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

特許第5797267号
(P5797267)

(45)発行日　平成27年10月21日(2015.10.21)　(24)登録日　平成27年8月28日(2015.8.28)

(51)Int.Cl.　F I
H04N 21/4367 (2011.01)　H04N 21/4367
G09C 1/00 (2006.01)　G09C 1/00　660D

請求項の数 15　(全 20 頁)

(21)出願番号　特願2013-520805 (P2013-520805)
(86)(22)出願日　平成23年7月19日 (2011.7.19)
(65)公表番号　特表2013-538486 (P2013-538486A)
(43)公表日　平成25年10月10日 (2013.10.10)
(86)国際出願番号　PCT/US2011/044518
(87)国際公開番号　WO2012/012413
(87)国際公開日　平成24年1月26日 (2012.1.26)
審査請求日　平成26年6月17日 (2014.6.17)
(31)優先権主張番号　12/842,190
(32)優先日　平成22年7月23日 (2010.7.23)
(33)優先権主張国　米国(US)

(73)特許権者　504441048
シリコン　イメージ, インコーポレイテッド
アメリカ合衆国　カリフォルニア州　９４０８５　サニーベイル　イースト　アーケス　アベニュー　１１４０
(74)代理人　100110928
弁理士　速水　進治
(74)代理人　100127236
弁理士　天城　聡
(74)代理人　100149696
弁理士　田中　俊夫

最終頁に続く

(54)【発明の名称】データストリームの部分暗号化のためのメカニズム

(57)【特許請求の範囲】
【請求項１】
オーディオコンテンツ、ビデオコンテンツ、及び制御コンテンツのグループの中から選択される第１タイプのコンテンツと、前記グループの中から選択され、前記第１タイプのコンテンツとは異なる第２タイプのコンテンツとを受信する処理と、
暗号化される前記第１タイプのコンテンツと、非暗号化状態のままとする前記第２タイプのコンテンツとを判断する処理と、
第１の保護帯域文字と前記第１タイプのコンテンツとの間に、ソースデバイスからシンクデバイスへ前記第１タイプのコンテンツを送信するために暗号化される前記第１タイプのコンテンツを示す第１フラグを挿入する処理と、
第２の保護帯域文字と前記第２タイプのコンテンツとの間に、前記ソースデバイスから前記シンクデバイスへの前記第２タイプのコンテンツの送信の間は非暗号化状態のままとする前記第２タイプのコンテンツを示す第２フラグを挿入する処理と、
前記第１タイプのコンテンツの送信のために前記第１タイプのコンテンツを暗号化する処理と、
暗号化されたバーションの前記第１タイプのコンテンツと非暗号化のバージョンの前記第２タイプのコンテンツを含むデータストリームを前記ソースデバイスから前記シンクデバイスへ送信する処理と、
が実行されることを特徴とする方法。
【請求項２】

前記第２タイプのコンテンツを暗号化せずに前記第１タイプのコンテンツを暗号化する処理は前記ソースデバイスにおいて実行されることを特徴とする請求項１に記載の方法。
【請求項３】
前記第２タイプのコンテンツへの１つ又はそれよりも多くのデバイスのアクセスを暗号解読することなく可能にする処理を更に含むことを特徴とする請求項１に記載の方法。
【請求項４】
前記第１タイプのコンテンツおよび前記第２タイプのコンテンツは、「高精細マルチメディアインタフェース」（ＨＤＭＩ（登録商標））ベースのコンテンツを含むことを特徴とする請求項１に記載の方法。
【請求項５】
前記第１タイプのコンテンツおよび前記第２タイプのコンテンツは、「モバイル高精細リンク」（ＭＨＬ）ベースのコンテンツを含むことを特徴とする請求項１に記載の方法。
【請求項６】
前記第１タイプのコンテンツは、「高帯域幅デジタルコンテンツ保護」（ＨＤＣＰ）プロトコルを用いて暗号化されることを特徴とする請求項１に記載の方法。
【請求項７】
前記第１の保護帯域文字は、暗号化データアイランド期間又は暗号化ビデオデータ期間を示す値を含み、
前記第２の保護帯域文字は、非暗号化データアイランド期間又は非暗号化ビデオデータ期間を示す別の値を含む請求項１に記載の方法。
【請求項８】
前記データストリームを中間受信デバイスにおいて受信する処理であって、該データストリームの前記第２タイプのコンテンツが、該中間受信デバイスにおいてアクセス、解析、又は修正される前記受信する処理と、
前記中間受信デバイスにおいて、前記第２タイプのコンテンツを有する前記データストリームを前記シンクデバイスに送信する処理であって、該第２タイプのコンテンツが、前記中間受信デバイスにおいて修正が実行された場合に修正された非暗号化コンテンツを有する前記送信する処理と、
が更に実行されることを特徴とする請求項１に記載の方法。
【請求項９】
前記第１タイプのコンテンツ又は前記シンクデバイスにおける該第１タイプのコンテンツの暗号解読に影響を及ぼすことなく、前記第２タイプのコンテンツのうちの１つ又はそれよりも多くの部分を前記データストリームから除去する処理を更に含むことを特徴とする請求項１に記載の方法。
【請求項１０】
オーディオコンテンツ、ビデオコンテンツ、及び制御コンテンツのグループの中から選択される第１タイプのコンテンツと、前記グループの中から選択され、前記第１タイプのコンテンツとは異なる第２タイプのコンテンツとを受信し、
暗号化される前記第１タイプのコンテンツと、非暗号化状態のままとする前記第２タイプのコンテンツとを判断し、
第１の保護帯域文字と前記第１タイプのコンテンツとの間に、前記第１タイプのコンテンツを送信するために暗号化される前記第１タイプのコンテンツを示す第１フラグを挿入し、
第２の保護帯域文字と前記第２タイプのコンテンツとの間に、前記第２タイプのコンテンツの送信の間は非暗号化状態のままとする前記第２タイプのコンテンツを示す第２フラグを挿入し、
前記第１タイプのコンテンツの送信のために前記第１タイプのコンテンツを暗号化し、
暗号化されたバージョンの前記第１タイプのコンテンツと非暗号化のバージョンの前記第２タイプのコンテンツを含むデータストリームを送信する、
ソースデバイスと、

前記データストリームを受信するシンクデバイスと、
を含むことを特徴とするシステム。
【請求項１１】
前記シンクデバイスは、暗号解読することなく前記第２タイプのコンテンツにアクセスすることを特徴とする請求項１０に記載のシステム。
【請求項１２】
前記第１の保護帯域文字は、暗号化データアイランド期間又は暗号化ビデオデータ期間を示す値を含み、
前記第２の保護帯域文字は、非暗号化データアイランド期間又は非暗号化ビデオデータ期間を示す別の値を含む請求項１０に記載のシステム。
【請求項１３】
前記ソースデバイスと前記シンクデバイスとに結合された中間受信デバイスを更に含み、
前記中間受信デバイスは、
前記データストリームを受信し、該データストリームの前記第２タイプのコンテンツが、該中間受信デバイスにおいてアクセス、解析、又は修正され、
前記第２タイプのコンテンツを有する前記データストリームを前記シンクデバイスに送信し、該第２タイプのコンテンツが、前記中間受信デバイスにおいて修正が実行された場合に修正された非暗号化コンテンツを有する、
ことを特徴とする請求項１０に記載のシステム。
【請求項１４】
オーディオコンテンツ、ビデオコンテンツ、及び制御コンテンツのグループの中から選択される第１タイプのコンテンツと、前記グループの中から選択され、前記第１タイプのコンテンツとは異なる第２タイプのコンテンツとを受信する受信機と、
暗号化される前記第１タイプのコンテンツと、非暗号化状態のままとする前記第２タイプのコンテンツとを判断し、
第１の保護帯域文字と前記第１タイプのコンテンツとの間に、前記第１タイプのコンテンツを送信するために暗号化される前記第１タイプのコンテンツを示す第１フラグを挿入し、
第２の保護帯域文字と前記第２タイプのコンテンツとの間に、前記第２タイプのコンテンツの送信の間は非暗号化状態のままとする前記第２タイプのコンテンツを示す第２フラグを挿入し、
前記第１タイプのコンテンツの送信のために前記第１タイプのコンテンツを暗号化する、
部分暗号化メカニズムと、
暗号化されたバーションの前記第１タイプのコンテンツと非暗号化のバージョンの前記第２タイプのコンテンツを含むデータストリームを送信する送信機と、
を備えることを特徴とする装置。
【請求項１５】
前記第１の保護帯域文字は、暗号化データアイランド期間又は暗号化ビデオデータ期間を示す値を含み、
前記第２の保護帯域文字は、非暗号化データアイランド期間又は非暗号化ビデオデータ期間を示す別の値を含む請求項１４に記載の装置。
【発明の詳細な説明】
【技術分野】
【０００１】
本発明の実施形態は、一般的に、データ通信の分野に関し、より具体的にはデータストリームの部分暗号化を実行することに関する。
【背景技術】
【０００２】

