

(19) 日本国特許庁 (JP)

(12) 特 許 公 報 (B2)

(11) 特許番号

特許第5086501号
(P5086501)

(45) 発行日 平成24年11月28日 (2012.11.28)

(24) 登録日 平成24年9月14日 (2012.9.14)

(51) Int.Cl.		F I
HO 4 N	5/91	(2006.01)
HO 4 N	5/92	(2006.01)
HO 4 N	5/76	(2006.01)
G 1 1 B	20/10	(2006.01)

HO 4 N	5/91	Z
HO 4 N	5/92	H
HO 4 N	5/76	A
G 1 1 B	20/10	3 O 1 Z

請求項の数 10 (全 9 頁)

(21) 出願番号	特願2000-354715 (P2000-354715)
(22) 出願日	平成12年11月21日 (2000.11.21)
(65) 公開番号	特開2001-189914 (P2001-189914A)
(43) 公開日	平成13年7月10日 (2001.7.10)
審査請求日	平成19年11月12日 (2007.11.12)
(31) 優先権主張番号	9914647
(32) 優先日	平成11年11月22日 (1999.11.22)
(33) 優先権主張国	フランス (FR)

(73) 特許権者	391000771
	トムソン マルチメディア
	フランス国 ブローニュ＝ビランクル ケ
	ア. ル ガロ 46
	46, Quai A. Le Gallo,
	Boulogne-Billancourt,
	France
(74) 代理人	100070150
	弁理士 伊東 忠彦
(72) 発明者	フィリップ ルイエンデッケル
	フランス国, 35410 シャトー＝ジロン
	, リュ・ポール・デュプレシス 10

審査官 梅本 章子

最終頁に続く

(54) 【発明の名称】 スランブルされたMPEGストリームを記録する方法

(57) 【特許請求の範囲】

【請求項 1】

記録装置が、スランブル解除する鍵とスランブルされたデータパケットとを含むMPEGビデオのデータストリームを記録媒体に記録する方法であって、

上記データストリームからスランブル解除する鍵を抽出し、

上記スランブル解除する鍵を用いて上記スランブルされたデータパケットをスランブル解除し、

記録されたデータストリームを再生するときトリックモードの動作のために必要とされる、画像の種類、画像のサイズ、画像開始を決めるポインタのうち、少なくとも1つ以上である追加的なデータを上記スランブル解除されたデータパケットから抽出し、

上記記録媒体上に、上記スランブルされたデータパケット及びスランブル解除された追加的なデータを記録する方法。

【請求項 2】

上記データストリームは、マルチプログラムMPEGデータストリームのトランスポートストリームヘッダを記録されるべき選択された1つ以上のプログラムの関数としてフィルタリングすることによって得られる請求項1記載の方法。

【請求項 3】

上記記録媒体は、ハードディスク又は記録可能なDVDである請求項1又は2記載の方法。

【請求項 4】

10

20

上記ポインタに関連する追加的なデータは、スクランブルされたデータストリームを暗号化するのに用いた鍵が存在するデータパケットのポインタ及び上記鍵が適用されるパケットのポインタである請求項1乃至3いずれか一項に記載の方法。

【請求項5】

上記鍵が適用されるデータパケットのポインタは、上記鍵が適用されるデータストリーム部分を決めるポインタである請求項4記載の方法。

【請求項6】

上記鍵が適用されるデータストリーム部分を指すポインタは、スクランブルされたMPEGデータストリームの「transport_scrambling_control」フィールドの値の変化に関する情報から得られる請求項5記載の方法。

10

【請求項7】

上記鍵が適用されるデータパケットのポインタは、鍵の対の2つの鍵が夫々連続して適用されるデータストリーム部分を決めるポインタである請求項4記載の方法。

【請求項8】

上記鍵は、上記ポインタに関連する追加的なデータと共に記録されるよう、上記データストリームから抽出される請求項4記載の方法。

【請求項9】

上記追加的なデータは、解読された鍵を有する請求項4記載の方法。

【請求項10】

上記追加的なデータは、解読された鍵が他の暗号化装置によって再び暗号化された鍵を有する請求項4記載の方法。

20

【発明の詳細な説明】

【0001】

【発明の属する技術分野】

本発明は、例えばハードディスクといった記録媒体上に、例えばMPEG型ストリームといったスクランブルされたオーディオビデオデジタルデータストリームを記録する方法に関する。

