(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2005-39835
(P2005-39835A)
(43)公開日　平成17年2月10日(2005.2.10)

(51)Int.Cl.[7]		F I			テーマコード（参考）
H04N	7/167	H04N	7/167	Z	5C059
H04L	9/08	H04L	9/00	601B	5C064
H04L	9/18	H04L	9/00	601E	5J104
H04N	7/24	H04N	7/13	Z	
		H04L	9/00	651	

審査請求 未請求　請求項の数 11　OL　（全 11 頁）

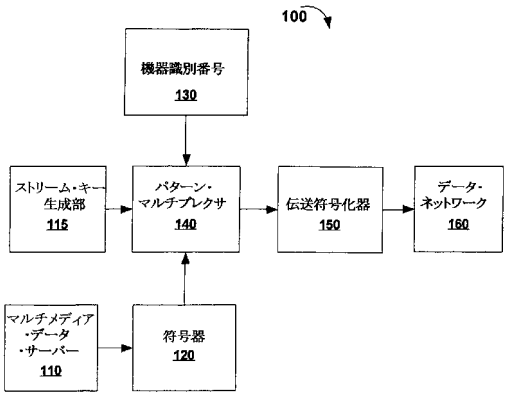
(21)出願番号　特願2004-208600(P2004-208600)
(22)出願日　平成16年7月15日(2004.7.15)
(31)優先権主張番号　03102202.3
(32)優先日　平成15年7月17日(2003.7.17)
(33)優先権主張国　欧州特許庁(EP)

(71)出願人　501263810
トムソン　ライセンシング　ソシエテ　アノニム
Ｔｈｏｍｓｏｎ　Ｌｉｃｅｎｓｉｎｇ　Ｓ．Ａ．
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
(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】個別画像暗号化システム及び暗号化方法

(57)【要約】
【課題】　マルチメディアデータを容易に保護することができる方法及び装置を提供することを課題とする。
【解決手段】　暗号化マルチメディアデータ（３１０）、復号化情報、及び、ストリーム・キー・データにより構成される多重化データ・ストリームを生成する方法が提供される。多重化データ・ストリーム（３２０）を生成する処理には、ストリーム・キー・データ及び機器識別番号を考慮して決定される多重パターンが用いられる。機器識別番号は、多重化データ・ストリームの受信者に対応することが望ましい。多重化データ・ストリームの一部として送信されるストリーム・キー・データは、所定の位置に配置される。これは、ストリーム・キー・データを所定の位置から抽出する復号器のためである。そして、多重化データ・ストリームは、伝送向けに処理される（３３０）。多重化データ・ストリームを逆多重化するための方法及び装置も提供される。
【選択図】　図１



【特許請求の範囲】
【請求項１】
複数種類のデータを多重化データ・ストリームに多重化する方法であって、
マルチメディアデータを暗号化マルチメディアデータに符号化するステップ（Ｓ３１０）と、
前記暗号化マルチメディアデータに、ストリーム・キー・データ及び復号化情報を多重化するステップ（Ｓ３２０）と
を含み、
前記多重化ステップ（Ｓ３２０）は、ストリーム・キー・データと機器識別番号を考慮して実行されることを特徴とする方法。
【請求項２】
請求項１記載の方法であって、前記データ・ストリームの所定の位置に、前記ストリーム・キー・データが挿入されていることを特徴とする方法。
【請求項３】
請求項１記載の方法であって、前記符号化ステップは、
マルチメディアデータをＭＰＥＧ－２等のマルチメディアデータ形式に符号化するステップと、
前記の符号化されたマルチメディアデータを暗号化するステップと、
を有することを特徴とする方法。
【請求項４】
請求項１記載の方法であって、前記データ・ストリームは、データ・ネットワーク経由での送信用に処理されることを特徴とする方法。
【請求項５】
請求項１記載の方法であって、前記機器識別番号は、前記多重化データ・ストリームの受信者に対応することを特徴とする方法。
【請求項６】
請求項１記載の方法であって、前記多重化ステップは、前記暗号化マルチメディアデータが使用されるアプリケーションを考慮して実行されることを特徴とする方法。
【請求項７】
複数種類のデータを多重化データ・ストリームに多重化するデータ多重化装置であって、
マルチメディアデータを暗号化マルチメディアデータに符号化する符号器（１２０）と、
前記暗号化マルチメディアデータに、ストリーム・キー・データ及び復号化情報を多重化するパターン・マルチプレクサ（１４０）と
を有し、
前記パターン・マルチプレクサ（１４０）は、前記ストリーム・キー・データ及び機器識別番号を考慮して前記多重化を実行することを特徴とするデータ多重化装置。
【請求項８】
複数種類のデータが多重化された多重化データ・ストリームを、暗号化マルチメディアデータと、復号化情報と、ストリーム・キー・データとに逆多重化する際に、
前記ストリーム・キー・データと機器識別番号を考慮して逆多重化するステップ
を含むことを特徴とする方法。
【請求項９】
請求項８記載の方法であって、前記ストリーム・キー・データは、前記ストリーム・キー・データの所定の箇所に配置されることを特徴とする方法。
【請求項１０】
請求項８記載の方法であって、前記暗号化マルチメディアデータは、前記復号化情報を用いて、再生に適した形式に復号化されることを特徴とする方法。
【請求項１１】

