に関するスクランブル・電子透かしの一手法」（第２１回情報理論とその応用シンポジュウム）に詳しい。
【００４４】
一般にＭＰＥＧ方式において、画像は１６×１６画素のマクロブロックに分割された後にフレーム予測が行われ、更に８×８画素のブロック毎にＤＣＴ（離散コサイン変換）が行われてＤＣＴ係数が算出される。これらＤＣＴ係数は変換後にジグザグスキャンされ、ゼロの係数を表すランと、係数を表すレベルの組で可変長の符号語として表される。このようなＭＰＥＧ方式では、レベルは異なるが、同じ符号語長及びラン値を持つ符号語は必ず複数存在することに着目する。最初に、暗号化／埋め込み対象の符号語Ｃiと同じ符号語長、ラン値を持つ符号語を、レベルの値が偶数であれば偶数番目に、奇数であれば奇数番目になるように配置する。次に暗号鍵から乱数列Ｓiを発生させ、暗号化／埋め込み対象の符号語Ｃiを、上記での２(Si mod N)＋Wi番目に配置されている符号語Ｃi’と置き換えることで暗号化と埋め込みを行う。ここでＮはＣiと同じ符号語長及びラン値を持つ符号語の数であり、Wiは“１”又は“０”をとる値である（対象の符号語に情報を埋め込む時は“１”を、埋め込まない時は“０”を選択する）。
【００４５】
こうして埋め込まれた情報を抽出する際は、上記配置においてＣi’が奇数番目に配置されていれば“１”が、偶数番目に配置されていれば“０”が埋め込まれていることに基づいて行われる。
【００４６】
ここでデスクランブルとは、Ｃi’が奇数番目に配置されている時には、１＋２(Si mod N)分、上記とは逆方向に配置されている符号語がＣiとなる。Ｃi’が偶数番目に配置されている時には、２(Si mod N)分、上記とは逆に配置されている符号語がＣiとなる。
【００４７】
このような方式を採用することにより、暗号化されたＭＰＥＧストリームに埋め込まれた情報をデスクランブル前に抽出することが可能となる。ただし、上記の方式が唯一のものではなく、他の方式を用いても暗号化されたＭＰＥＧストリームに埋め込まれた情報をデスクランブル前に抽出することは可能である。
【００４８】

以下では本発明の実施の形態に係る再生機における動作、特にデスクランブル制御と鍵情報生成処理の一例について図３のフローチャートを参照して説明する。

【００４９】

図３は、本実施の形態の再生機において、再生機情報２２２と著作権管理情報２２１とから認証情報２２３を生成し、その認証情報２２３と透かし情報２２４とから鍵情報２２５を生成し、この鍵情報２２５を用いて暗号化データのデスクランブルを行うデスクランブル処理と鍵情報生成処理を説明するためのフローチャートである。以下、一連の処理を、鍵情報２２５の生成と、暗号化／透かしデータのデスクランブルの２つ処理の流れに分けて説明する。

【００５０】

まずステップＳ３０１で、再生機は、シーン記述情報、動画オブジェクトデータ、音声オブジェクトデータ、オブジェクト記述データ、ＩＰＭＰ情報等を含むＭＰＥＧ－４ストリームを受信すると、デマルチプレクサ１０２にて各オブジェクトデータに分離する。次にステップＳ３０２では、デマルチプレクサ１０２により分離した各オブジェクトデータを、それぞれ対応するメモリ部に格納する。ここで、ＩＰＭＰ情報１２０については、鍵情報生成処理ルーチンが処理を行い、暗号化／透かしが埋め込まれた動画オブジェクトデータ、音声オブジェクトデータについては、デスクランブル処理ルーチンが処理を行う。以下のステップＳ３０３、Ｓ３０５、Ｓ３０６、Ｓ３０７、Ｓ３０８の処理は、鍵情報生成処理ルーチンが行い、ステップＳ３０４及びＳ３０９の処理はデスクランブル処理ルーチンが行う。

