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

特許第6055155号
(P6055155)

(45)発行日　平成28年12月27日(2016.12.27)　(24)登録日　平成28年12月9日(2016.12.9)

(51)Int.Cl.		F I	
G06F 21/54	(2013.01)	G06F	21/54
H04N 21/438	(2011.01)	H04N	21/438
H04N 21/443	(2011.01)	H04N	21/443
H04N 19/42	(2014.01)	H04N	19/42
G06F 21/71	(2013.01)	G06F	21/71

請求項の数 16　(全 18 頁)

(21)出願番号	特願2016-500518(P2016-500518)
(86)(22)出願日	平成26年2月28日(2014.2.28)
(65)公表番号	特表2016-517568(P2016-517568A)
(43)公表日	平成28年6月16日(2016.6.16)
(86)国際出願番号	PCT/US2014/019601
(87)国際公開番号	WO2014/149563
(87)国際公開日	平成26年9月25日(2014.9.25)
審査請求日	平成27年10月30日(2015.10.30)
(31)優先権主張番号	61/789,855
(32)優先日	平成25年3月15日(2013.3.15)
(33)優先権主張国	米国(US)
(31)優先権主張番号	14/192,782
(32)優先日	平成26年2月27日(2014.2.27)
(33)優先権主張国	米国(US)

(73)特許権者　310021766
株式会社ソニー・インタラクティブエンタテインメント
東京都港区港南１丁目７番１号
(74)代理人　100105924
弁理士　森下　賢樹
(72)発明者　ワン、ジェイソン　エヌ.
アメリカ合衆国、カリフォルニア州　９４４０４、サン　マテオ、ブリッジポイント　パークウェイ　２２０７、ソニー　コンピュータ　エンタテインメント　アメリカ内

最終頁に続く

(54)【発明の名称】ハードウェアデコーダアクセラレータのためのセキュリティ強度の向上

(57)【特許請求の範囲】

【請求項１】

プロセッサモジュール、メモリ及びハードウェアデコーダアクセラレータを有するシステム内で符号化したデジタルストリーミングデータの１つ以上のフレームを受信し、

前記ハードウェアデコーダアクセラレータを使用した前記符号化したデジタルストリーミングデータの前記フレームを１つ以上復号し、

ソフトウェアセキュリティレイヤを使用して、前記符号化したデジタルストリーミングデータの前記１つ以上のフレーム内に埋め込まれた悪意のあるデータによる前記ハードウェアデコーダアクセラレータの利用からシステムを保護することを含む方法。