【0002】

【従来の技術】

スクランブルされた形式でのデータの記憶は、現在急速に開発されている。例えば、圧縮されスクランブルされた形式で伝送されるオーディオビデオデジタルデータは、一般的にはデータへのアクセスを制御するためにこの形式で記録される。従って、データは対応する画像が見られるときにのみスクランブル解除される。他の例は、1394デジタルバスに関連するものであり、このデジタルバスを利用した枠組みでの解法は、デジタルデータをスクランブルされた形式で伝送し、従ってスクランブルされた形式で記憶することである。

30

【0003】

【発明が解決しようとする課題】

このスクランブルされた形式でデジタルビデオデータストリームを記録することについての問題は、読出しの特定のモード又はMPEG標準の用語では「トリックモード」と称される特殊なモードを利用することに関連し、「トリックモード」とは、早送り、巻き戻し、スローモーション、ファストモーション、フリーズフレームを示す。これらの機能は、実際に記録されたデータに対するアクセス及び高速な復号化、即ちスクランブルモードでの記録に適合させることが困難な状態を必要とする。

40

【0004】

本発明は、上述の欠点を軽減することを目的とする。

【0005】

【課題を解決するための手段】

本発明は、スクランブル解除する鍵とスクランブルされたデータパケットとを含むMPEGビデオのデータストリームを、記録装置が記録媒体に記録する方法であって、上記デ

50

ータストリームからスクランブル解除する鍵を抽出し、上記スクランブル解除する鍵を用いて上記スクランブルされたデータパケットをスクランブル解除し、記録されたデータストリームを再生するとき、トリックモードの動作のために必要とされる追加的なデータを上記スクランブル解除されたデータパケットから抽出し、上記記録媒体上に、上記スクランブルされたデータパケット及びスクランブル解除された追加的なデータを記録する方法を提供する。

【0006】

追加的なデータは、画像の種類、画像のサイズ、画像開始を決めるポイントのうち、少なくとも1つ以上である。

【0007】

本発明は、スクランブルされたデジタルビデオストリームのデータと、特殊モード即ち「トリックモード」の動作のためのストリームのビデオデータに関する追加的なデータとを含むことを特徴とする記録媒体を提供する。

【0008】

参考例は、ビデオデータパケットが、画像の開始を含むパケットを除き、スクランブルされることを特徴とするMPEGオーディオビデオデジタルデータストリームを提供する。

【0009】

参考例はまた、「トリックモード」の少なくとも1つの機能によって必要とされる情報の抽出を可能とする追加的なデータを含むこと、及び、追加的なデータが上記ストリームの「適合フィールド」中で搬送されることを特徴とするMPEGオーディオビデオデジタルデータストリームを提供する。

【0010】

参考例はまた、MPEG標準によってデータを符号化して、データパケットの形式でトランスポートストリームを搬送すること、及び画像の開始を含むデータパケットをスクランブルし、他のパケットをスクランブルしないことを特徴とする、デジタルビデオデータストリームを符号化する方法を提供する。

【0011】

参考例はまた、スクランブルされたデジタルビデオストリームを記録媒体上に記録する方法であって、ストリームがスクランブルされたストリームを暗号化するための鍵に関連する追加的なデータを抽出するようスクランブル解除され、このデータもまた記録媒体上に記録されることを特徴とする方法を提供する。

【0012】

1つの変形例によれば、方法は、鍵に関連する追加的なデータが、鍵が存在するパケットのポイント及び上記鍵が適用されるパケットのポイントであることを特徴とする。

【0013】

他の変形例によれば、方法は、鍵に関連する追加的なデータが、解読された鍵であることを特徴とする。

【0014】

本発明はまた、スクランブルされたデジタルビデオストリームのデータと、暗号化鍵に関連する追加的なデータとを含むことを特徴とする記録媒体を提供する。

【0015】

【発明の実施の形態】

本発明の他の特徴及び利点は、例として与えられ添付の図面を参照する以下の説明より明らかとなろう。スクランブルされたオーディオビデオデータストリームは、例えばMPEG標準で定義されるようにトランスポートストリーム(TS)である。ストリーム又はパケットのスクランブリングは、有用なデータ(又は「ペイロード」)に関連し、パケットヘッダに関連しない。従って、このストリームはスクランブルされた形式で記録装置によって受信される。