複数種類のデータが多重化された多重化データ・ストリームを逆多重化するデータ逆多重化装置であって、
前記多重化データ・ストリームを、暗号化マルチメディアデータと、復号化情報と、ストリーム・キー・データとに逆多重化し、当該逆多重化を前記ストリーム・キー・データと機器識別番号とを考慮して行うパターン・デマルチプレクサ（５４０）と、
前記逆多重化データ・ストリームを再生又は記憶に適した形式に復号化する復号器（５２０）と、
を有することを特徴とするデータ逆多重化装置。
【発明の詳細な説明】
【技術分野】
【０００１】
本発明は、マルチメディアデータを暗号化するための方法及び装置に関し、特に、送信前に暗号化されるマルチメディアデータに関する。
【背景技術】
【０００２】
インターネット等のデータ・ネットワークの発展及びブロードバンド接続の広範な普及に伴い、画像や音声のデータ（例えば、テレビ番組、映画、ビデオ会議、及び、ラジオ番組）を選択し、かつ、通信ネットワークを介してオン・デマンドで受信したいという需要がユーザの間で高まっている。オン・デマンド配信システムを設計する際には、メディア・オブジェクトの配信に用いられるコーデック（符号化／復号化プログラム）、配信されるマルチメディアデータの送信で問題となるＱｏＳ（サービス品質）、通信ネットワークを介したマルチメディアデータ（信号として配信される音声データや画像データ）の送信方法などを考慮しなければならない。
【０００３】
一般的に、コーデックはソフトウェアとハードウェアとを組み合わせて導入される。このシステムが用いられるのは、通信ネットワークの送信元でメディアのマルチメディアデータを符号化する際と、その通信ネットワークの受信先でデータを復号化する際である。コーデックの設計時に考慮すべき問題としては、ネットワーク帯域幅のスケーラビリティ、データの符号化／復号化時の計算の複雑性、ネットワーク損失（データ損失）に対する復元性、メディア・ストリームであるデータを送信する際の符号器／復号器の待ち時間などがある。これらの詳細な問題について考慮したコーデックの例としては、離散コサイン変換（ＤＣＴ）（例えば、ＩＴＵの「低ビット・レート通信のための画像符号化方法Ｈ．２６３」に記載されている画像符号器）と、ＤＣＴ以外の技術（例えば、ウェーブレットやフラクタル）の両方を用いた、一般的に使用されるコーデックがある。通信ネットワークで使用可能な帯域幅は限られているため、コーデックはデータの圧縮及び伸張にも用いられる。
【０００４】
サービスの質の問題は、音声及び画像情報の配信や、メディアを鑑賞するユーザの総合的な経験に関連する。メディア・オブジェクトは、パケットと呼ばれる個々の単位で通信ネットワークを介して配信される。通常、連続して送信されるこれらの情報単位は、サーバーやルーターなどのノードを介してデータ・ネットワークを通じて送られる。連続して送信された二つのパケットは、インターネット上の異なるパスを通って、一つの送信先に異なる時間に到着する。ＱｏＳのばらつき等の問題が生じ得るのは、後に送信されたパケットが、先に送信されたパケットよりも早く、送信先の装置で処理されて表示される場合である。これは、表示画像が途切れる原因になる。同様に、送信中にパケットが失われる可能性もある。通常、送信先の装置は、データ損失を目立たなくするために誤り補正を行う。ネットワーク上のＱｏＳを確保する方法、例えば送信パケット数の割り当てや、負荷のかかった状態にあるネットワークの質を向上させる方法を使用することもできるが、これらの方法はオーバーヘッドの増大をもたらし、ネットワークのパフォーマンスに影響を及ぼしてしまう。