【請求項２】

プロセッサモジュールと、

前記プロセッサに連結されたハードウェアデコーダアクセラレータと、

前記プロセッサに連結されたメモリを含むシステムであって、前記メモリが方法を実行するよう構成された実行可能な命令を含み、前記方法は、

前記システム内で符号化したデジタルストリーミングデータのフレームを１つ以上受信し、

前記ハードウェアデコーダアクセラレータを使用した符号化したデジタルストリーミングデータの前記フレームを１つ以上復号し、

ソフトウェアセキュリティレイヤを使用して、符号化したデジタルストリーミングデータの前記１つ以上のフレーム内に埋め込まれた悪意のあるデータによって、前記ハードウ

ェアデコーダアクセラレータの利用することから前記システムを保護することを含むシステム。
【請求項３】
前記ソフトウェアセキュリティレイヤが前記システムのファームウェア内に実装される、請求項２に記載のシステム。
【請求項４】
前記ソフトウェアセキュリティレイヤが前記システムのシステムソフトウェア中のカーネルドライバ内に実装される、請求項２に記載のシステム。
【請求項５】
前記ソフトウェアセキュリティレイヤが前記システムのシステムソフトウェア中のカーネルドライバ上部のソフトウェアレイヤ中に実装される、請求項２に記載のシステム。
【請求項６】
前記ソフトウェアセキュリティレイヤが、前記１つ以上のフレームを復号する際に使用される１つ以上のバッファの必要なサイズを計算し、範囲内のすべてのメモリが有効であるか確認するよう構成されている、請求項２に記載のシステム。
【請求項７】
前記ソフトウェアセキュリティレイヤが、一旦タスクが送信されると任意のユーザ処理アクセスから１つ以上の前記フレームを復号するのに使用される、１つ以上のバッファを保護するよう構成されている、請求項２に記載のシステム。
【請求項８】
前記ソフトウェアセキュリティレイヤがユーザメモリ空間から安全なメモリ空間へと前記１つ以上のバッファをコピーするよう構成されている、請求項７に記載のシステム。
【請求項９】
前記ソフトウェアセキュリティレイヤが、ユーザの処理によって書き込まれたデータ範囲内の１つ以上のメモリページをロックするよう構成されている、請求項７に記載のシステム。
【請求項１０】
前記ハードウェアデコーダアクセラレータが、マクロブロックよりも高いレベルで符号化したストリームを復号する場合、前記ストリームで符号化したパラメータに関連するバッファサイズが、ユーザの要求のこれらのパラメータに不一致であるため、前記ソフトウェアセキュリティレイヤが任意の入力したビットストリームを拒否する、請求項２に記載のシステム。
【請求項１１】
ソフトウェアセキュリティレイヤが、スライスの位置が現在のピクチャバウンダリ内にあるかをチェックし、スライスが前記現在のピクチャバウンダリ内でないと結論付けたときには前記スライスを破棄する、請求項２に記載のシステム。
【請求項１２】
前記１つ以上のフレーム内にあるそれぞれ符号化したマクロブロックに対して、前記ソフトウェアセキュリティレイヤが、前記１つ以上のフレーム内の所与のマクロブロックが、現在のピクチャバウンダリ内であるかチェックし、もし前記現在のピクチャバウンダリ内でない場合には、前記所与のマクロブロックを破棄する、請求項２に記載のシステム。
【請求項１３】
前記１つ以上のフレーム中のそれぞれのマクロブロックに対して、関連する同位置の参照マクロブロックヘッダが、参照マクロブロックヘッダバッファと一緒であるか前記ソフトウェアセキュリティレイヤがチェックし、前記参照マクロブロックヘッダバッファ内にない場合には、前記参照マクロブロックを破棄する、請求項２に記載のシステム。
【請求項１４】
前記ソフトウェアセキュリティレイヤが、前記１つ以上のフレーム内のマクロブロック内の動きベクトルが、参照ピクチャバウンダリ内であるかチェックし、前記動きベクトルが前記参照ピクチャバウンダリ内にない場合には、前記マクロブロックを破棄する、請求