【００５１】

まず最初に、鍵情報生成処理ルーチンの処理について説明する。

【００５２】

ステップＳ３０３では、ＩＰＭＰ情報１２０に記述されている情報を解析して次にどのような動作を行うかを決定する。本実施の形態では、再生機情報２２２と著作権管理情報２２１とから認証情報２２３が生成され、そしてこの認証情報２２３と透かし情報２２４とから鍵情報２２５が生成される。そして、この鍵情報２２５を用いて暗号化データのデスクランブルが行われるので、ＩＰＭＰ情報１２０において、オブジェクトデータは「暗号化、透かし埋め込み」、認証情報２２３は「必要」、再生機情報２２２は「必要」、著作権管理情報２２１は「必要」をそれぞれ示していることになる。

【００５３】

そこで鍵情報生成処理ルーチンでは、まずステップＳ３０５で再生機情報２２２を抽出し、ステップＳ３０６で著作権管理情報２２１を抽出し、ステップＳ３０７で、この再生機情報２２２と著作権管理情報２２１とから認証情報２２３を生成し、ステップＳ３０８で、この認証情報２２３と透かし情報２２４とから鍵情報２２５を生成するという順に各処理を行う。またステップＳ３０３では、ＩＰＭＰ情報１２０の透かし埋め込みフラグが「透かし埋め込み」を示しているので、鍵情報生成処理ルーチンでは、後述するデスクランブル処理ルーチン（Ｓ３０４）に対して、オブジェクトデータから透かし情報２２４を抽出し、その抽出した透かし情報２２４を鍵情報生成処理ルーチン（Ｓ３０８）へ入力するような命令を発行する。

【００５４】

以下、各ステップを説明すると、まずステップＳ３０５では、再生機の記憶媒体に予め組み込まれている、もしくは再生機に接続可能な外部記憶媒体に組み込まれている再生機情報２２２を抽出する。次にステップＳ３０６では、ＩＰＭＰ情報１２０の情報部に記述されている著作権管理情報２２１を抽出する。次にステップＳ３０７に進み、上記ステップＳ３０５で抽出した再生機情報２２２と、ステップＳ３０６で抽出した著作権管理情報２２１とから認証情報２２３を生成する。

【００５５】

次にステップＳ３０８に進み、鍵情報生成処理ルーチンにおいて、上記ステップＳ３０７で生成した認証情報２２３と、デスクランブル処理ルーチンが抽出した透かし情報２２４

とから鍵情報２２５を生成し、その鍵情報２２５をデスクランブル処理ルーチン（Ｓ３０９）に出力する。

【００５６】

次にデスクランブル処理ルーチンについて説明する。

【００５７】

まずステップＳ３０４では、ＩＰＭＰ情報１２０の透かし埋め込みフラグが「埋め込み」を示しているので、鍵情報生成処理ルーチン（Ｓ３０３）からの命令に従って動画オブジェクトデータ、音声オブジェクトデータ等のオブジェクトデータに埋め込まれている透かし情報２２４を抽出する。そして、この抽出した透かし情報２２４を鍵情報生成処理ルーチン（Ｓ３０８）へ入力する。

【００５８】

ステップＳ３０９では、ステップＳ３０８において生成された鍵情報２２５により暗号化データのデスクランブルが行われる。ここでは、正当なユーザの再生機の場合には、鍵情報処理ルーチンにて正しい鍵情報２２５（送信側でオブジェクトデータを暗号化する際に使用した暗号鍵）が生成されるので、正しくデスクランブルできるが、正当でないユーザの再生機の場合には、正しくない鍵情報２２５が生成されて使用されるので、正しくデスクランブルできない。

【００５９】

このようなサイクルを繰り返すことにより、暗号化されたオブジェクトデータのデスクランブルが行われ、もしも再生機がオブジェクトデータの正当なユーザでない場合、データが正しくデスクランブルされることがないので、オブジェクトデータを再生することができない。