【０００５】
通信ネットワークにおいては、データ・パケットの伝送制御に、伝送プロトコルを用いる。ＩＥＴＦ（Internet Engineering Task Force）のＲＦＣ（Request For Comments）７９３に記載の伝送制御プロトコル（TCP）は、通信ネットワーク全体にわたる情報の流れを制御する周知の伝送プロトコルである。伝送プロトコルは、フロー制御、エラー制御、及び、データ・パケットの時間制御配信等のパラメータを保守することによって通信ネットワークの安定化を図るものである。この種の制御の管理には、パケットのヘッダーに含まれる命令や、通信ネットワークを介して装置間で送信されるパケットから別に供給される命令が使用される。この制御情報は、データ・パケットが順序正しく送信される、「同期」した通信ネットワークに非常に効果的である。

【０００６】
通信ネットワークを介してマルチメディアデータを伝送する際に、そのマルチメディアデータの製作者が望むことは、送信した商品が、その送信データに対して正当なアクセス権限のあるユーザにのみ受信され、使用されることである。多くの場合、マルチメディアデータは、そのデータに対して正当なアクセス権限を持たない不正使用者（pirate）によってハイジャックされ、使用される。マルチメディアデータの不正な使用を最小限にとどめるために、製作者は、不正ユーザによるデータへのアクセスやデータの使用が困難になるように、アクセス制限手段を用いてデータを保護している。

【０００７】
アクセス制限の一般的な方法としては、データにアクセスする際にパスワードの使用を要求する方法、データ・スクランブル、及び、データ暗号化などがある。アクセス制限システムが頻繁に使用されるにつれ、不正使用者は、保護されたデータへの不正アクセスを目的としてこうしたシステムに侵入することに精通するようになっている。これは、不正使用者がデータ保護に使用されている手法を事前に知っている場合に生じる問題である。

【発明の開示】
【発明が解決しようとする課題】
【０００８】
こうした状況にも関わらず、従来は、マルチメディアデータの製作者にとって、データの保護に使用されている特定の方法を開示することなく、マルチメディアデータを容易に保護できる方法がなかった。例えば、１９９８年１２月１０日に公開された、CM COMMUNITY MEDIA GMBH&CO, ET AL.のDE-U-29814544には、ビデオ・ストリームを鍵を使用して暗号化する処理が記載されている。鍵自体も暗号化されて衛星経由でユーザに送信される。ユーザは、暗号化された鍵を受信して暗号化されたデータを復号化する。

【課題を解決するための手段】
【０００９】
本発明の目的は、マルチメディアデータを保護する処理を提供することにある。この処理は、
マルチメディアデータを暗号化マルチメディアデータに符号化するステップと、
前記暗号化マルチメディアデータに、ストリーム・キー・データ及び復号化情報を多重化するステップとを有し、
前記多重化ステップは、ストリーム・キー・データ及び機器識別番号に基づいて実行されることを特徴とする。

【００１０】
本発明の別の側面によれば、マルチメディアデータを多重化データ・ストリームに多重化する装置が提供される。

【００１１】
本発明のさらに別の側面によれば、データ・ストリームに含まれるストリーム・キー・データを考慮して、多重化データ・ストリームを逆多重化する方法が提供される。

【００１２】
本発明のさらに別の側面によれば、データ・ストリームに含まれるストリーム・キー・

データを考慮して、多重化データ・ストリームを逆多重化する装置が提供される。

【００１３】

以下で、本発明の様々な特徴や利点、及び、その好適な実施例を図面と共に説明するが、この図面は本発明を説明するためのものであって、本発明の範囲を制限するものではない。