項２に記載のシステム。
【請求項１５】
前記ソフトウェアセキュリティレイヤが、データが使用されるとき、前記１つ以上のフレーム内の前記データのデータ値のチェックを実行する、請求項２に記載のシステム。
【請求項１６】
方法を実行するよう構成されたコンピュータが読取り可能な命令をその中に埋め込まれた非一時的なコンピュータ可読媒体であって、前記方法が、
プロセッサモジュール、メモリ及びハードウェアデコーダアクセラレータを有するシステム内で符号化したデジタルストリーミングデータの１つ以上のフレームを受信し、
前記ハードウェアデコーダアクセラレータを使用した符号化したデジタルストリーミングデータの前記１つ以上のフレームを復号し、
ソフトウェアセキュリティレイヤを使用して、符号化したデジタルストリーミングデータの前記１つ以上のフレーム内に埋め込まれた悪意のあるデータによって、前記ハードウェアデコーダアクセラレータの利用することから前記システムを保護することを含むコンピュータ可読媒体。
【発明の詳細な説明】
【技術分野】
【０００１】
優先権の主張
本出願は、２０１３年3月１５日に出願されたＵＳ６１／７８９，８５５の優先権の利益を主張し、その開示内容全体が参照により本明細書に組み込まれる。
【０００２】
本出願は、２０１４年2月２７日に出願されたＵＳ１４／１９２，７８２の優先権の利益を主張し、その開示内容全体が参照により本明細書に組み込まれる。
【０００３】
本開示の態様は、圧縮デジタル信号の復号に関する。特に、本開示は、デコーダアクセラレータ用のセキュリティに関する。
【背景技術】
【０００４】
デジタル信号圧縮（ビデオコーディングまたはビデオエンコーディングと呼ばれることもある）は、多くのマルチメディアアプリケーションやデバイスにて広く使用されている。コーダ／デコーダ（コーデック）を使用したデジタル信号圧縮によって、オーディオまたはビデオ信号などのストリーミングメディアをインターネット上で送信したり、コンパクトディスクに保存することが可能になる。Ｈ．２６１、Ｈ．２６３、ＤＶ、ＭＰＥＧ－１、ＭＰＥＧ－２、ＭＰＥＧ－４、ＶＣ１、及びＡＶＣ（Ｈ．２６４）を含めて、多数の異なるデジタルビデオ圧縮規格が登場している。これらの規格ならびに他のビデオ圧縮技術は、ピクチャ及び連続するピクチャ内の空間的及び時間的冗長性を除去することによって、ビデオフレームピクチャを効率的に表現することを追求している。このような圧縮規格を使用することによって、ビデオコンテンツが高度に圧縮されたビデオビットストリームとなって伝送され、従って、効率良くディスクに保存する、またはネットワークを介して送信することができるようになる。
【０００５】
Ｈ．２６４としても知られるＭＰＥＧ－４ＡＶＣ（Ａｄｖａｎｃｅｄ　Ｖｉｄｅｏ　Ｃｏｄｉｎｇ）は、先行規格よりもはるかに高い圧縮率を提供するビデオ圧縮規格である。Ｈ．２６４規格は、以前のＭＰＥＧ－２規格の２倍までの圧縮を提供することが期待される。Ｈ．２６４規格はまた、知覚品質の向上を提供することが期待される。結果として、より多くのビデオコンテンツがＡＶＣ（Ｈ．２６４）で符号化されたストリームの形式で配信されている。２つのライバルＤＶＤフォーマットであるＨＤ－ＤＶＤフォーマットとブルーレイディスクフォーマットは、必須プレーヤー機能としてＨ．２６４／ＡＶＣハイプロファイルの復号をサポートする。ＡＶＣ（Ｈ．２６４）の符号化は、ＩＴＵ－Ｔ勧告

Ｈ．２６４、Ｈシリーズ：オーディオビジュアル及びマルチメディアシステム、オーディオビジュアルサービスのインフラ－動画の符号化、「オーディオビジュアルサービス全般のための高度ビデオ符号化方式」国際電気通信連合、電気通信標準化部門、ジュネーブ、スイス、２０１２年１月に詳細に記述され、その内容の全体はすべての目的において参考として本明細書に組み込まれている。

【０００６】

ビデオエンコーディングは、汎用コンピュータ上のソフトウェアで行うことができる。またはハードウェアビデオエンコーダと称される専用のハードウェアで行い得る。ハードウェアビデオエンコーダの使用は、システムのリソース使用を低くした状態で高性能のビデオ圧縮を達成する鍵と考えられている。

【発明の概要】

【発明が解決しようとする課題】

【０００７】

ハードウェアデコーダアクセラレータは、複数のユーザに共有されるシステムリソースである。典型的には、アクセラレータは、ユーザのプライベートメモリ、システムレジスタ及び場合によってはカーネルメモリにアクセスするために、通常のプロセス権限よりも高度の権限を有する。このためにアクセラレータはセキュリティ攻撃のためにありうるターゲットとなる。

【０００８】

本開示の態様が生じるのはこのような文脈の中である。

【図面の簡単な説明】

【０００９】

本開示の教示は、添付の図面と併せて、以下の詳細な説明を考慮すれば容易に理解できる。

【００１０】

【図１】本開示の態様による、ハードウェアビデオデコーダアクセラレータ及びアクセラレータ用のソフトウェアセキュリティレイヤを含んだシステムを使用する、コンピュータシステムのブロック図である。

【図２】本開示の態様による、セキュリティ強化の実行が可能であることを示すハードウェアアクセラレータの最上部にある、ソフトウェアスタックの一例を示すブロック図である。