【0016】

この装置によって実施される方法は、図1のフローチャートに概略的に示される。第1のステップ1は、単一のプログラムを記録しようとする場合は、受信されたストリームをプログラムの選択に基づいてフィルタリングする段階である。このフィルタリング段階は、PID（パケットヘッダ識別子）に対して行なわれる。

【0017】

選択されたプログラムに対応する得られた部分ストリームは、ステップ2、ステップ3、ステップ6において並列に処理される。部分ストリームは、記憶ユニット又は記録媒体へ直接送信される（ステップ6）。部分ストリームはまた、パケットのスクランブル解除を可能とするデータ（部分）を抽出する鍵抽出回路（ステップ2）へ送信される。ステップ2では、おそらく暗号化されている鍵をこの場合はそれらを解読すると同時に抽出する。

10

【0018】

ステップ3では、部分ストリームから、デスクランブル回路によってスクランブル解除するためのビデオ情報を含むパケットを抽出する。このスクランブル解除のために必要とされる鍵は、ステップ2から生ずる。

【0019】

このスクランブル解除は、明らかに、ビデオデータを見るためのフェーズとは区別されねばならないデータ記録フェーズ中に、条件付きアクセス制御システムにより受信されるストリームのスクランブル解除が一時的に可能とされることを必要とし、即ち、条件付きアクセス情報が使用可能であることが必要とされる。この条件付きアクセス情報により、ステップ2において抽出された鍵に基づいてビデオデータの解読が可能とされ、また、適切であればステップ2においてキーを解読することが可能とされる。

20

【0020】

次のステップ4において、これらのスクランブル解除されたビデオデータから、「トリックモード」の動作のために必要とされる補助データ又は追加的なデータと称される情報が抽出される。この情報は、画像のサイズ、画像開始を決めるポインタ、画像の種類等である。

【0021】

ステップ5において、これらのデータは部分ストリームに関連する記録されスクランブルされたデータからなるオーディオビデオファイルを添付ファイルを構成するよう編成される。次のステップ6において、この添付ファイルが媒体上に記録される。ステップ6ではまた、一連のファイルが構成され、「トリックモード」に関連するデータはスクランブルされたデータの記録に続いて記録される。

30

【0022】

ステップ6において、ステップ1から生じた部分ストリームに対応するスクランブルされたデータもまた記録される。このように、オーディオビデオファイルのデータ及び付随するファイルのデータは、記録媒体上に記憶される。

【0023】

記録されたファイルの補助又は追加的なデータと記録されたスクランブルされたデータとの間には時間の対応性がなくてはならない。記録された追加的なデータは、例えばオーディオビデオファイルの対応するデータに対してインデックス付けされる。

40

【0024】

もちろん、本発明の範囲を逸脱することなく、分解（デマルチプレックス）されたストリーム、即ち部分ストリームだけでなく、MPEGストリーム全体を記録することがわかる。また、あるプログラムを選択し、選択されたプログラムのみを記録することが可能である。また、同一のプログラムにおいて、例えば幾つかの視角に対応する幾つかのビデオストリーム（PID）が存在することがある。すると、方法は記録された各ビデオストリームに対して個々に適用される。各ビデオストリームに対して添付ファイルがあってもよい。

【0025】

望ましくは、デスクランブル回路は、スクランブル解除されたオーディオビデオストリー

50

ムに対するアクセスを防止するよう、トリックモードに関するデータの抽出を行なう回路と一体化される。

【0026】

本発明の変形は、「トリックモード」に関する情報又は追加的なデータをスクランブルされていない形式で含み、他のデータをスクランブルされた形式で含むMPEGストリームを形成するものである。

【0027】

例えば、スクランブルされないのは、「トリックモード」のために有用な情報を含むパケットのみである。この情報は、ストリームをスクランブル解除することなく、ハンドラーによって容易に認識され抽出されうる。これは例えば、画像開始を含み、画像タイプ等を提供するパケットを含む。このように、ステップ2及び3は、鍵を抽出し、追加的なデータがもはや必要とされないよう追加的なデータをスクランブル解除することからなり、画像開始、画像の種類等といった追加的なデータはデータストリームのスクランブルされていないパケットから得られる。