【発明を実施するための最良の形態】

【００１４】

ここでは、マルチメディアデータとは、テキスト、画像、ビデオ及び音声等のデータのあらゆる組み合わせを指すものとする。ストリーミング・メディアは、音声データ、ビデオデータ、マルチメディアデータ、テキストデータ、インタラクティブ・データ等、インターネットや他の通信データ・ネットワーク経由でユーザに配信されるデータを含み、ストリーミング・メディアは、そのメディアのマルチメディアデータが全て受信される前に再生可能である。

【００１５】

実施例で、マルチメディアデータを映画、テレビ番組、放送番組等としてデータ・ネットワーク経由でユーザに配信するビデオ・オンデマンド・サーバーを例にとって説明する。しかし、本発明はこのような実施例に限定されるものではなく、第三者による不正アクセスから保護する必要のあるマルチメディアデータをユーザに伝送するあらゆるシステムに適用可能である。

【００１６】

図１は、本発明の一実施形態に係る、メディア・オブジェクトのマルチメディアデータを保護された多重化データ・ストリームに変換する符号器のブロック図である。本実施形態では、マルチメディアデータは、サービス・プロバイダーから加入者へのデータ送信に備えて処理され、第三者による当該データの使用を防止するための保護がかけられる。データ受信者は、一意の識別番号（ＵＩＤ）を有する復号器を操作できることが望ましい。この識別番号は、データ受信者を識別するための指標として用いられる。識別番号を復号器に割り当てる際には、データ・ネットワークへのＩＥＥＥ８０２．３準拠の接続に使用されるネットワーク・インターフェース・カード（NIC：Network Interface Card）が用いる識別番号、復号処理に使用されるMAC（Media Access Control）アドレス、又は、サービス・プロバイダーがデータ受信者に割り当てるＵＩＤなどを用いても良い。サービス・プロバイダーは、ＵＩＤに対応するデータ受信者のアクセス権限を識別し、確認するのにＵＩＤを用いることもできる。

【００１７】

符号化システム１００が備えるマルチメディアデータ・サーバー１１０は、マルチメディアデータを格納し、送信する。マルチメディアデータは、データ受信者に送信されることが望ましい。マルチメディアデータとは、メディア・オブジェクト・コンテンツのオーディオ／ビデオデータであり、例えば、映画、テレビ番組、及び、ラジオ番組などである。マルチメディアデータ・サーバー１１０は、ＨＤＤ（ハードディスク・ドライブ）、リムーバブル・ハードディスク、ＣＤ（コンパクト・ディスク）、ＤＶＤ、あるいは、これらの組み合わせ、又は、符号化処理のためにマルチメディアデータの格納、配信に用いられるいかなる装置であっても良い。本発明の他の実施例によれば、マルチメディアデータ・サーバー１１０は、最終的に符号化されて送信されるリアルタイム生成されるマルチメディアデータの配信元であっても良い。

【００１８】

マルチメディアデータ・サーバー１１０に接続される符号器１２０は、マルチメディアデータを処理に適したフォーマットに符号化する。例えば、符号器１２０が受信したマルチメディアデータは、ＭＰＥＧ－２に準拠した形式にフォーマットされる。符号器１２０は、マルチメディアデータを、ＭＰＥＧ－２、ＭＰＥＧ－４、ＪＶＴ（Joint Video Team Compression）などの様々なマルチメディア形式へ変換するために用いられており、このような符号化処理に符号器１２０を用いることは公知である。

【００１９】
また、符号器１２０は、マルチメディアデータを、第三者によるアクセスがより困難な形式に変換して保護するのに用いられる。本発明の一実施形態によれば、符号器１２０はＭＰＥＧ－２のデータを暗号化フォーマットに符号化するために符号化テーブルを使用する。このため、第三者はデータがどのような方法で暗号化されたのかを知ることができず、暗号化されたマルチメディア形式への第三者による直接的なアクセスが制限される。あるいは、符号器１２０は、DES（Data Encryption Standard）、ＩＤＥＡ（International Data Encryption Algorithm）、ＳＡＦＥＲ（Secure and Fast Encryption Routine）、その他、マルチメディアデータを暗号化するための公知の方法で暗号化処理を行っても良い。この暗号化処理によって、暗号化マルチメディアデータが生成される。