デジタルコンテンツ保護に対して、非圧縮デジタルデータを送信するためのコンパクトなオーディオ／ビデオインタフェースである「高精細マルチメディアインタフェース」（ＨＤＭＩ（登録商標））のようなデジタルインタフェースを通じて送信されるコンテンツ又はデータの暗号化を可能にする「高帯域幅デジタルコンテンツ保護」（ＨＤＣＰ（登録商標））が利用される。現在のＨＤＣＰプロトコルでは、データストリームの全ての種類のコンテンツ又はデータ（例えば、オーディオデータ、ビデオデータ、制御データ等）が、送信システムと受信システムとの間で通信される場合に暗号化される。従って、暗号化データストリームのコンテンツのうちのいずれのものも、下流のＨＤＣＰ受信機（例えば、高精細テレビジョン（ＨＤＴＶ））においてコンテンツが暗号解読されるまで使用することができない。「モバイル高精細リンク」（ＭＨＬ（登録商標））の場合には、中間受信デバイスとして機能し、かつモバイルデバイス（例えば、セル電話）とＨＤＭＩ受信機の間のＭＨＬベースのデータストリームの通信及び送信を容易にするブリッジチップを使用することができる。ＭＨＬは、ＭＨＬが、モバイルデバイス（例えば、スマート電話）を他のデバイス（例えば、ＨＤＴＶ）に接続するためのモバイルオーディオ／ビデオインタフェース規格を指す点でＨＤＭＩとは区別される。ＨＤＭＩ又はＭＨＬのいずれも暗号化を要求又は定義せず、ＨＤＣＰは、暗号化処理に対して使用することができる多くの暗号化処理のうちの１つである。

【０００３】

既存のＨＤＣＰプロトコルを使用すると、ストリームのある一定のコンテンツ（フォーマット実行の理由による制御コンテンツ等）を修正するか又は少なくとも閲覧することが有利になる場合であっても、ＨＤＭＩデータストリーム及びＭＨＬデータストリーム内の全ての種類のコンテンツが完全に暗号化されるので、データストリーム全体を端末受信デバイスに送信することが必要とされ、そこでコンテンツをアクセスして分析することができる前に完全に暗号解読する必要がある。

【０００４】

送信機と受信機の間では、暗号化データストリームを提供してデータストリームの暗号化が有効又は無効のいずれであるかなどの暗号化データストリームを検出するのに様々な信号伝達プロトコル（例えば、「オリジナル暗号化ステータス信号伝達」（ＯＥＳＳ）、「拡張暗号化ステータス信号伝達」（ＥＥＳＳ））を使用することができるように考えられている。例えば、ＥＥＳＳプロトコルは、ＨＤＭＩプロトコルと共に使用され（かつ「デジタルビジュアルインタフェース」（ＤＶＩ（登録商標））プロトコルにおける任意的な機能である）、一方、ＯＥＳＳは、ＤＶＩプロトコルと共に使用される。

【先行技術文献】

【非特許文献】

【０００５】

【非特許文献１】「高性能シリアルバス規格（Ｓｔａｎｄａｒｄ ｆｏｒ ａ Ｈｉｇｈ Ｐｅｒｆｏｒｍａｎｃｅ Ｓｅｒｉａｌ Ｂｕｓ）」、ＩＥＥＥ、１３９４～１９９５ページ及び相補、１９９６年８月３０日

【発明の概要】

【発明が解決しようとする課題】

【０００６】

本発明の実施形態は、データストリームの部分暗号化を実行することに関する。

【課題を解決するための手段】

【０００７】

本発明の第１の態様において、方法の一実施形態は、オーディオコンテンツ、ビデオコンテンツ、及び制御コンテンツのうちの１以上を含むコンテンツを有するデータストリームをデータ送信デバイスで受信する処理と、暗号化される１以上のコンテンツを判断する処理とを含む。更に、本方法は、１以上のコンテンツを暗号化し、他のコンテンツを非暗号化状態のままに残すことによってデータストリームを部分的に暗号化する処理と、部分暗号化データストリームをデータ送信デバイスからデータ受信デバイスに送信する処理と

を含む。

【０００８】

本発明の第２の態様において、システムの一実施形態は、ストレージ媒体及びストレージ媒体に結合されたプロセッサを有し、データ受信デバイスに結合されたデータ送信デバイスを更に有するデータ処理デバイスを含む。データ送信デバイスは部分暗号化メカニズムを有し、オーディオコンテンツ、ビデオコンテンツ、及び制御コンテンツのうちの１以上を含むコンテンツを有するデータストリームを受信し、暗号化される１以上のコンテンツを判断する。更に、データ送信デバイスは、１以上のコンテンツを暗号化し、他のコンテンツを非暗号化状態のままに残すことによってデータストリームを部分的に暗号化し、部分暗号化データストリームをデータ送信デバイスに結合されたデータ受信デバイスに送信する。

【０００９】

本発明の第２の態様において、装置の一実施形態は、オーディオコンテンツ、ビデオコンテンツ、及び制御コンテンツのうちの１以上を含むコンテンツを有するデータストリームを受信し、暗号化される１以上のコンテンツを判断する部分暗号化メカニズムを有するデータ送信デバイスを含む。更に、データ送信デバイスは、１以上のコンテンツを暗号化し、他のコンテンツを非暗号化状態のままに残すことによってデータストリームを部分的に暗号化し、部分暗号化データストリームをデータ送信デバイスに結合されたデータ受信デバイスに送信する。

【００１０】

本発明の実施形態を類似の参照番号が類似の要素を指す添付図面の図に限定としてではなく例として示している。

【図面の簡単な説明】

【００１１】

【図１】本発明の一実施形態によるデータストリームにおける部分暗号化のためのシステムを示す図である。

【図２】本発明の一実施形態によるソース送信デバイスを示す図である。

【図３Ａ】本発明の一実施形態によるブリッジデバイスを示す図である。

【図３Ｂ】本発明の一実施形態によるシンク受信デバイスを示す図である。

【図４Ａ】本発明の一実施形態によるデータストリームの部分暗号化を示す図である。

【図４Ｂ】本発明の一実施形態によるデータストリームの部分暗号化を示す図である。

【図５】本発明の一実施形態によるデータストリームの部分暗号化を示す図である。

【図６】本発明の一実施形態によるデータストリームの部分暗号化を示す図である。

【図７】本発明の一実施形態によるデータストリームの部分暗号化を実行する方法を示す図である。

【図８】本発明の一実施形態によるデータストリームの部分暗号化を実行する方法を示す図である。

【図９】本発明の実施形態を使用することができるシステムの要素の図である。

【発明を実施するための形態】

【００１２】

本発明の実施形態は、データストリームの部分暗号化を実行することに関する。

【００１３】

一実施形態において、データストリームのある一定のコンテンツ（ビデオコンテンツ及びオーディオコンテンツ）が暗号化され、その一方、そのようなデータストリームのビデオコンテンツ及びオーディオコンテンツのような他の形態のコンテンツの保護を損なうことなく、例えば、非暗号化制御データへのアクセスを提供することができるように、ある一定の他のコンテンツ（例えば、制御コンテンツ）が暗号化されないままに留まるようなデータストリームの部分暗号化を開示している。言い換えれば、データストリームのビデオコンテンツ及び／又はオーディオコンテンツが保護に向けて暗号化されるが、その制御コンテンツが暗号化さないままアクセス及び解析に向けて平常状態に留まるデータストリ

ームの選択的部分暗号化を開示している。あらゆる種類のコンテンツ（例えば、オーディオ、ビデオ、又は制御）を暗号化するか又は非暗号化状態に残すことができるように考えられている。例えば、バックグランド・オーディオがいずれの保護値も保持しない場合には、このデータストリームのオーディオコンテンツは暗号化することができない。同様に、オーディオコンテンツのうちの一部（全てとは対照的に）を暗号化状態に残すことができ、又はコンテンツのあらゆる組合せ（オーディオコンテンツと制御コンテンツ等）を非暗号化状態に残すことができ、他のコンテンツ（ビデオコンテンツ等）を暗号化することができる。データストリームにおけるコンテンツ暗号化のそのような柔軟性が与えられる。「コンテンツ」という用語と「データ」という用語とは同義であるとみなし、本明細書を通して交換可能に使用する。

【００１４】

一実施形態において、暗号化されるコンテンツの暗号化が行われ、一方、データストリーム内の他のコンテンツが非暗号化状態で残されるように、送信機（「ソース」とも称する。）への構成拡張が行われる。同様に、最終的な下流の受信機（「シンク」とも称する。）及び下流の中間受信機（ブリッジチップを有する「ブリッジデバイス」とも称する。）が、部分暗号化データストリームを認識して処理する機能を有するように、これらの受信機に他の拡張が加えられる。一実施形態において、ＨＤＣＰデータストリーム（例えば、ＨＤＭＩデータストリーム、ＭＨＬデータストリーム等）のあらゆる既存の制御コンテンツを暗号化することを可能にし（例えば、バージョン１．４までのＨＤＣＰバージョン内で指定されている通りに）、同時に制御情報を有する付加的なデータアイランド期間（「データアイランド」とも称する。）を非暗号化状態に留めることを可能にすることのような更に別の拡張が与えられる。暗号化されるデータと非暗号化状態に留めるべきデータとの間で区別を付けるためのプロトコルも導入され、それに対して本明細書で説明する。制御コンテンツを非暗号化状態に留める１つの利点は、制御コンテンツにアクセスし、そのうちのいずれかを暗号解読することを必要とせずに読み取り、精査し、解析することを可能にすることである。ＭＨＬデータストリームの場合の一実施形態における別の利点は、ブリッジチップ又はポートプロセッサが、データストリームを伝達するリンクのいずれの端末における暗号処理にも影響を及ぼすことなく、全体のデータストリームに非暗号化データアイランド期間を挿入し、及び／又は全体のデータストリームから非暗号化データアイランド期間を除去することを可能にすることである。例えば、この新しいプロトコルの使用は、初期認証中に受信機又は受信デバイス又はシステムのＨＤＣＰ表示データチャンネル（ＤＤＣ）において付加的なレジスタビットを用いて調整される。様々なプロトコル（例えば、暗号化／暗号解読プロトコル、暗号化データ／非暗号化データ検出プロトコル等）がＨＤＣＰを含むことができ、データ信号は、ＨＤＭＩ信号又はＭＨＬ信号を含むことができるが、本実施形態はそのような技術に限定されない。