10

【0028】

他の例では、トリックモードに有用なデータを搬送するために、例えばトランスポートストリーム中のビデオパケットの「適合フィールド」に属し、プライベートデータをグループ化する1つ以上のフィールドが使用される。ステップ4において、「適合フィールド」から「トリックモード」情報が直接抽出される。

20

【0029】

鍵の抽出及びビデオデータのスクランブル解除に対応するステップ2及び3は、また、もはや有用でない。実際、トリックモードに有用な情報を抽出するためにデータストリームをスクランブル解除することはもはや必要なく、従って記録媒体上にデータを記録するときにスクランブル解除のためのアクセス権を得る。

【0030】

しかしながら、これらの変形は、データストリーム符号化チェーンのレベルにおける介入を必要とし、従って放送者のレベルにおける制約を生じさせるが、一時的なスクランブル解除に関するアクセス制御及び安全性の問題を回避することを可能とする。

【0031】

「トリックモード」を使用することは、スクランブル解除を行なうことを可能とするために、添付ファイル中に記憶される有用な情報のほかに、各パケットのために使用される鍵に関する情報を必要とする。

30

【0032】

これは、画像シーケンスの任意の点を評価するときに、トリックモード中に見られる画像をスクランブル解除することは、対応する解読鍵を読むこと、できれば解読することを必要とするためである。鍵は、ストリーム中で、およそ100ms秒毎に、画像に対して非同期化され、リアルタイムでスクランブル解除を実行することが可能であるよう十分に前もって使用可能である。解読された鍵は、実際に対応するスクランブルされたデータが読まれたときに使用可能でなくてはならない。

【0033】

これに対して、使用可能性は、従来の読み出しモードでは問題とならず、「トリックモード」を利用しているときに生ずる。これは、この場合、鍵に関連し、ストリーム中で前もって提供されるデータは、トリックモードに有用であり従って前もって利用可能でない画像に対する一時的なアクセスを考慮して読み出されないためである。

40

【0034】

1つの解法は、解読されるべきデータを読み出す前に解読鍵を抽出し復号化することが可能であるよう、データストリームをアクセスの点に対して例えば0.5秒だけ「後ろに置く」ことからなる。読出しポインタ又は記録媒体の読出しヘッドは、復号化しようとし、添付ファイルから抽出されるポインタによってその位置が分かる画像へのアクセスの点の数百ミリ秒前に配置される。この解法は、応答に遅延を生じさせ、有用でないデータを読

50

み出すことを必要とし、誤りを生じさせる可能性がある。

【0035】

ここで提案され、独立に、又は、上記の方法と組み合わせて使用されうる方法は、「トリックモード」中のデータのスクランブル解除を容易とするために鍵に対して特別な操作を行なうことからなる。

【0036】

図2は、実施される方法の様々なステップを表わす図である。ステップ1、3、4、5は、上述のステップと同様であり、同じ数字が付されている。新しいステップ7がステップ2の代わりに用いられ、以下に示されるように採用される解法に依存してステップ2のステップを補足する操作を行なう。このステップ7の後には、ステップ7から生ずる情報が記憶される1つ以上のファイルを形成する新しいステップ8が続く。最後に、これらのファイルからのデータは、ステップ6において記憶されるよう記録媒体へ送信される。

10

【0037】

第1の解法は、暗号鍵を含むストリーム中のパケットの位置にタグを付すこと、これらのパケットに対応するポインタを記憶すること、及び鍵が適用されるストリームの部分を示すポインタを記憶することからなる。従って、ビデオデータをスクランブル解除するためのステップ3において送信される鍵の抽出を補足するステップ7は、ポインタ又は印を抽出し、添付ファイルに記憶され、次にステップ6において記録媒体上に記録されるよう、ステップ8においてそれらを送信する。

【0038】

20

このように、特殊モードの動作中、添付ファイルは読み出されるべきストリームの部分に対して適用される鍵を含むパケットの位置を与える。これらのパケットが読み出され、読み出されるストリームの位置を解読するために鍵が抽出される。