【００２０】
次に、パターン・マルチプレクサ１４０は、符号器１２０から暗号化マルチメディアデータを受け取る。パターン・マルチプレクサ１４０は、符号器１２０から受け取った暗号化マルチメディアデータを他の種類のデータと多重化することで、データ保護の第二ステップを実行する。このような多重化処理を、多重化パターン（MUXP）処理と称する。

【００２１】
ＭＵＸＰ処理は、サービス・プロバイダーが、ストリーム・キーとして知られる値や条件をランダムに選択することによって開始される。これは、ストリーム・キー生成部１１５により行われる。また、パターン・マルチプレクサ１４０は、ユーザ又はユーザの装置に対応するＵＩＤを、機器識別番号１３０から取得する。ストリーム・キー及びＵＩＤは、符号器１２０からのデータの多重化方法を決定するためにパターン・マルチプレクサ１４０によって用いられ、ストリーム・キー及び復号化情報は、符号器１２０からのデータの復号化に用いられる。

【００２２】
パターン・マルチプレクサ１４０によるストリーム・キー、復号化情報、暗号化マルチメディアデータの多重化は、多重化パターン処理（ＭＵＸＰ）において、ストリーム・キーとＵＩＤをシード値として使用し、演算式を参照して行われる。あるいは、データ・ストリーム中に少なくとも三つの異なるデータ・タイプの位置を割り当てる他の方法を用いても良い。例えば、パターン・マルチプレクサ１４０が使用する多重化パターン（ＭＵＸＰ）は、ストリーム・キー及びＵＩＤをシード値として用いる統計的多重化処理であるが、ＭＵＸＰを決定するのに他の式や処理を用いても良い。なお、ＵＩＤ又はストリーム・キーの値が変化したときには、ＭＵＸＰも変わることに留意すべきである。

【００２３】
図2は、ＭＵＸＰ制御の多重化処理の結果を示す。図２には、保護多重化データ・ストリームの内容が示されている。保護多重化データ・ストリーム２００（以後、データ・ストリーム２００と称する）は、データ・パケットの形で送信されるのが望ましい。ただし、データ・ストリーム２００は、どのようなデータ形式であっても良い。データ・ストリーム２００は、少なくとも三つの異なる種類のデータから構成される。つまり、ストリーム・キー２１０、暗号化マルチメディアデータ２２０、及び、復号化情報２３０である。ストリーム・キー２１０は、データ・ストリーム２００の多重化／逆多重化に用いられるストリーム・キー・データである。ストリーム・キー２１０は、データ・ストリーム２００中の常に同じパケット位置を占めることが望ましい。この位置は、所定の周期で繰り返されるものであっても良い。暗号化マルチメディアデータ２２０は、符号器１２０から受け取ったマルチメディアデータである。

【００２４】
復号化情報２３０は、暗号化マルチメディアデータ２２０の復号化に用いられるデータであり、データ・ストリーム２００の一部である。復号化情報２３０は、暗号化マルチメディアデータ２２０を生成するのに実行される暗号化処理とは逆の処理を実行する際に用いられるのが望ましい。復号化情報２３０の内容は、暗号情報、鍵、又は、保護データを復号化するのに用いられる他のデータ等である。