【００１５】

一実施形態において、コンテンツ自体を集積回路（チップ又はプロセッサ）の外側で可視にすることなくデータストリームの内側を閲覧するために、保護コンテンツデータストリームの中間担体として機能するブリッジデバイスが利用される。このようにして、この中間段は、コンテンツが非保護形態で複写される危険性なしに制御コンテンツを処理することができる。更に、ブリッジデバイスは、ソースからシンクへの中継ブリッジデバイスを経由した暗号化データのシーケンスに影響を及ぼすことなく、データストリームにデータを挿入するか又はそこから除去することができる。

【００１６】

受信機チップ及び送信機チップにおいて、ロッキング回路、「位相ロックループ」（ＰＬＬ）、「遅延ロックループ」（ＤＬＬ）、暗号化論理、暗号解読論理、認証エンジン、１つ又はそれよりも多くの（バックグランド／フォアグランド）処理エンジンなどのようないくつかの論理／回路を使用することができるように考えられている。しかし、本発明の実施形態は、ＨＤＭＩ及びＭＨＬに限定されず、あらゆる他の種類のデータストリームに対して使用することができる。同様に、本発明の実施形態は、ＨＤＣＰに限定されず、

他の暗号化プロトコル又はメカニズムに適用し、これらと共に使用することができる。しかし、本明細書では簡略化、明瞭化、及び説明の平易化のために、ＨＤＣＰ、ＨＤＭＩ、及びＭＨＬなどを使用する。

【００１７】

図１は、本発明の一実施形態によるデータストリーム内の部分暗号化のためのシステムを示している。図示の実施形態において、第１のデバイス１１０は、データストリームのコンテンツの暗号化を実行する暗号化エンジン１１２を含むデータ送信デバイス（「ソース」又は「拡張送信機」とも称する。）である。一実施形態において、更に第１のデバイス１１０は、暗号化エンジン１１２との通信状態で、本明細書を通して説明するように、特定の種類のコンテンツ（例えば、オーディオコンテンツ）を暗号化し、一方、他の種類のコンテンツ（例えば、ビデオコンテンツ及び制御コンテンツ）を非暗号化状態のままに残すことのようなデータストリームの部分暗号化を容易にする部分暗号化メカニズム１１４を含む。部分暗号化メカニズム１１４は、本発明の実施形態による部分暗号化を実行することができるように拡張された送信デバイス１１０を開発するために、ソフトウエアモジュール、ハードウエア構成要素、又はソフトウエアとハードウエアの組合せを有するファームウエアのようなそれらのあらゆる組合せを含む。図示のように、第１のデバイス１１０は、この図ではブリッジデバイス１２０である第２のデバイスにデータストリームを送信する。次に、第２のデバイスは、データストリームを利用するデータ受信デバイス又はシンクデバイスとすることができる第３のデバイス１３０に受信したデータストリームを送信することができる。

【００１８】

一実施形態において、第１のデバイス１１０は、データリンク１４０を通じて、暗号化データ１４２、非暗号化データ１４４、及び非暗号化ＭＨＬ固有制御コンテンツ１４６のようなあらゆる他の追加コンテンツを第２のデバイス１２０に送信する。第２のデバイス１２０が、データストリームを部分的に暗号化しようとする拡張送信機１１０の意図に対応することができるという情報を第２のデバイス１２０から読み戻す第１のデバイス１１０から第２のデバイス１２０に送られる指令のような指令１５２を第１のデバイスと第２のデバイス１２０との間で送信するために、指令バス１５０を使用することができる。一実施形態において、この図ではブリッジチップである第２のデバイス１２０は、第１のデバイス１１０の部分暗号化制御メカニズム１１４との通信状態で、第１のデバイス１１０から受信するデータストリームの暗号化と非暗号化の両方のコンテンツ１４２～１４６を受信して検出及び理解するブリッジ部分暗号化制御メカニズム（「ＰＥＣメカニズム」）を有することによって拡張される。データストリームの非暗号化コンテンツ１４４（例えば、非暗号化制御コンテンツ）は、閲覧、解析、及び修正などのために使用することができる。

【００１９】

一例では、第２のデバイスは、次に、データストリームの暗号化及び非暗号化のコンテンツ１４２～１４６を第２のデータリンク１６０を通じて第３のデバイス１３０に送信することができ、第３のデバイス１３０は、受信データストリームを利用するデータ受信デバイス（「シンク」又は「拡張受信機」とも称する。）である。第３のデバイス１３０は、第３のデバイス１３０において受信される暗号化コンテンツ１４２の暗号解読のための暗号解読エンジン１３２を含む。一実施形態において、第３のデバイス１３０は、第２のデバイス１２０と同様に、第１のデバイス１１０から受信される暗号化及び非暗号化のコンテンツ１４２～１４６の組合せを受信して検出及び理解するために、第２のデバイス１２０から暗号化及び非暗号化のコンテンツ１４２～１４６を受信するシンクＰＥＣメカニズム１３４を含む。

【００２０】

一般的なデータストリームは、ビデオコンテンツ、オーディオコンテンツ、及び制御コンテンツのような３つの種類のコンテンツを含む。ビデオコンテンツは、各ピクセル値が、送信デバイス１１０内で生成されるマスクによって暗号化されるビデオデータ期間内に

保持することができる。オーディオコンテンツは、各データペイロードバイトが、送信デバイス１１０内で生成されるマスクによって暗号化されるデータアイランド期間内のある種類のパケット内に保持することができる。制御データは、（この状況では）各ペイロードバイトが、同じ種類の送信デバイス生成マスクによって暗号化されるデータアイランド期間内の異なる種類のパケット内に保持することができる。マスク生成は、クロックサイクル毎に進行させることができ、ビデオデータ期間又はデータアイランド期間内の各クロック期間において進む。マスク発生器は、ＨＤＣＰ規格内のプロトコルに従って定期的に「キー変更」することができる。

【００２１】

歴史的にＨＤＣＰの元来の意図は、ＤＶＩリンクのビデオコンテンツを保護することであったが、その後に、オーディオコンテンツ及びこのオーディオコンテンツの暗号化を含める拡張に伴って、制御コンテンツも暗号化プロトコル内に含められたが、制御コンテンツは暗号化を保証することができない。この場合、データストリームのビデオコンテンツ及びオーディオコンテンツは、暗号化コンテンツ１４２として暗号化して送ることができ、一方、制御コンテンツは、非暗号化状態のままに残され、送信デバイス１１０から下流のシンク又は受信デバイス１３０までの経路に沿った様々な受信デバイスに対して可視である。１つのそのようなデバイスはブリッジデバイス１２０を含み、ブリッジデバイス１２０では、入力ポートから出力ポートへの制御コンテンツプロトコルをＨＤＣＰの保護を損ねることなく変更することができ、一方、ポートプロセッサが、ＨＤＣＰによって与えられる保護に影響を及ぼすことなく、入力ポートを選択して、単一の出力ポートを用いて制御コンテンツを出力することができる。部分暗号化の実施形態の更なる詳細をその後の図に開示している。

【００２２】

図２は、本発明の一実施形態によるソース送信デバイスを示している。一部の実施形態において、ソース送信デバイス１１０（ソース）は、データストリームの送信用送信機２１４と、データ送信を制御するコントローラ２１６と、別のデバイス（例えば、中継ブリッジデバイス又はシンクのような受信デバイス）への送信の前にデータストリームのコンテンツを暗号化する（図１に示すように）暗号化エンジンとを含む。更に、送信デバイス１１０は、送信の前のデータの格納のためのデータストレージ２１２と、送信の前に外部データソース２４０からある一定のデータを受信する受信機２３０とを更に含むことができる。

【００２３】

送信デバイス１１０は、データポート２２０と制御ポート２２２とを更に含むことができる。送信デバイス１１０は、データストリームを複数の異なるモードでデータポート２２０を通じて送信する間に、例えば、第１のモードから第２のモードに移行することができるなどで作動中にデータストリームの送信を変更することができる。送信デバイス１１０は、制御ポート２２２を通じてメッセージを送信して、送信デバイス１１０が、暗号化コンテンツと非暗号化コンテンツの両方を含む部分暗号化データストリームを送ることを受信デバイス又はブリッジデバイスに知らせるなどで、受信デバイスにある一定の状況を通知（又は警告）する。次に、送信デバイス２１０は、部分暗号化データストリームを送信する前に制御ポート２２２において確認応答（ＡＣＫ）が受信されるまで待機することができ、又は確認応答を受信することなく、この送信に進むことができる。