【0039】

第2の解法は、ステップ7において抽出された解読された鍵を、ステップ3におけるビデオデータのスクランブル解除のためにだけでなく、ステップ8における添付ファイルへの記憶のために送信することからなる。上述の通り、方法はまた、ステップ7において暗号化された鍵を含むストリーム中のパケットの位置にタグを付し、これらのパケットに対応するポインタ、及びこれらの鍵が適用されるストリームの部分を示すポインタを記憶することからなる。これらのポインタ又は印、ステップ8において送信されるために抽出される。このステップは、鍵だけでなく、ポインタ又は印を記憶する。添付ファイルは、この場合は、暗号化鍵を含み、記録されたストリームからこれらを獲得する必要はない。

30

【0040】

第3の解法は、ステップ7において、上述の操作のほかに、鍵を解読することからなる。これらの鍵は、鍵を解読するアクセス制御装置へ送信される。解読された鍵だけでなく、ポインタ又は印もファイルに記憶され、このファイルは、その内容を鍵に関連するオーディオ及び／又はビデオデータをスクランブル解除するために使用することを考慮して、添付ファイルの形式で記録媒体上に記録される。

【0041】

もちろん、これらのデータ全ては、別々の添付ファイルに記録される。この（これらの）記録されたファイルのデータと、記録されたスクランブルされたデータとの間には常に時間の対応性があるべきである。記録されたデータは、例えばオーディオビデオファイルの対応するデータに対してインデックス付けされる。

40

【0042】

本発明は、例えばハードディスク又はDVD（デジタル・バーサタイル・ディスク）といった任意の種類の記録媒体に対して適用される。

【0043】

変形例としての実施例について以下説明する。

【0044】

ステップ7において事項される鍵の抽出に関して、第3の解法はこのステップ7において

50

、上述の操作のほかに、鍵を解読し、他のアルゴリズムによって鍵を再び暗号化することからなる。これらの鍵は、鍵を解読するアクセス制御装置へ送信される。解読された鍵は、次に他の暗号化装置へ送信される。再び暗号化された鍵は、ポインタ又は印と共にファイルに記憶され、このファイルはステップ6において、これらの鍵に関連するオーディオ及び／又はビデオデータをスクランブル解除するためにその内容を利用することを考慮に入れて、添付ファイルの形式で記録する。

【0045】

鍵が適用されるストリームの部分を示すステップ8において記録されるポインタに関して、これらのポインタの正確な値、即ち鍵に関連するストリーム部分に対応するものは、必要でない。

10

【0046】

一般的に、暗号化された鍵は対として送信され、ストリームの2つの連続する部分に適用され、更に、ストリームの2つの部分の間の正しい遷移を確実にするために、2つの解読された鍵がデマルチプレクサに対して任意の時間において利用可能である。従って、ストリームにインデックスを付す1つの方法は、鍵を対として記憶し、それらを2つの鍵の夫々が連続して適用されるストリームセグメントの開始及び終端に対応する1対のポインタと関連付けることである。これらのポインタは、例えばアクセス制御システム（「スマートカード」又はチップカード）から解読された鍵の対が受信されたときに発生されうる。

【0047】

鍵が適用されるストリーム部分の開始は、MPEGストリームでは、パケットのヘッダの「transport_scrambling_control」フィールドの値の変化によって特徴付けられる。この変化を検出することにより、鍵の対から新しい鍵の適用が決定される。従って、鍵の対を、第1の鍵が適用されるパケットを指すポインタにリンクさせ、ストリーム中でヘッダ中のこのフィールドの次の変化により新しい鍵が適用されねばならないことが示されるとすると、このポインタを記憶することで十分である。このポインタは、新しい鍵の対のスクランブル解除の時点に対応するものでありうる。

20

【0048】

鍵が適用されるストリーム部分は、ポインタ間に含まれる全てのパケットを含む必要はなく、鍵に関連するパケットはPIDによって識別されることに注意すべきである。

【0049】

もちろん、MPEGストリームのデータを使用するために、記録媒体上にスクランブルされたMPEGストリームのデータ及びトリックモードの動作に特定のデータを含む補助ファイルを記憶することを含む方法は、これらのデータを読むことと同様、媒体に対するデータの書き込みに同等によく関連する。

30

【0050】

本発明は、また、記録媒体からMPEGストリームのスクランブルされたデータ及びスクランブルされたデータ以外でありスクランブルに用いられる暗号化鍵に関連する追加的なデータを読み出すこと、並びに、読み出された追加的なデータに基づいて読み出されたMPEGストリームデータをスクランブル解除することを含む、記録媒体上に記録されたスクランブルされたMPEGストリームを復号化する方法に関連する。