【００２５】
多重化処理の後、データ・ストリーム２００は、伝送符号化器１５０によって伝送に適した形式にフォーマットされる。伝送に適した形式とは、例えば、ＴＣＰ／ＩＰ準拠のネットワークで用いられるデータ・パケット等である。フォーマットされたデータは、復号器における復号化処理に用いるために、伝送符号化器１５０によってデータ・ネットワーク１６０を介して送信される。
【００２６】
本発明の他の実施例によれば、データ・ストリーム２００を生成するためのデータを配信する際に用いられるＭＵＸＰは、復号化されたマルチメディアデータの再生又は記憶への適用を考慮して選択される。例えば、マルチメディアデータをストリーミングにより再生することが意図されている場合、ＭＵＸＰは、大部分の復号化情報がデータ・ストリーム２００の冒頭部に配置され、マルチメディアデータはデータ・ストリーム２００の後半に多重化されたものになると考えられる。このため、マルチメディアデータをバッファリングしながら行う復号器における処理は、マルチメディアデータをストリーミングする際に上記のような配置を採用するとより効率的となる。一方、記憶処理については、復号化データは、ＭＵＸＰに従って、データ・ストリーム２００の全体に渡って均一に分散される。これは、データは、リアルタイム処理で直接再生されている訳ではないからである。
【００２７】
図３は、本発明の一実施形態に係る、マルチメディアデータを保護多重化データ・ストリームに符号化する方法を説明するフローチャートである。ステップＳ３１０で、音声／ビデオのメディア・オブジェクトのマルチメディアデータは、符号化される。ここで、マルチメディアデータは、本発明の原理に従って、符号器１２０（図１参照）で暗号化マルチメディアデータに暗号化されることが望ましい。上述したように、どのような符号化処理及び暗号化処理を用いても良い。
【００２８】
ステップＳ３２０で、暗号化マルチメディアデータは、復号化情報及びストリーム・キー・データと共にアクセス制限付きの多重化データ・ストリームに多重化される。上述したように、パターン・マルチプレクサ１４０は、（ストリーム・キー生成部１１５からの）ストリーム・キーと機器識別番号１３０からのＵＩＤに応じて決定されるＭＵＸＰに従って、三種類のデータ・タイプを保護多重化データ・ストリーム２００（図２参照）に多重化する。多重化データ・ストリーム中の各データ・タイプの位置は、ストリーム・キー・データ又はＵＩＤの変化により変化する。
【００２９】
ステップＳ３３０で、データ・ストリーム２００は、伝送符号化器１５０によって、データ・ネットワーク１６０経由での伝送に適した形式にフォーマットされる。データ・ストリーム２００は、ＵＩＤに対応する復号器に送信されることが望ましい。
【００３０】
図4は、本発明の一実施形態に係る、アクセス制限付きの多重化データ・ストリームを逆多重化する方法を説明するフローチャートである。好適な実施形態によれば、データ・ストリーム２００は、ストリーム・キー２１０、暗号化マルチメディアデータ２２０、及び、復号化情報２３０といったデータ・タイプに逆多重化される。そして、これらのデータ・タイプは、暗号化マルチメディアデータ２２０を処理して、再生や記憶に適したフォーマットの復号化マルチメディアデータを得るために用いられる。
【００３１】
図４のステップを、図５に示す復号化システム５００を参照しながら説明する。図５は、本発明の一実施形態に係る、多重化データ・ストリームをマルチメディアデータに逆多重化する復号器のブロック図である。
【００３２】
逆多重化方法４００は、ステップＳ４１０における、データ・ネットワーク５６０からの多重化データ・ストリームの受信で始まる。ステップＳ４１０では、伝送復号化器５５

０等のデータ・ネットワークからデータを受信可能な装置を用いることが望ましいが、データを受信可能な装置なら、どのような装置を用いても良い。伝送復号器５５０は、受信したデータ・ストリームを、パターン・デマルチプレクサ５４０で処理できるようにフォーマットする。

【００３３】

受信した多重化データ・ストリームは、ステップＳ４２０で（パターン・マルチプレクサ１４０とは逆の処理を行う）デマルチプレクサ５４０によって逆多重化される。この逆多重化処理においては、多重化データ・ストリームの一部として送信されたストリーム・キー情報が使用される。一般に、ストリーム・キー情報は、多重化データ・ストリーム中の所定の位置に配置されているため、パターン・デマルチプレクサ５４０は、受信データ・ストリームのどこからストリーム・キー情報を抽出すべきかを把握している。また、パターン・デマルチプレクサ５４０は、自身又は接続されている復号器に対応するＵＩＤを使用して逆多重化処理を行う。