【００６０】

［データ処理システムの説明］

図４は、以上説明した本実施の形態に係る再生機と、この再生機に符号化データを送信する符号化装置を含むデータ処理システム全体の構成例を示す図である。

【００６１】

コンテンツＤＢ４０２には、ＭＰＥＧ－４ストリームのコンテンツとして伝送される動画像、音声、ＣＧ等の各データが保存されていて、その伝送要求に応じて、各データが符号化部４０３へ送られる。符号化部４０３では、コンテンツＤＢ４０２から送られてきた各データに応じた高効率符号化を行う。これは、音声データであれば、ＣＥＬＰ符号化や変換領域重み付けインターリーブ・ベクトル量子化符号化を意味し、動画像データであればＨ－２６３やＤＣＴ変換に基づいた圧縮符号化を示している。シーン記述情報は符号化された後に直ちに多重化部４１１へ送られる。これはシーン記述情報が各オブジェクトを再生する際に必要となるデータであり、動画像、音声といった著作権を有する可能性のあるコンテンツデータではないので暗号化する必要がないためである。符号化部４０３で符号化された各データは暗号化／透かし埋め込み部４０４へ送られて暗号化され、かつ透かしの挿入が行われる。この「圧縮動画像に関するスクランブル・電子透かしの一手法」で説明したような、符号化、暗号化、透かし埋め込みが同時に行われるような方式では、符号化部４０３と暗号化／透かし埋め込み部４０４は１つの部分で構成される。

【００６２】

暗号化／透かし埋め込み部４０４では、符号化された音声、動画及びオブジェクト記述データのそれぞれに対して、鍵情報生成部４０５からの鍵情報４２０に基づいた暗号化と、透かし情報生成部４０６からの透かし情報４２１のデータへの埋め込みが行われる。この暗号化は著作権を有するデータに対して行われるものであり、暗号化の必要性がない、つまり著作権を有しないデータは、この暗号化／透かし埋め込み部４０４をスキップして多重化部４１１へ送られる。また、透かしを埋め込む必要がない場合も同様に、この暗号化／透かし埋め込み部４０４をスキップする。

【００６３】

鍵情報生成部４０５では、制御部４０８の制御に従って鍵情報４２０を生成する。この鍵

情報４２０は、暗号化／透かし埋め込み部４０４において、データの暗号化の際に使用されるデータ、つまり暗号鍵である。

【００６４】

透かし情報生成部４０６は、制御部４０８の制御の下に透かし情報を生成する。この透かし情報４２１は、暗号化／透かし埋め込み部４０４にてデータに埋め込まれるデータである。

【００６５】

著作権を有するコンテンツデータが正当なユーザの再生機のみでデスクランブル、復号、再生できるようにするためには、暗号化で使用される鍵情報４２０、埋め込まれる透かし情報４２１、ＩＰＭＰ情報１２０及び再生機情報２２２が正しく組み合わさり、正確なタイミングで再生機に送られる必要がある。そこで制御部４０８では、ユーザ管理部４０７からの制御情報に基づいて、鍵情報生成部４０５、透かし情報生成部４０６、ＩＰＭＰ情報生成部４０９を制御することにより、鍵情報４２０の生成、透かし情報４２１の生成、ＩＰＭＰ情報１２０の生成処理を管理して、再生機４１０がコンテンツの正当なユーザである場合にのみ正常なデスクランブルが行えるようにしている。

【００６６】

再生機情報２２２は、例えば再生機ＩＤ、受信者ＩＤといったそれぞれの再生機又はユーザに固有な情報であり、制御部４０８が生成して再生機４１０内の記憶媒体又は外部記憶媒体に予め組み込むか、或はオフラインで送られる。

【００６７】

ユーザ管理部４０７では、符号化されて送出されるコンテンツデータがどのようなものであるか、契約者は誰であるのかといった情報を有している。具体的には、そのコンテンツデータが著作権を有するデータであるか、有しないデータであるかといった情報を有している。そして著作権を有するデータである場合には、正当なユーザ（契約者）の氏名、契約期間、契約形態、ユーザＩＤまたは再生機ＩＤなどが含まれている。更には、正当なユーザの再生機４１０において鍵情報２２５を生成するためには、透かし情報、再生機情報、著作権管理情報のうち、いずれを必要とするかという情報を備えてもよい。そしてこれらの情報を基にして制御情報を制御部４０８に送る。