【００２４】

一実施形態において、ソース送信デバイス１１０は、ソース送信デバイス１１０が、データストリームのある一定の保護可能コンテンツを暗号化し、一方、他のコンテンツを非暗号化状態に残すことによって部分暗号化データストリームを生成するのを容易にする部分暗号化メカニズム１１４を含む。部分暗号化メカニズム１１４は、暗号化エンジン１１２と協働してデータストリームの部分暗号化のタスクを実施することができる。部分暗号化メカニズム１１４は、上述の部分暗号化、暗号化されるコンテンツを非暗号化状態のままに残されるコンテンツに対して識別して分離する処理、部分暗号化データストリームを

下流の受信デバイスに送信する処理、及び類似の処理を含むいくつかのタスクを実施する様々な構成要素を含む。部分暗号化メカニズム１１４のこれらの構成要素は、ソフトウエアモジュール、ハードウエア構成要素、又はファームウエアのようなそれらの組合せを含む。

【００２５】

図３Ａは、本発明の一実施形態によるブリッジデバイスの実施形態を示している。ブリッジデバイス１２０は、ソース送信デバイスから受信する部分暗号化データストリームを受信して利用し、部分暗号化データストリームを下流のシンク受信デバイスに更に送信する。一実施形態において、ブリッジデバイス１２０は、ブリッジデバイス１２０が、データストリーム全体を暗号解読する必要なく、ソース送信デバイスから受信している部分暗号化データストリームの暗号化コンテンツを判断し、非暗号化コンテンツを判断し、それにアクセスし、それを読み取って理解し、更に、修正することを容易にするいくつかのエンティティを含むブリッジＰＥＣメカニズム１２６を含む。ブリッジＰＥＣメカニズム１２６のこれらの構成要素は、ソフトウエアモジュール、ハードウエア構成要素、又はファームウエアのようなそれらの組合せを含む。

【００２６】

ブリッジデバイス１２０は、データ操作を制御するコントローラ３１４と、データストリームを受信する受信機３１６と、データストリームを送信する送信機３１８とをデータストリームの受信及び送信それぞれのためのデータポート３４０及び３４４、並びに送信デバイスとの指令の交換のための制御ポート３４２と共に含むことができる。ブリッジデバイス１２０は、ビデオディスプレイ３５０、オーディオスピーカ３６０、データストリームの受信コンテンツの格納のためのデータストレージデバイス３１２などのような１つ又はそれよりも多くのデバイスと結合することができる。一実施形態において、ブリッジデバイス１２０は、部分暗号化データストリームを受信することができ、更に、非暗号化コンテンツを暗号解読又は再暗号化するか又は更に非暗号化コンテンツの認証処理に介入することなく、データストリームの非暗号化コンテンツ（例えば、制御コンテンツ）を精査し、更に、修正することができる。

【００２７】

図３Ｂは、シンク受信デバイス１３０を示している。シンク受信デバイス１３０は、部分暗号化データストリームを受信し、ビデオディスプレイ３９２及びオーディオスピーカ３９４を通じてデータストリームを提供又は提供する下流のシンクデバイスとして機能することができる。受信デバイス１３０のいくつかの構成要素は、ブリッジデバイス１２０の構成要素に類似し、簡略化のためにかつ反復を回避するために、ここではそのような共通の構成要素を解説しない。一実施形態において、シンク受信デバイス１３０は、シンク受信デバイス１３０が、ソース送信デバイスから受信している部分暗号化データストリームの暗号化コンテンツを判断し、非暗号化コンテンツを判断し、それにアクセスし、読み取って理解することを容易にするいくつかのエンティティを含むシンク部分暗号化制御メカニズム１３４を含む。シンク受信デバイスは、部分暗号化データストリームのコンテンツのうちのいずれかをビデオ表示デバイス３９２及び／又はオーディオスピーカ３９４を通じて提供することができる。ブリッジＰＥＣメカニズム１２６の場合と同様に、シンクＰＥＣメカニズム１３４のこれらの構成要素は、ソフトウエアモジュール、ハードウエア構成要素、又はファームウエアのようなそれらの組合せを含む。更に、シンク受信デバイス１３０は、ブリッジデバイス又はソース送信デバイスから受信する部分暗号化データストリームの暗号化コンテンツを暗号解読する暗号解読エンジン１３２を含む。

【００２８】

図４Ａは、本発明の一実施形態によるデータストリームの部分暗号化を示している。ＨＤＣＰ暗号化は、ＨＤＭＩリンクにおいて、ビデオデータ期間４１０の先頭保護帯域文字４１２及び４２２の直後に始まり、データアイランド期間４２０が、それぞれ拡張送信機４３０と拡張受信機４４０との間で通信される。ビデオデータ期間４２０では、コンテンツの暗号化は、ビデオデータ期間４２０の最終のピクセルまで各ピクセルに対して進行し

、従って、回避されるいずれの後尾保護帯域も存在しない。しかし、データアイランド期間４１０の場合には、コンテンツの暗号化は、後尾保護帯域４１４（暗号化されない）に達するまで各クロック期間（各クロック期間内にパケットデータを有する）に対して進行する。一実施形態において、データアイランド期間とビデオデータ期間の両方４１０、４２０に対する先頭保護帯域４１２、４２２の後に、付加的な文字を有するフラグ４１６、４２６が挿入される。フラグ又はフラグ文字４１６、４２６は、拡張送信機４３０及び拡張受信機４４０それぞれの暗号化エンジン及び暗号解読エンジンに対する暗号化／暗号解読指示として機能する。一実施形態において、フラグ４１６、４２６が設定されると、拡張送信機４３０の暗号化エンジンは、フラグ４１６、４２６が設定されたデータアイランド期間４１０又はビデオデータ期間４２０の関連コンテンツを暗号化し、一方、フラグが設定されていないデータアイランド期間及びビデオデータ期間４１０、４２０の他のコンテンツを非暗号化状態のままに残す。

【００２９】

一実施形態において、拡張送信機４３０に到着するデータストリーム４５０が既に暗号化されている場合には、拡張送信機４３０の部分暗号化メカニズム１１４は、先頭保護帯域４１２、４２２の前の最後の制御期間文字を先頭保護帯域４１２、４２２の最初の文字として用い、「１クロックサイクル前にシフト」させて「着信保護帯域を時間的に１サイクル前に移動」させるこの処理を繰返し、この文字の後にフラグ文字４１６、４２６を挿入するための１クロック期間を残すことにより、依然としてフラグ文字をクロック制御されたストリーム内に挿入することができる。そのような操作は、先入れ先出し（ＦＩＦＯ）又は他の類似のバッファ方式に基づいている。別の実施形態において、先頭保護帯域４１２、４２２の後にフラグ４１６、４２６を挿入するために、データアイランド期間及びビデオデータ期間４１０、４２０全体を１クロック期間遅延させることができる。ＨＤＭＩは、データアイランド期間４１０及びビデオデータ期間４２０が、１２クロック期間よりも短くない制御期間によって互いから分離されることを要求するので、フラグ文字４１６、４２６を挿入するための余地が存在し、更に、プリアンブルを挿入するための８クロック期間さえも与える。例えば、クロック期間は、最小制御期間をゼロにすることなく１クロック期間短くすることを可能にするように改修することができる。

【００３０】

別の実施形態において、先頭保護帯域４１２、４２２内で新しい値が文字として使用される。先頭保護帯域４１２、４２２のあらゆるシーケンス内の文字は等しい値を含むが、これらの値は、ＨＤＭＩプロトコル内で提供されている２つの選択肢ではなく４つの選択肢から選択することができる。これらの４つの選択肢は、暗号化データアイランド期間、非暗号化データアイランド期間、暗号化ビデオデータ期間、及び非暗号化ビデオデータ期間を含む。次に、図４Ｂを参照すると、上述のメカニズムを用いて、拡張送信機及び拡張受信機４３０、４４０は、どの種類のコンテンツ（例えば、オーディオ、ビデオ、制御）を暗号化されるか（又は非暗号化状態のままに残されるか）を調整する。一実施形態において、拡張送信機４３０は、表示データチャンネル（ＤＤＣ）バス４８５（ＭＨＬベースのシステムでは制御バス（ＣＢＵＳ）を使用することができる）上の（ＨＤＣＰ）拡張受信機４４０のデバイスアドレスにあるその（ＨＤＣＰ）拡張受信機４４０内のレジスタ４７２～４７６から特徴値４８０を読み取る。ＤＤＣは、I^2Cバス規格に基づく通信チャンネルを意味する。ＨＤＭＩは、シンク受信機が対応するオーディオ／ビデオフォーマットを判断するのにソース送信機を使用することができる拡張ＤＤＣ（Ｅ－ＤＤＣ）への対応を特に要求する場合がある。ＣＢＵＳは、ソースデバイス又はシンクデバイスが、その対応するＭＨＬ準拠のシンクデバイス及びソースデバイスそれぞれへの接続性を検知するためのメカニズムを意味し、単線（１ビット）の双方向制御バスを含むことができる。

【００３１】

一実施形態において、この特徴値４８０内のビットに従って拡張送信機４３０は、（ａ）ビデオ、（ｂ）オーディオ、又は（ｃ）データアイランド期間４１０内の１つ又はそれよりも多くの種類のパケットを暗号化することを選択する。１つよりも多いパケットが、