【００３４】

逆多重化処理とは、多重化データ・ストリームを生成するために実行される処理と逆の処理である。具体的には、パターン・デマルチプレクサ５４０は、ストリーム・キー及びＵＩＤを用いる逆ＭＵＸＰ処理を使用して、多重化データ・ストリームを復号化情報及び暗号化マルチメディアデータに再構成する。

【００３５】

ステップＳ４３０で、暗号化マルチメディアデータは、再生又は記憶に適したフォーマットに処理される。このステップは、復号器５２０等の、（符号化及び暗号化を行う符号器１２０とは逆の処理を行う）復号化装置を使用して実行される。復号器５２０は、多重化データ・ストリームから逆多重化された復号化情報を用いて、暗号化マルチメディア情報を暗号化マルチメディアデータに復号化する。そして、このデータは、テレビセット、コンピューター、ＣＤプレーヤーその他のマルチメディア装置（再生装置）５１０での再生又は記憶に適したフォーマットに復号化される。このデータは、マルチメディアデータ・サーバー１１０（図１参照）からのデータに類似したマルチメディアデータであると理想的である。

【００３６】

本発明は、コンピューターにより実行される処理や、そのような処理を実行する装置に適用しても良い。また、本発明は、フレキシブル・ディスク、ＲＯＭ、ＣＤ－ＲＯＭ、ハードディスク・ドライブ、高密度ディスク、又は、他のいかなるコンピューター読取可能な記憶媒体等の有形の媒体に記憶されたコンピューター・プログラム・コードに適用しても良い。この場合、コンピューター・プログラム・コードをコンピューターが読み取って実行すると、このコンピューターが本発明を実行する装置となる。さらに、本発明は、コンピューター・プログラム・コードに適用しても良い。この場合、コンピューター・プログラム・コードは、記憶媒体に記憶されていても良いし、コンピューターに読み込まれ、実行されても良い。また、電線やケーブル、光ファイバー、アンテナ（電磁放射線）等、任意の送信媒体を用いて送信され得る。コンピューター・プログラム・コードがコンピューターに読み込まれて実行されると、そのコンピューターが本発明を実行する装置となる。汎用プロセッサに導入された場合には、当該プロセッサは、コンピューター・プログラム・コードのセグメントによって、特定の論理回路を構成するように設定される。

【図面の簡単な説明】

【００３７】

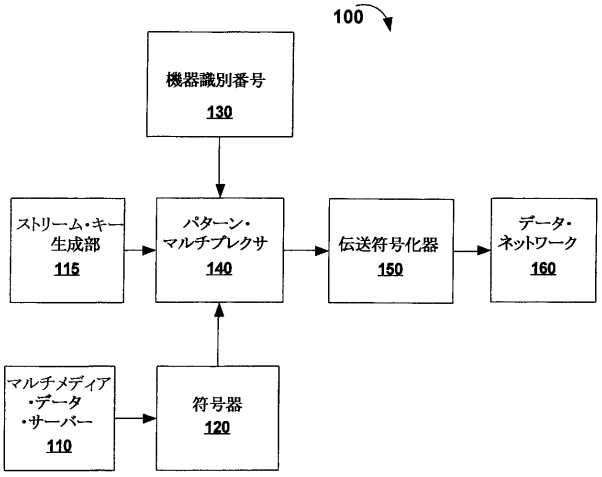
【図１】本発明の一実施例による、マルチメディアデータを保護多重化データ・ストリームに変換する符号器のブロック図である。

【図２】本発明の一実施例による、保護多重化データ・ストリームのコンテンツを図示した概略図である。

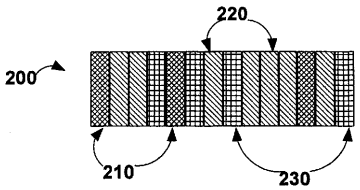
【図３】本発明の一実施例による、マルチメディアデータを保護多重化データ・ストリームに符号化する方法を説明するためのフローチャートである。