【００６８】

ＩＰＭＰ情報生成部４０９では、制御部４０８からの制御情報を基にして、透かし情報、著作権管理情報、再生機情報のうちのいずれが使用され、どのように組み合わされているかについての情報である各フラグ情報や、著作権管理情報の実データを生成し、これらの情報を基にしてＩＰＭＰ情報１２０を生成して多重化部４１１へ送る。

【００６９】

例えば、図２に基づいて説明した「著作権管理情報と再生機情報とを用いて認証情報が生成され、そして認証情報と透かし情報とを用いて鍵情報が生成されて、暗号化されたデータのデスクランブルが行われる」場合には、ＩＰＭＰ情報１２０のヘッダ部のＩＰＭＰ＿Ｔｙｐｅ＝１、情報部のフラグ部では、透かし情報は「埋め込み」、認証情報は「必要」、再生機情報は「必要」、著作権管理情報は「必要」をそれぞれ示す情報が設定される。

【００７０】

多重化部４１１では、これら符号化された動画像、音声、ＣＧ等の各データ、シーン記述情報、ＩＰＭＰ情報１２０の各データを多重化してＭＰＥＧ－４ストリームを生成する。その後、このＭＰＥＧ－４ストリームが再生機４１０に向けて送出される。

【００７１】

このような送信側装置４０１と再生機４１０でＭＰＥＧ－４のデータ処理システムを構成することで、著作権を有するオブジェクトデータが正当な再生機４１０のみで再生可能になり、また正当でない再生機では暗号化されたままのデータしか扱えないため、著作権データの保護が可能になる。

【００７２】

なお本発明は、複数の機器（例えばホストコンピュータ、インターフェース機器、リーダ

、プリンタなど）から構成されるシステムに適用しても、一つの機器からなる装置（例えば、複写機、ファクシミリ装置など）に適用してもよい。

【００７３】

また、本発明の目的は、前述した実施形態の機能を実現するソフトウェアのプログラムコードを記録した記憶媒体（または記憶媒体）を、システムあるいは装置に供給し、そのシステムあるいは装置のコンピュータ（またはCPUやMPU）が記憶媒体に格納されたプログラムコードを読み出し実行することによっても達成される。この場合、記憶媒体から読み出されたプログラムコード自体が前述した実施形態の機能を実現することになり、そのプログラムコードを記憶した記憶媒体は本発明を構成することになる。また、コンピュータが読み出したプログラムコードを実行することにより、前述した実施形態の機能が実現されるだけでなく、そのプログラムコードの指示に基づき、コンピュータ上で稼働しているオペレーティングシステム(OS)などが実際の処理の一部または全部を行い、その処理によって前述した実施形態の機能が実現される場合も含まれる。

【００７４】

さらに記憶媒体から読み出されたプログラムコードが、コンピュータに挿入された機能拡張カードやコンピュータに接続された機能拡張ユニットに備わるメモリに書込まれた後、そのプログラムコードの指示に基づき、その機能拡張カードや機能拡張ユニットに備わるCPUなどが実際の処理の一部または全部を行い、その処理によって前述した実施形態の機能が実現される場合も含まれる。

【００７５】

以上説明したように本実施の形態によれば、複数の暗号化されたオブジェクトストリームの少なくとも１つについて、暗号化ストリームのデスクランブルを行う際に鍵情報に基づいてデスクランブルを行う。ここで、この鍵情報は、透かし情報、著作権管理情報、再生機情報のうちからの少なくとも１つを用いて生成される。この透かし情報は、このオブジェクトストリームに電子透かしとして埋め込まれ、著作権管理情報は知的財産を保護、管理するためのストリームに含まれ、再生機情報は各オブジェクトストリームを分離、デスクランブル、再生を行うデータ処理装置の記憶媒体に予め組み込まれている、またはデータ処理装置に接続可能な外部記憶媒体に組み込まれるようにすることで、著作権を有するデータが暗号化されていない状態で正当でないユーザの再生機上のメモリ等に存在する虞がなくなる。このようにして、著作権を有するデータを、第三者による不正コピー等の脅威から守ることが可能になった。