いずれか１つのデータアイランド期間４１０内に含まれている場合には、データアイランド期間４１０毎に１つの先頭保護帯域４１２及び１つの挿入フラグ文字４１６しか存在しないので、データアイランド期間４１０内の全てのパケットが暗号化され、又は非暗号化状態のままに残されるかのいずれかである。別々のデータアイランド期間４１０へのパケットのセグメント化は、拡張送信機４３０によって制御される。

【００３２】

一実施形態において、拡張送信機４３０は、ビデオコンテンツとオーディオコンテンツの両方を暗号化するが、制御コンテンツ（インフォフレーム、データパケットのような）を非暗号化状態のままに残す。拡張受信機（下流のブリッジデバイス、ポートプロセッサ、又は他の受信デバイス等）は、部分暗号化制御メカニズムを用いてこれらのデータパケットを検出して読み取って、データストリームの態様を（ａ）ビデオモード、（ｂ）リンクモード［赤、緑、青（ＲＧＢ）、ＹＣｂＣｒ等］、（ｃ）オーディオコンテンツ保護［ＡＣＰ］設定等として判断することができる。この情報を用いて、又は経時的なこの情報の変化に反応して、下流の拡張受信機４４０は、最初にＨＤＣＰストリーム全体を暗号解読する必要なく、新しい構成に向けて準備を整える。言い換えれば、一実施形態により、部分暗号化技術を用いて、データストリームの制御コンテンツは非暗号化状態で供給され、受信端末上でデータストリーム全体を暗号解読する必要性が排除される。

【００３３】

別の実施形態において、データストリームのビデオコンテンツは暗号化されるが、オーディオコンテンツ（及び制御コンテンツ）は、非暗号化状態のままに留まり、又はその逆も同様である。この場合、コンテンツプロバイダ（例えば、ケーブルヘッドエンド）は、ビデオコンテンツを保護する及び従って暗号化する必要があるが、オーディオコンテンツは、非保護状態及び従って非暗号化状態のままに留めることができることを示す（拡張送信機４３０の上流から）。そのような場合の例は、保護を必要とするビデオ表示であり、ある一定の音楽オーバーレイ又は関連性のない背景音（例えば、鳥のさえずり、パトカーの音等）は、保護又は暗号化に値するとは見なされない。それとは逆に、オーディオコンテンツは、保護及び暗号化され、拡張送信機４３０から暗号化を必要としない「オーバーレイ」ビデオパターン（例えば、渦巻く光等）と共に送ることができる。この技術を用いて、下流の受信デバイス４４０は、暗号化コンテンツ、又は暗号化／暗号解読マスク値を増分するカウンタに影響を及ぼすことなく、非暗号化コンテンツを剥奪することができる。

【００３４】

図５は、本発明の一実施形態によるデータストリームの部分暗号化を示している。図示の実施形態において、非暗号化データアイランド期間（非暗号化制御コンテンツ５４０及び非暗号化オーディオコンテンツ５４５を含む）及び非暗号化ビデオデータ期間（非暗号化ビデオコンテンツ５５０を含む）を有するデータストリームが拡張送信機５１０に入り、そこでデータストリームは部分的に暗号化される。データストリームの部分暗号化は、制御コンテンツ５６０及びビデオコンテンツ５７０の暗号化を含み、一方、オーディオコンテンツ５４５を非暗号化状態のままに残す。拡張送信機５１０は、部分暗号化メカニズムを用いて暗号化された制御コンテンツ及びビデオコンテンツ５６０、５７０を製造する。例えば、図４Ｂを参照して上述したように、暗号化される、又は非暗号化状態のままに残されるデータストリームのコンテンツの種類を判断するために、ＨＤＣＰレジスタから拡張送信機５１０に特徴値を送ることができる。

【００３５】

図示の実施形態において、暗号化制御コンテンツ５６０、並びに暗号化ビデオコンテンツと非暗号化オーディオコンテンツの両方を含むデータストリームの全てのコンテンツが、ブリッジデバイス５２０に送られる。オーディオコンテンツ５４５は非暗号化状態のままに留まるので、一実施形態において、ブリッジデバイスのオーディオデバイス５２５によって再生される。一実施形態において、暗号化ビデオコンテンツ５７０及び暗号化制御コンテンツ５６０は、下流のＨＤＣＰシンク又は受信デバイス５３０に送られる。

【００３６】
図６は、本発明の一実施形態によるデータストリームの部分暗号化を示している。暗号化オーディオコンテンツ６４０及び暗号化ビデオコンテンツ６５０を含むＨＤＭＩベースのデータストリームがＭＨＬベースの拡張送信機６１０に供給される。一実施形態において、拡張ＭＨＬ送信機６１０は、下流の拡張送信機ＨＤＣＰシンクデバイスが、（シンク）部分暗号化制御メカニズムを用いて、暗号化コンテンツ期間６４０、６５０を暗号化状態として検出することができるように、部分暗号化メカニズムを用いて、暗号化オーディオコンテンツ６４０及び暗号化ビデオコンテンツ６５０の各々の先頭保護帯域の後に、設定フラグ文字を挿入する。
【００３７】
更に、一実施形態において、拡張ＭＨＬ送信機６１０は、制御期間幅の制限内で、制御コンテンツ６６０を含む新しいデータアイランド期間を挿入することができる。図示の実施形態において、ＭＨＬ固有制御コンテンツ６６０は非暗号化状態にあり、従って、制御コンテンツＭＨＬ固有データアイランド期間６６０の先頭保護帯域の後に非設定フラグ文字が含まれることに示している。暗号化オーディオコンテンツ及びビデオコンテンツ６４０、６５０の場合と同様に、この非設定フラグ文字は、拡張ブリッジ６２０及び拡張受信機６３０が、制御コンテンツ６６０が非暗号化状態にあることを認識することができるように、非暗号化制御コンテンツ６６０に関連付けられ、この関連付けは、暗号化されたオーディオコンテンツ及びビデオコンテンツ６４０、６５０のストリームに影響を及ぼすことなく行われる。更に、一実施形態において、下流のＭＨＬブリッジ６２０は、（ブリッジ）部分暗号化制御メカニズムを用いて、暗号化されたオーディオコンテンツ及びビデオコンテンツ６４０、６５０、並びに非暗号化制御コンテンツ６６０を検出し、非暗号化ＭＨＬ固有制御コンテンツ６６０の吟味、解析、更に、要求及び必要に応じてのデータストリームからの除去を可能にする。暗号化されたＨＤＭＩオーディオコンテンツ及びビデオコンテンツ６４０、６５０は、次に、下流のＨＤＣＰシンク６３０又はポートプロセッサ又は更に別の拡張ブリッジデバイスに供給される。
【００３８】
図７は、本発明の一実施形態によるデータストリームの部分暗号化を実行する方法を示している。方法７００は、ハードウエア（例えば、回路、専用論理、プログラム作成可能論理、マイクロコード等）、ソフトウエア（処理デバイス上で作動する命令等）、又はファームウエア又はハードウエアデバイス内の機能回路のようなそれらの組合せを含むことができる処理論理によって実施することができる。一実施形態において、方法７００は、図１の部分暗号化メカニズム及び／又は部分暗号化制御メカニズムによって実施される。
【００３９】
方法７００は、ブロック７０５において非暗号化データストリームが拡張送信機又はソースにおいて受信される時に始まる。データストリームは、オーディオコンテンツ、ビデオコンテンツ、及び制御コンテンツという３つの種類のコンテンツを含むＨＤＭＩデータストリームを含む。データストリームのどの種類のコンテンツを暗号化されるかということは、ブロック７１０においてコンテンツプロバイダ（例えば、コンテンツ制作者、放送者、ケーブルヘッドエンド等）によって判断され、１つ又はそれよりも多くの特徴値を用いて拡張送信機に通信される。この場合、拡張送信機は、拡張ＨＤＣＰ送信機である。この実施形態において、ブロック７１５において、拡張送信機における部分暗号化メカニズムを用いてオーディオ及びビデオのコンテンツ種類が暗号化されるが、制御コンテンツは、非暗号化状態のままに残される。ブロック７２０では、部分暗号化データストリームが、ブリッジデバイスのような拡張受信機デバイスに供給される。
【００４０】
拡張受信デバイスがブリッジデバイスである場合には、ブロック７２５において、受信デバイスは、部分暗号化データストリームを受信し、ブリッジ部分暗号化制御メカニズムを用いてデータアイランド期間及びビデオデータ期間のフラグ文字挿入物を読み取ることによって暗号化コンテンツ及び非暗号化コンテンツを検出及び認識する。例えば、一実施

形態において、拡張送信機は、オーディオコンテンツにおける暗号化データアイランド期間、ビデオコンテンツにおける暗号化ビデオデータ期間、及び制御コンテンツの非暗号化データアイランド期間の先頭保護帯域の直後にフラグ文字（暗号化コンテンツに対する有効フラグ及び非暗号化コンテンツに対する無効フラグ等）を挿入する。一部の実施形態において、拡張ブリッジデバイスにおいて、必要及び必要に応じて、データストリーム全体を暗号解読することを必要とせず、非暗号化制御コンテンツを読み取り、それにアクセスし、それを解析し、修正することができる。