【図４】本発明の一実施例による、保護多重化データ・ストリームを逆多重化する方法を説明するためのフローチャートである。
【図５】本発明の一実施例による、多重化データ・ストリームをマルチメディアデータに逆多重化する復号器のブロック図である。
【符号の説明】
【００３８】
１１０　マルチメディアデータ・サーバー
１１５　ストリーム・キー生成部
１２０　符号器
１３０　機器識別番号
１４０　パターン・マルチプレクサ
１５０　伝送符号化器
１６０　データ・ネットワーク
２００　保護多重化データ・ストリーム
２１０　データ・ストリーム
２２０　暗号化マルチメディアデータ
２３０　復号化情報
５１０　再生装置
５２０　復号器
５４０　パターン・デマルチプレクサ
５５０　伝送復号化器
５６０　データ・ネットワーク

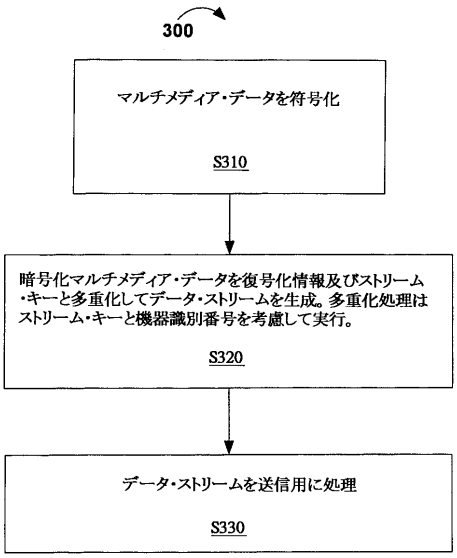
【図１】



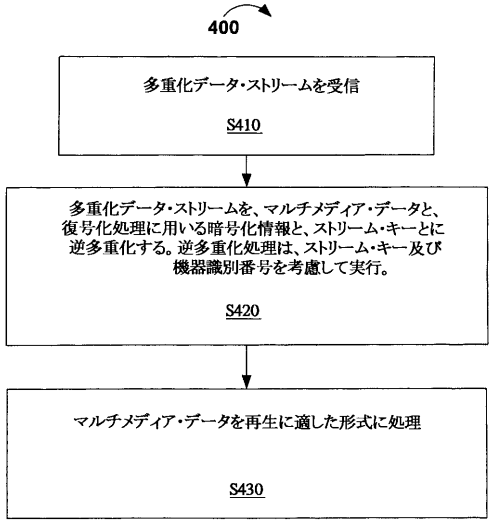
【図２】



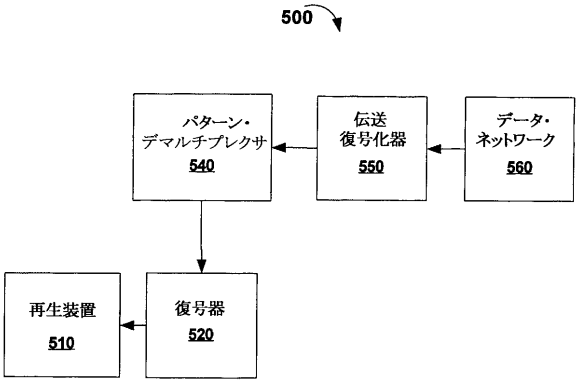
【図３】



【図４】


400
多重化データ・ストリームを受信
S410
多重化データ・ストリームを、マルチメディア・データと、復号化処理に用いる暗号化情報と、ストリーム・キーとに逆多重化する。逆多重化処理は、ストリーム・キー及び機器識別番号を考慮して実行。
S420
マルチメディア・データを再生に適した形式に処理
S430

【図５】


500
パターン・デマルチプレクサ
540
伝送復号化器
550
データ・ネットワーク
560
再生装置
510
復号器
520

フロントページの続き

(72)発明者　ディルク　アードルフ
ドイツ連邦共和国，３０９５２　ローネンベルク，ヴァルブリンク　２
(72)発明者　アンドレイ　シェフツォフ
ドイツ連邦共和国，３０１６３　ハノーヴァー，タラフェラシュトラーセ　１４
(72)発明者　マルコ　ヴィンター
ドイツ連邦共和国，３０１７３　ハノーヴァー，ベーマーシュトラーセ　１７

Ｆターム(参考) 5C059 KK43 MA00 RB01 RC32 RC35 SS06 UA02 UA05
5C064 CA18 CB01 CC04
5J104 EA16 JA03 PA07