40

【0051】

本発明はまた、特殊モードによって必要とされる情報を含む記録媒体からの追加的なデータを読み出し、次にこれらの追加的なデータの関数として媒体のデータを読み出すことを含む、記録媒体上に記憶されたデータに基づいて特殊モード即ち「トリックモード」機能（早送り、巻き戻し、スローモーション、ファストモーション等）を実施する方法に関連する。これらのデータは、例えば、画像の開始又は画像のタイプを指すポインタである。

【0052】

これらの2つの方法は、記憶されたデータがスクランブルされたデータであれば、組み合わせられうる。1つの例は、データパケットのレベルで行なわれるMPEG標準に準拠したスクランブル操作であり、その場合、スクランブルによっては変更されない。

50

【0053】

【発明の効果】

本発明によれば、特殊モードによって必要とされる情報はこの情報を検索又は計算するために記録されたデータをスクランブル解除する必要なしに直接利用することが可能となり、それにより操作者の命令に対する迅速な応答が可能となる。

【0054】

本発明の主な利点は、スクランブルされた形式で記録されたオーディオビデオデータを読み出すときに、トリックモードを使用することを可能とすることである。

【図面の簡単な説明】

【図1】追加的なデータのための処理の段階を定義するフローチャートである。

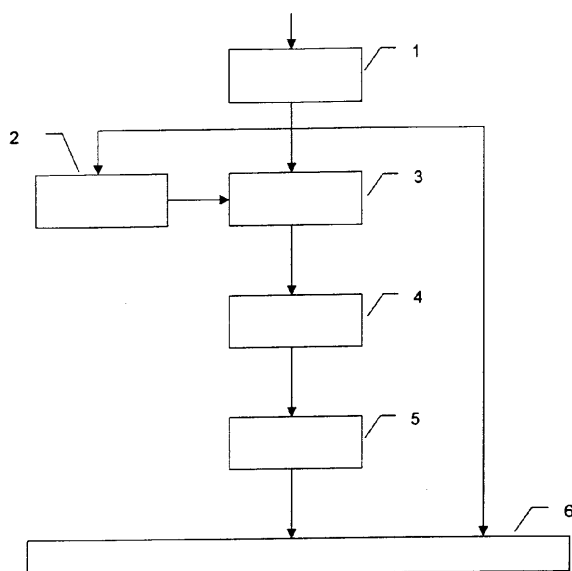
10

【図2】暗号化鍵に関するデータを記録するための方法の段階を定義するフローチャートである。

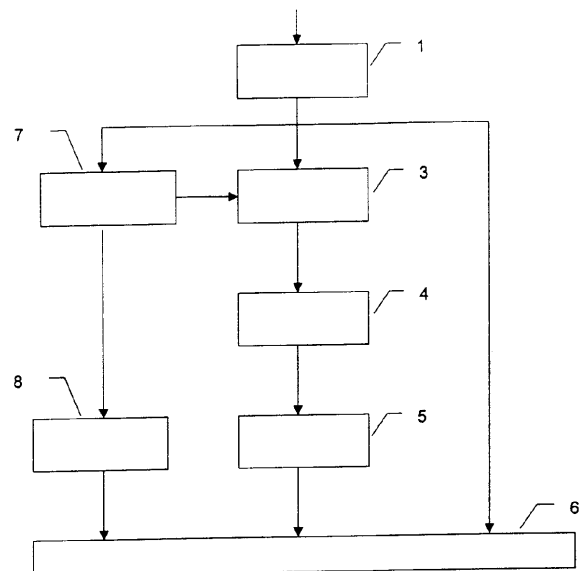
【符号の説明】

- 1 フィルタリング
- 2 鍵抽出
- 3 スクランブル解除
- 4 追加的なデータ抽出
- 5 添付ファイル構成
- 6 ファイル記憶

【図1】



【図2】



フロントページの続き

- (56)参考文献 特開平07-288769 (JP, A)
特開平08-130516 (JP, A)
特開平08-340541 (JP, A)
特開平08-273296 (JP, A)
特開平08-331508 (JP, A)
特表平09-512148 (JP, A)

- (58)調査した分野(Int.Cl., DB名)
H04N 5/76 - 5/956
H04N 7/16 - 7/173
H04N 7/24 - 7/68
G11B 20/10 - 20/12