【００４１】

一実施形態では、次に、ブロック７３０において、部分暗号化データストリームは、下流の拡張ＨＤＣＰ受信機（シンク等）に送信される。ブリッジデバイスの場合と同様に、拡張受信機は、シンク部分暗号化制御メカニズムを含み、ブロック７３５においてデータストリームの暗号化コンテンツと非暗号化コンテンツとを検出及び認識するのにそれを使用することができる。

【００４２】

図８は、本発明の一実施形態によるデータストリームの部分暗号化を実行する方法を示している。方法８００は、ハードウエア（例えば、回路、専用論理、プログラム作成可能論理、マイクロコード等）、ソフトウエア（処理デバイス上で作動する命令等）、又はファームウエア又はハードウエアデバイス内の機能回路のようなそれらの組合せを含むことができる処理論理によって実施することができる。一実施形態において、方法８００は、図１の部分暗号化メカニズム及び／又は部分暗号化制御メカニズムによって実施される。

【００４３】

一実施形態において、ブロック８０５において、暗号化オーディオコンテンツ（データアイランド期間内の）及び暗号化ビデオコンテンツ（ビデオデータ期間内の）を有するＨＤＭＩ暗号化データストリームが、ＭＨＬ拡張送信機又はソースにおいて受信される。８１０において、部分暗号化メカニズムを有する拡張送信機が、暗号化されたオーディオコンテンツ及びビデオコンテンツを読み取り、非暗号化ＭＨＬ固有制御コンテンツをデータストリームに追加することができる。この部分暗号化データストリーム（暗号化されたオーディオコンテンツ及びビデオコンテンツ、並びに新しく追加された非暗号化ＭＨＬ固有制御コンテンツを有するもの等）は、ブロック８１５において拡張ブリッジデバイスに送信される。ブロック８２０において、ブリッジデバイスは、部分暗号化データストリームを検出し（フラグ文字を使用する等して）、データストリーム全体を暗号解読することを必要とせずに、その非暗号化ＭＨＬ固有制御コンテンツへのアクセスを可能にする。次に、ブロック８２５において、追加された非暗号化ＭＨＬ固有制御コンテンツをデータストリームから除去することができる。次に、ブロック８３０において、残りの暗号化データストリーム（暗号化されたオーディオコンテンツ及びビデオコンテンツを有するもの等）が、下流のＨＤＣＰ受信機又はシンクに送られる。シンクデバイスは、「標準」シンク又は「拡張」シンクとすることができる。「標準」シンクデバイスにデータストリームを送る処理は、（ａ）シンクが「標準」のものであり、「拡張」のものではないことを把握する処理（ＤＤＣ指令又はＣＢＵＳ指令等により）、及び（ｂ）シンクが「標準」のものであった場合に、ビデオデータ期間及びデータアイランド期間から挿入されたフラグ文字を剥奪する処理を含む。

【００４４】

図９は、本発明の一実施形態による部分暗号化メカニズムを有する送信機及び受信機を使用するためのシステムを示している。この図には、本説明に密接に関連しないある一定の標準で公知の構成要素を示していない。一部の実施形態の下では、デバイス９００は、送信デバイス、受信デバイス、又はその両方とすることができる。

【００４５】

一部の実施形態の下では、デバイス９００は、データの送信用相互接続部又はクロスバー９０５又は他の通信手段を含む。データは、視聴覚データ及び関連の制御データを含むことができる。デバイス９００は、情報を処理するために相互接続部９０５に結合した１

つ又はそれよりも多くのプロセッサ９１０のような処理手段を含むことができる。プロセッサ９１０は、１以上の物理プロセッサと１以上の論理プロセッサとを含むことができる。更に、プロセッサ９１０の各々は、複数のプロセッサコアを含むことができる。簡略化のために、相互接続部９０５を単一の相互接続部として示すが、相互接続部９０５は、複数の異なる相互接続部又はバスを表すことができ、そのような相互接続部への構成要素接続は異なるとすることができる。この図に示す相互接続部９０５は、１以上のあらゆる別々の物理バス、ポイントツーポイント接続部、又は適切なブリッジ、アダプタ、又はコントローラによって接続したこれらの両方を表す抽象表現である。相互接続部９０５は、例えば、システムバス、ＰＣＩバス又はＰＣＩｅバス、ハイパートランスポートバス又は工業規格アーキテクチャ（ＩＳＡ）バス、スモールコンピュータシステムインタフェース（ＳＣＳＩ）バス、ＩＩＣ（Ｉ２Ｃ）バス、又は時に「ファイヤワイヤ」と呼ばれる米国電気電子学会（ＩＥＥＥ）規格１３９４バスを含むことができる（１９９６年８月３０日に出された「高性能シリアルバス規格（Ｓｔａｎｄａｒｄ ｆｏｒ ａ Ｈｉｇｈ Ｐｅｒｆｏｒｍａｎｃｅ Ｓｅｒｉａｌ Ｂｕｓ）」、ＩＥＥＥ、１３９４～１９９５ページ及び付録）。更に、デバイス９００は、１つ又はそれよりも多くのＵＳＢ対応接続部を連結することができるＵＳＢバス９７０のようなシリアルバスを含むことができる。

【００４６】

一部の実施形態において、デバイス９００は、情報及びプロセッサ９１０によって実行される命令を格納するための主メモリ９２０としてランダムアクセスメモリ（ＲＡＭ）又は他の動的ストレージデバイスを更に含む。主メモリ９２０は、プロセッサ９１０による命令の実行中に一時変数又は他の中間情報を格納するために使用することができる。ＲＡＭメモリは、メモリ内容のリフレッシュを必要とするランダムアクセスメモリ（ＤＲＡＭ）と、内容をリフレッシュする必要はないが、高価である静的ランダムアクセスメモリ（ＳＲＡＭ）とを含む。ＤＲＡＭメモリは、信号を制御するためのクロック信号を含む同期動的ランダムアクセスメモリ（ＳＤＲＡＭ）と、拡張データ出力動的ランダムアクセスメモリ（ＥＤＯ ＤＲＡＭ）とを含むことができる。一部の実施形態において、システムのメモリは、レジスタ又は他の専用メモリを含むことができる。デバイス９００は、静的情報及びプロセッサ９１０に対する命令を格納するための読取専用メモリ（ＲＯＭ）９２５又は他の静的ストレージデバイスを含むことができる。デバイス９００は、ある一定の要素の格納のための１つ又はそれよりも多くの不揮発性メモリ要素９３０を含むことができる。

【００４７】

デバイス９００の相互接続部９０５には、情報及び命令を格納するためのデータストレージ９３５を結合することができる。データストレージ９３５は、磁気ディスク、光ディスク、及びそれに対応するドライブ、又は他のメモリデバイスを含むことができる。そのような要素は、互いに組み合わせることができ、又は別々の構成要素とすることができ、デバイス９００の他の要素の一部を利用することができる。

【００４８】

デバイス９００は、相互接続部９０５を通じてディスプレイ又は表示デバイス９４０に結合することができる。一部の実施形態において、ディスプレイは、液晶ディスプレイ（ＬＣＤ）、プラズマディスプレイ、ブラウン管（ＣＲＴ）ディスプレイ、又はエンドユーザに対して情報又はコンテンツを表示するためのあらゆる他の表示技術を含むことができる。一部の実施形態において、ディスプレイ９４０は、テレビジョン番組を表示するのに利用することができる。一部の実施形態において、ディスプレイ９４０は、入力デバイスの少なくとも一部分としても利用されるタッチスクリーンを含むことができる。一部の実施形態において、ディスプレイ９４０は、テレビジョン番組のオーディオ部分を含むオーディオ情報を提供するためのスピーカのようなオーディオデバイスとすることができ、又はそれを含むことができる。入力デバイス９４５は、情報及び／又は指令選択をプロセッサ９１０に通信するために相互接続部９０５に結合することができる。様々な実施において、入力デバイス９４５は、キーボード、キーパッド、タッチスクリーン及びスタイラス

、オーディオ起動システム、又は他の入力デバイス、又はそのようなデバイスの組合せとすることができる。含めることができる別の種類のユーザ入力デバイスは、方向情報及び指令選択を１つ又はそれよりも多くのプロセッサ９１０に通信し、ディスプレイ９４０上のカーソル移動を制御するためのマウス、トラックボール、又はカーソル方向キーのようなカーソル制御デバイス９５０である。

【００４９】

相互接続部９０５には、１つ又はそれよりも多くの送信機又は受信機９５５を結合することができる。一実施形態において、図１を参照して上述したように、送信機９５５は、部分暗号化メカニズムを使用する拡張送信機又はソースを含み、それに対して受信機９５５は、ブリッジ部分暗号化メカニズムを使用するブリッジデバイス、又はシンク部分暗号化メカニズムを使用する下流の拡張受信機又はシンクを含む。一部の実施形態において、デバイス９００は、データの受信又は送信用１つ又はそれよりも多くのポート９８０を含むことができる。受信又は送信することができるデータは、ＨＤＭＩデータのようなビデオデータ又はオーディオ－ビデオデータを含むことができ、ＨＤＣＰ暗号化データのように暗号化することができる。一部の実施形態において、デバイス９００は受信デバイスであり、データ受信用ポートを選択するように作動し、一方、１つ又はそれよりも多くの他のポートからデータをサンプリングして、フォアグランド処理に向けて選択されなかったポートにおいて受信されるデータが暗号化されているか否かを判断する。更に、デバイス９００は、無線信号を通じたデータの受信のための１つ又はそれよりも多くのアンテナ９５８を含むことができる。デバイス９００は、電源、バッテリ、太陽電池、燃料電池、又は電力を供給するか又は発生させるための他のシステム又はデバイスを含むことができる電力デバイス又は電力システム９６０を含むことができる。電力デバイス又は電力システム９６０によって供給される電力は、必要に応じてデバイス９００の要素に分配することができる。