【００７６】

また、透かし情報を電子透かしとして埋め込む場合には、透かし情報をオブジェクトデータに埋め込んで伝送することにより、透かしとして埋め込むデータ量分だけ伝送効率が良くなる。

【００７７】

更には、鍵情報の基になる重要な情報が埋め込まれることで、セキュリティーの面でも良い効果が得られる。

【００７９】

【発明の効果】

以上説明したように本発明によれば、著作権を有するオブジェクトデータを、第三者による不正な再生から守ることができるという効果がある。

【図面の簡単な説明】

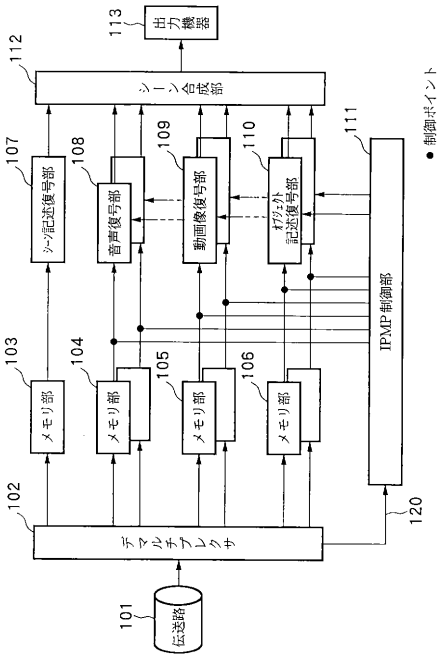
【図１】本実施の形態に係るＭＰＥＧ－４再生機の概略基本構成を示すブロック図である。

【図２】本発明の実施の形態に係るデータ処理装置の動作を説明するための機能ブロック図である。

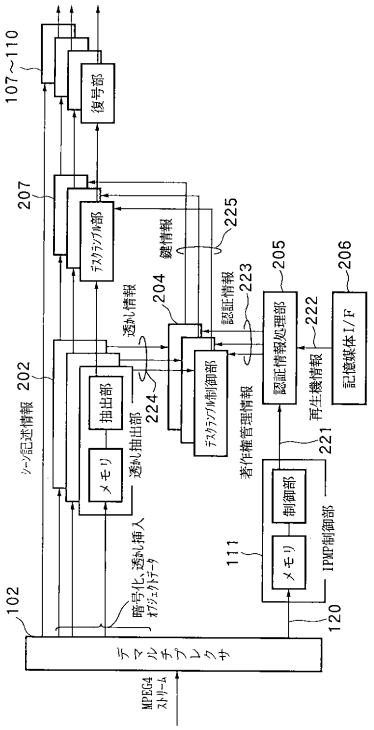
【図３】本実施の形態のデータ処理装置の動作を説明するためのフローチャートである。