【図３】本開示の態様のコンテキストにおけるストリーミングデータピクチャの１つの可能な分割を示す概略図である。

【図８】本開示の態様による、ハードウェアデコーダアクセラレータ及びソフトウェアセキュリティ強化レイヤを利用するシステムの一例の概略図である。

【発明を実施するための形態】

【００１１】

図面の説明

以下の詳細な説明には、説明のための多くの具体的な詳細事項が含まれるが、それらに対する多くの変更や修正も本発明の技術範囲に含まれることは、当業者であれば誰でも理解するであろう。したがって、以下に説明する本発明の例示的な実施形態は、クレームされた発明の普遍性をなんら損なうことなく、また限定も行うことなく記載されている。

【００１２】

本開示の態様は、アクセラレータが損傷した場合、ハードウェアデコーダアクセラレータが損傷しないよう保護し、損傷を最小限にするためのソフトウェアセキュリティ強化レイヤを目的とする。

【００１３】

序文

従来技術では、典型的には、ハードウェアデコーダアクセラレータは、個々のハードウェアデバイスベンダにより実装されてきた。製品の仕様により、それぞれのハードウェア

ベンダはセキュリティ機能を定め、ハードウェアの一部としてこれらのセキュリティ機能を実行する。例えば、多くのパーソナルコンピュータ（ＰＣ）のハードウェアベンダには、セキュリティ目標は、著作権のあるビデオコンテンツを保護することである。そのため、ハードウェアアクセラレータの大部分は、セキュリティ機能に関するコンテンツ保護を有する。

【００１４】

あるデバイスは異なるセキュリティ目標を有する。具体的には、あるゲーム機供給者にとっては、セキュリティ目標は、ゲーム機自体用のビデオコンテンツ及びシステムカーネルの双方を保護し得る。その結果、追加のソフトウェアレイヤでセキュリティ強化をする必要がある。

【００１５】

ハードウェアデコーダのセキュリティ強化に対する必要性は、コンピュータセキュリティの専門家には明白でない場合がある。コンピュータセキュリティの専門家の見地からすると、ハードウェアデコーダアクセラレータはビデオ信号処理のタスクを実行するのみであり、大変簡単なセキュリティ保護のみ必要とする。しかしながら、ビデオ処理の専門家の見地からすると、ハードウェアデコーダアクセラレータは、符号化されたビデオストリームに埋め込まれた命令を実行するよう構成されたプログラム可能なデバイスである。入力ビデオストリームを慎重に設計することにより、デコーダアクセラレータは何かを行うよう命令され得る。これはデバイスに有害なものを含む。したがって、セキュリティ保護を強化することは、ハードウェアデコーダアクセラレータを使用するある種のデバイスには必要である。

【００１６】

ある種の本開示の実施形態によると、デコーダアクセラレータのセキュリティの強化は、ソフトウェアセキュリティ強化レイヤによって実装され得る。例として、限定するものではないが、デコーダサービスダイモン、デコーダアクセラレータカーネルドライバまたはアクセラレータファームウェア内の、このようなソフトウェアレイヤは、ソフトウェアの一部として実装され得る。ハードウェアのブロックとしても実装され得る。あるセキュリティ保護では、ハードウェアビデオエンコーダアクセラレータを有するハードウェア内にも適用され得る。

【００１７】

発明の詳細な説明

図１に示されているように、コンピュータシステム１００は、中央処理装置（ＣＰＵ）１０２、統合ハードウェアビデオデコーダアクセラレータ１０４、及び１つ以上のプログラム可能なモジュール１０６を含み得る。アクセラレータ１０４は、符号化したビデオストリームを復号するよう構成されている。これらの符号化したビデオストリームは、Ｈ．２６４、ＭＰＥＧ２，ＭＰＥＧ４及びＶＣＩのような、ビデオ符号化規格に従い得る。ＣＰＵ１０２は、ハードウェアデコーダアクセラレータ１０４をあるシステムレジスタ１０８を通じて制御する。ＣＰＵ１０２及びアクセラレータ１０４は、共通のシステムメモリ１１０を共有する。所望により、ハードウェアデコーダアクセラレータ１０４はプログラム可能でもあり得る。デコーダの機能の一部は、ソフトウェアに実装することが可能であり、メモリ１１０内に保存した命令１１２として実装され得る。ハードウェアアクセラレータの性能をソフトウェアで増強することで、アクセラレータをよりフレキシブルにすることができる。しかしながら、そうすることでハッカーがアクセラレータ１０４を攻撃する機会をより与えてしまうことにもなる。これは、現在、市場のほとんどすべてのハードウェアデコーダアクセラレータがプログラム可能であるため、重大である。これを避けるためには、命令１１２はソフトウェアセキュリティレイヤ１１４を含むことができ、以下に論じるように構成され得る。