【００５０】

以上の説明では、本発明の完全な理解を提供するために説明の目的で多くの特定の詳細内容を開示した。しかし、これらの特定の詳細内容のうちの一部を用いずに本発明を実施することができることは当業者には明らかであろう。その他としては、公知の構造及びデバイスをブロック図形態に示している。図示の構成要素の間の中間構造を存在させることができる。本明細書に説明又は例示する構成要素は、例示又は説明していない付加的な入力又は出力を有することができる。示す要素又は構成要素は、あらゆるフィールドの順序変更又はフィールドサイズの修正を含む異なる配列又は順序で配置することができる。

【００５１】

本発明は、様々な処理を含むことができる。本発明の処理は、ハードウエア構成要素によって実施することができ、又は命令を用いてプログラムされた汎用又は専用プロセッサ又は論理回路にこれらの処理を実施させるのに使用することができるコンピュータ可読命令に具現化することができる。代替的に、処理は、ハードウエアとソフトウエアの組合せによって実施することができる。

【００５２】

本発明の一部分は、本発明による処理を実施するようにコンピュータ（又は他の電子デバイス）をプログラムするのに使用することができるコンピュータプログラム命令が格納されたコンピュータ読み取り可能な記録媒体を含むことができるコンピュータプログラム製品として提供することができる。コンピュータ読み取り可能な記録媒体は、フロッピー（Ｒ）ディスケット、光ディスク、ＣＤ－ＲＯＭ（コンパクトディスク読取専用メモリ）、及び光磁気ディスク、ＲＯＭ（読取専用メモリ）、ＲＡＭ（ランダムアクセスメモリ）、ＥＰＲＯＭ（消去可能プログラム作成可能な読取専用メモリ）ＥＥＰＲＯＭ（電気的に消去可能なプログラム作成可能な読取専用メモリ）、磁気カード又は光カード、フラッシュメモリ、又は電子命令を格納するのに適する他の種類の媒体／コンピュータ読み取り可能な記録媒体を含むことができるが、これらに限定されない。更に、本発明は、コンピュータプログラム製品としてダウンロードすることができ、プログラムは、遠隔コンピュー

タから要求コンピュータに転送することができる。

【００５３】

本方法のうちの多くをその最も基本的な形態で説明したが、本発明の基本的な範囲から逸脱することなく、これらの方法のうちのいずれかに処理を追加するか又はこれらから処理を削除することができ、説明したメッセージのうちのいずれかに情報を追加するか又はこれらから情報を低減することができる。多くの更に別の修正及び調整を加えることができることは当業者には明らかであろう。特定的な実施形態は、本発明を限定するためではなく、例示するために提供したものである。

【００５４】

要素「Ａ」が要素「Ｂ」に結合されるか又は要素「Ｂ」と結合されると示した場合には、要素Ａを要素Ｂに直接結合するか又は例えば要素Ｃを通じて間接的に結合することができる。本明細書において、構成要素、特徴、構造、処理、又は特性Ａが、構成要素、特徴、構造、処理、又は特性Ｂを「引き起こす」と示した場合には、これは、「Ａ」が、少なくとも部分的に「Ｂ」の原因であるが、「Ｂ」をもたらすのを補う少なくとも１つの他の構成要素、特徴、構造、処理、又は特性が存在する可能性もあることを意味する。本明細書において、構成要素、特徴、構造、処理、又は特性を含む「ことができる」、「場合がある」、又は「可能性がある」と示した場合には、その特定の構成要素、特徴、構造、処理、又は特性は、含まれることが必要ではない。本明細書において、「ａ」又は「ａｎ」の付いた要素に言及した場合には、これは、説明した要素が１つしか存在しないことを意味しない。

【００５５】

実施形態は、本発明の実施又は例である。本明細書における「実施形態」、「一実施形態」、「一部の実施形態」、又は「他の実施形態」への参照は、これらの実施形態に関連して説明した特定の特徴、構造、又は特性が少なくとも一部の実施形態に含まれることを意味し、必ずしも全ての実施形態に含まれることを意味しない。「実施形態」、「一実施形態」、又は「一部の実施形態」の様々な登場は、必ずしも全てが同じ実施形態を参照しているわけではない。本発明の例示的な実施形態の以上の説明では、開示を効率化し、様々な本発明の態様のうちの１つ又はそれよりも多くの理解を助けるために、本発明の様々な特徴を場合によって単一の実施形態、図、又はこれらの説明の中にまとめ合わせたことを理解すべきである。