【図４】本実施の形態のデータ処理装置および送信側装置を含むデータ処理システムの機能ブロック図である。

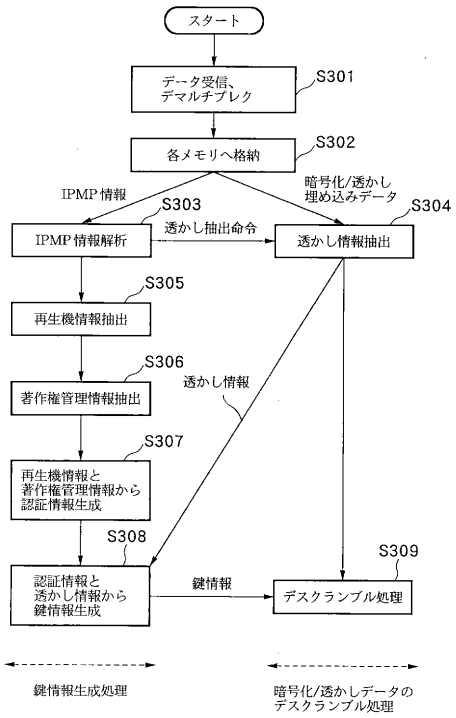
【図１】


出力機器
113
シーン合成部
112
111
● 制御ポイント
IPMP制御部
120
シーン記述復号部
107
音声復号部
108
動画像復号部
109
オブジェクト記述復号部
110
メモリ部
103
メモリ部
104
メモリ部
105
メモリ部
106
デマルチプレクサ
102
伝送路
101

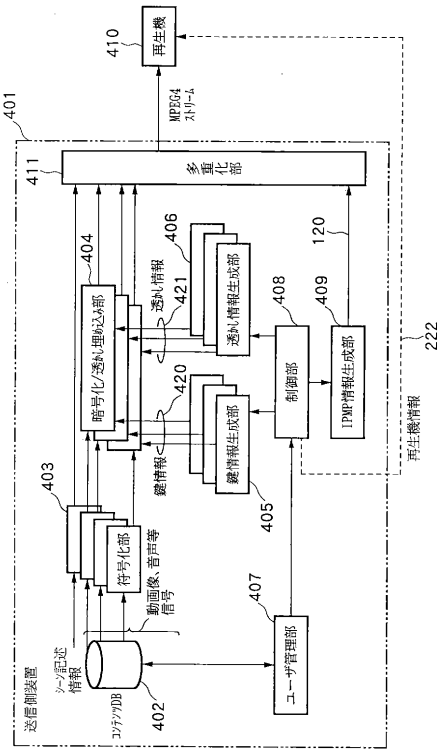
【図２】


107～110
復号部
207
デスクランブル部
225
鍵情報
透かし情報
204
認証情報
223
205
206
202
抽出部
224
デスクランブル制御部
認証情報処理部
222
記憶媒体I/F
シーン記述情報
メモリ
透かし抽出部
著作権管理情報
再生機情報
221
制御部
IPMP制御部
暗号化、透かし挿入オブジェクトデータ
111
メモリ
102
120
デマルチプレクサ
MPEG4ストリーム

【図３】


スタート
データ受信、デマルチプレク
S301
各メモリへ格納
S302
IPMP情報
暗号化/透かし埋め込みデータ
S303
S304
IPMP情報解析
透かし抽出命令
透かし情報抽出
S305
再生機情報抽出
S306
著作権管理情報抽出
透かし情報
S307
再生機情報と著作権管理情報から認証情報生成
S308
S309
認証情報と透かし情報から鍵情報生成
鍵情報
デスクランブル処理
鍵情報生成処理
暗号化/透かしデータのデスクランブル処理

【図４】


410
再生機
MPEG4ストリーム
401
411
多重化部
404
暗号化/透かし埋め込み部
406
透かし情報
421
透かし情報生成部
120
408
409
420
鍵情報
鍵情報生成部
制御部
IPMP情報生成部
222
再生機情報
403
符号化部
405
動画像、音声等
信号
407
ユーザ管理部
シーン記述情報
コンテンツDB
402
送信側装置

フロントページの続き

(51)Int.Cl.		FI		
H04N 7/167	***(2006.01)***	H04N	5/91	P
		H04N	7/167	Z

審査官　白石　圭吾

(56)参考文献　特開平１１－２９８８７８（ＪＰ，Ａ）
特開平１１－０８５９６６（ＪＰ，Ａ）
特開平１０－３１３４０２（ＪＰ，Ａ）
特開平０８－２４２４３８（ＪＰ，Ａ）

(58)調査した分野(Int.Cl.，ＤＢ名)
H04N 1/387
H04N 7/08