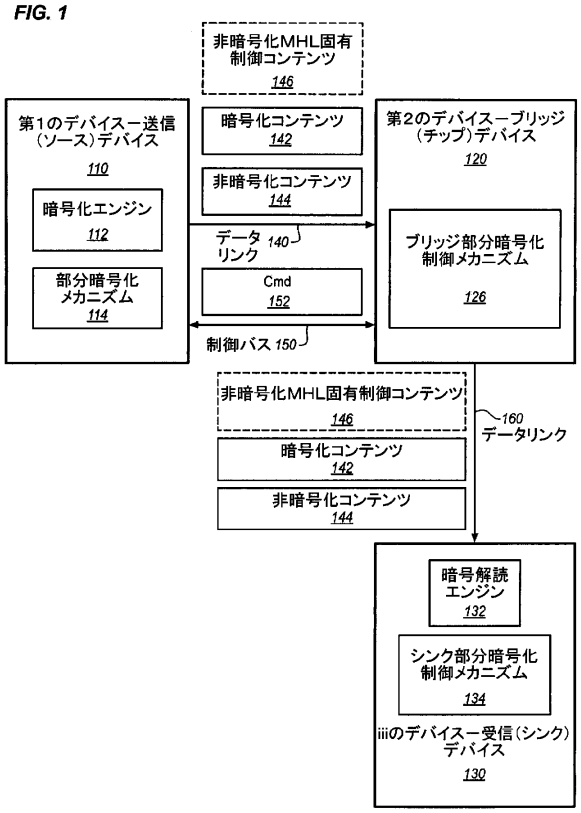
【符号の説明】

【００５６】

１１２　暗号化エンジン
１１４　部分暗号化メカニズム
１３２　暗号解読エンジン
１４２　暗号化コンテンツ
１４４　非暗号化コンテンツ
１５０　制御バス

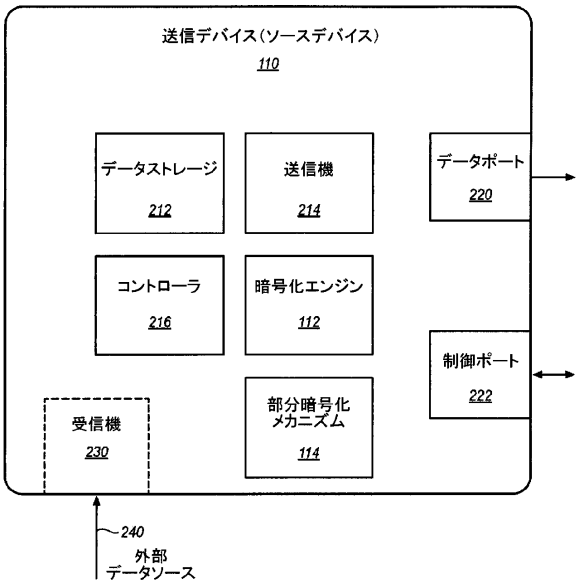
【図１】

FIG. 1



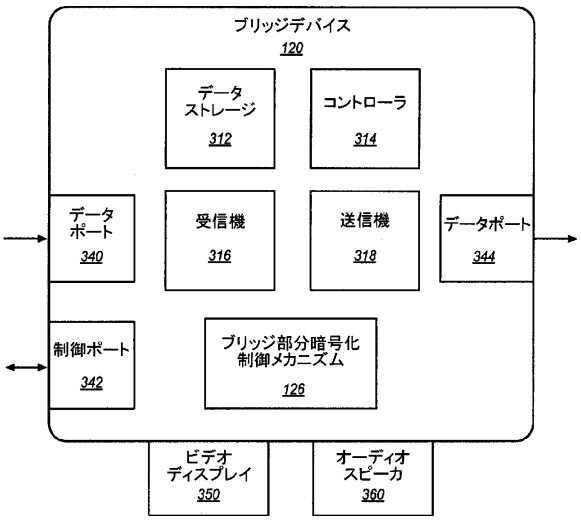
【図２】

FIG. 2



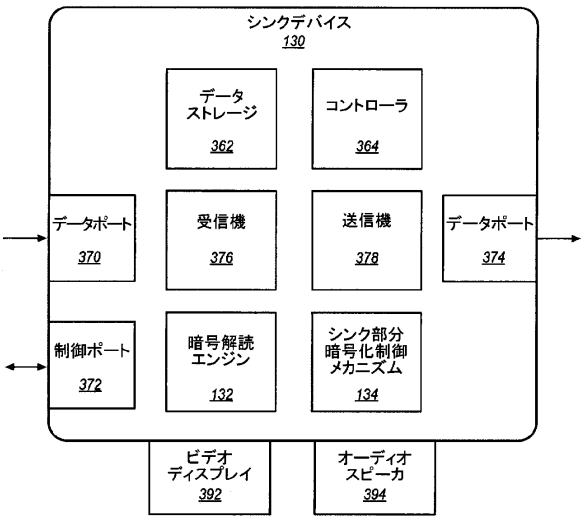
【図３Ａ】

FIG. 3A



【図３Ｂ】

FIG. 3B



【図４Ａ】

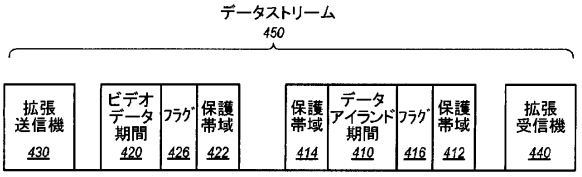


FIG. 4A

【図４Ｂ】

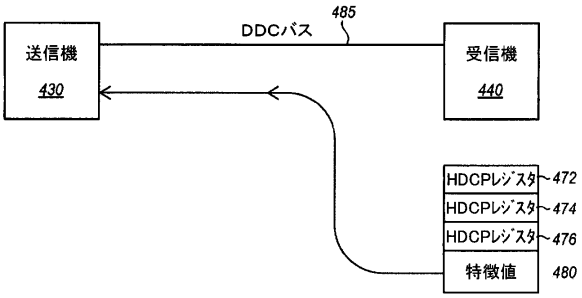


FIG. 4B

【図５】

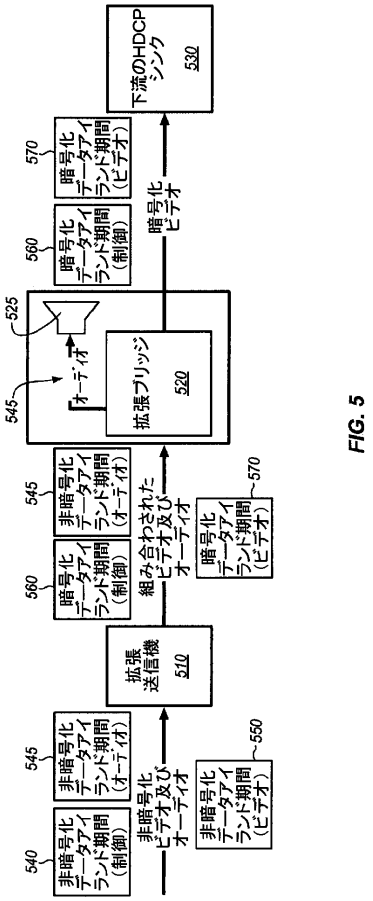


FIG. 5

【図６】

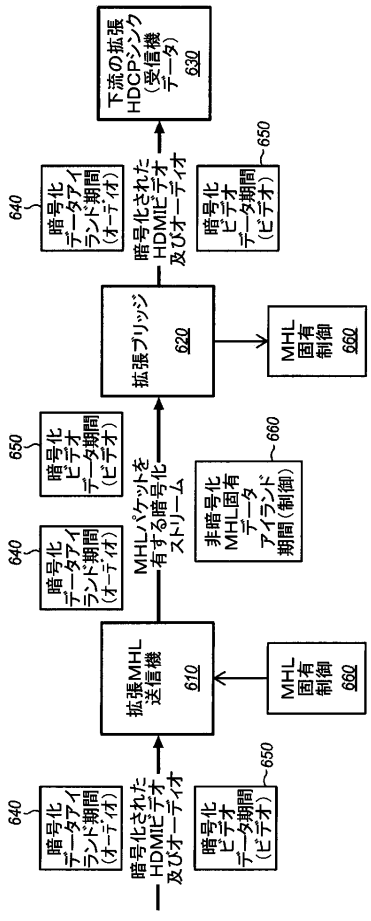
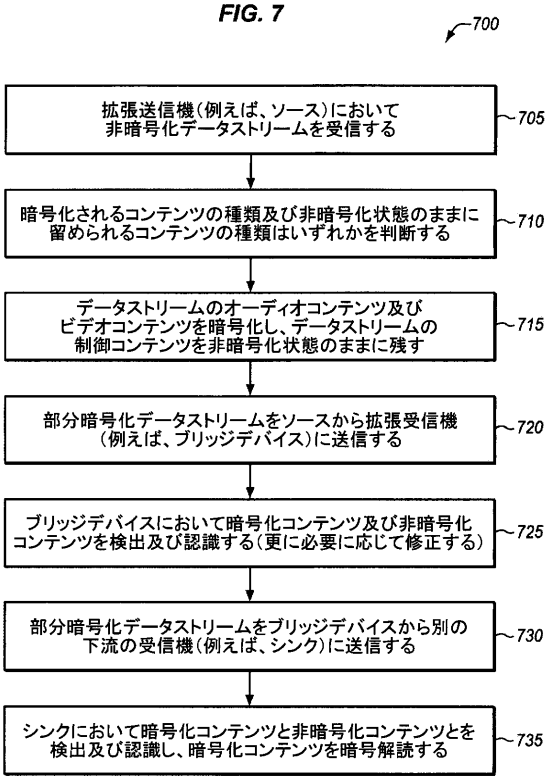


FIG. 6

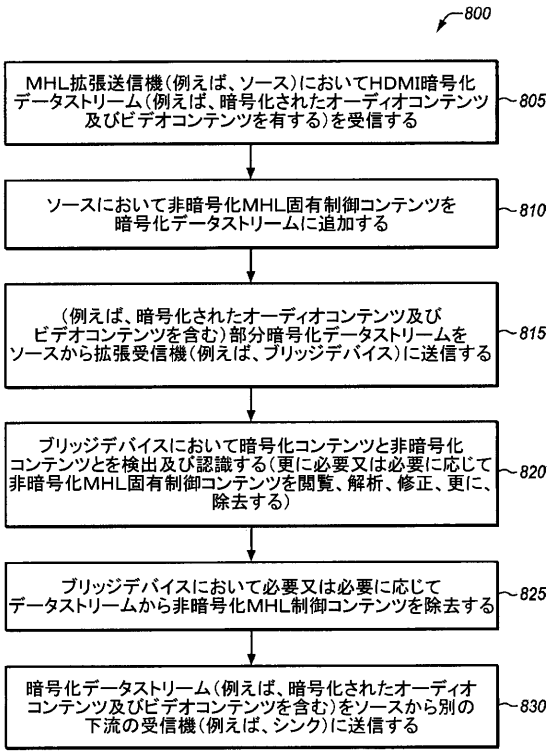
【図７】

FIG. 7



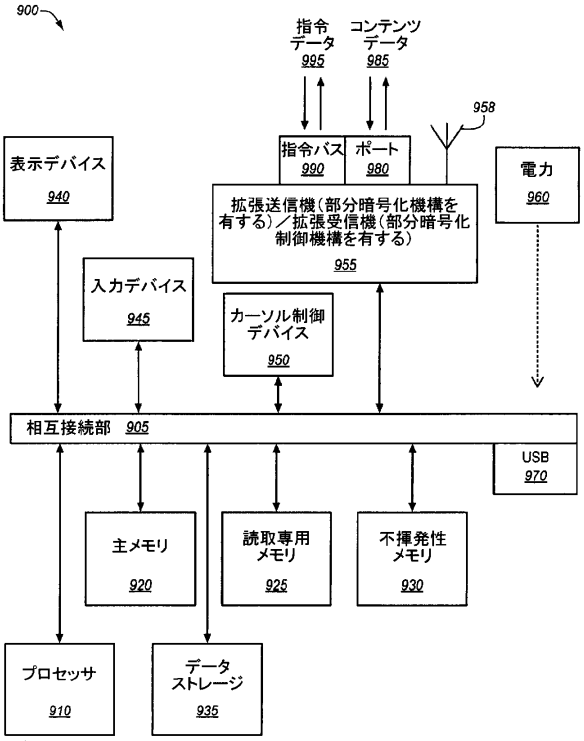
【図８】

FIG. 8



【図９】

FIG. 9



フロントページの続き

(72)発明者　アルトマン　ウィリアム　コンラッド
アメリカ合衆国　カリフォルニア州　９５１２４　サン　ホセ　フロビシャー　ウェイ　１７５９

審査官　松元　伸次

(56)参考文献　特開２００８－２５８６９７（ＪＰ，Ａ）
特表２００５－５１４８７３（ＪＰ，Ａ）

(58)調査した分野(Int.Cl.，ＤＢ名)
Ｇ０６Ｆ１２／１４
２１／１０
２１／６０－２１／８８
Ｇ０９Ｃ１／００－５／００
Ｈ０４Ｋ１／００－３／００
Ｈ０４Ｌ９／００－９／３８
Ｈ０４Ｎ７／００－７／１０
７／１４－７／１７３
７／２０－７／５６
２１／００－２１／８５８