【００１８】

命令１１２は、ユーザソフトウェア、システムソフトウェア及びハードウェアレイヤを含むソフトウェアスタック内に実装され得る。図２は、セキュリティレイヤ１１４用のス

タック内での可能な位置を示すハードウェアアクセラレータ１０４の最上部で稼働しうる、典型的なソフトウェアスタック２００の一例を示す。図２に示すように、１つ以上のユーザアプリケーション２０２は、カーネルドライバ２０６に復号タスクをサブミットするために、ユーザランドライブラリ２０４でファンクションを呼び出し得る。ユーザアプリケーション２０２及びランドライブラリ２０４は、「ユーザソフトウェア」と称されるソフトウェアスタックの一部内にある。カーネルドライバ２０６は、オペレーティングシステムソフトウェアの一部である。カーネルドライバ２０６は、システムレジスタ１０８を介してハードウェアアクセラレータ１０４を動かす。

【００１９】

本開示の実施形態によると、セキュリティ強化レイヤ１１４は、ハードウェアレイヤ（例えば、ファームウェア）中、またはカーネルドライバ２０６中の追加のモジュールであり得る。あるいは、セキュリティ強化レイヤは、カーネルドライバ２０６の上にある、システムソフトウェアの追加部分であり得る。

【００２０】

図２に示すように、ユーザアプリケーションのみが、システムメモリ１１０内のユーザメモリ空間でメモリバッファ２０８にアクセス可能である。時として、ハードウェアアクセラレータ１０４は、ユーザのメモリ空間にアクセスすることができない。この場合、オペレーティングシステムソフトウェアは、ハードウェアアクセラレータ１０４用のシステムメモリ内で、ユーザのデータバッファ２０８をマップまたはコピー可能である。

【００２１】

セキュリティ強化レイヤ１１４がどのように動くのか理解するためには、ハードウェアアクセラレータ１０４がどのように動くのか、ハッカー及びその他のセキュリティ脅威に対していかに脆弱であるかを理解することが有用である。典型的には、ピクチャをハードウェアアクセラレータで復号する手順の概要は以下の通りであり得る。

【００２２】

ユーザアプリケーションは、ユーザメモリ空間中のメモリバッファにインプットしたビデオストリームを保存する。次に、オペレーティングシステムソフトウェアは、ハードウェアアクセラレータ１０４にユーザメモリバッファを開いてアクセスするか、またはオペレーティングシステムがユーザメモリバッファをハードウェアアクセラレータの可視メモリ空間にコピーする。時として、このハードウェアアクセラレータの可視メモリ空間は、カーネルメモリ空間である。

【００２３】

ユーザアプリケーション２０２は、ユーザランドライブラリ２０４内でファンクションを呼び出すことにより、復号したタスクを作成する。ビデオ復号タスクのコントロールパラメータは、実ハードウェアアクセラレータ１０４及びオペレーティングシステムに依存する。例えば、Ｍｉｃｒｏｓｏｆｔ　ＤＸＶＡは、ユーザアプリケーションがＷｉｎｄｏｗｓ（登録商標）のパソコンでハードウェアアクセラレータをどのように使用するのか定義する。

【００２４】

カーネルドライバ２０６は、ユーザの要求をシステムレジスタに書き込む。ハードウェアデコーダアクセラレータ１０４は、復号命令を受信し、インプットしたビデオストリームの一部を復号する。復号した結果は、ユーザ可視メモリバッファ２０８に保存される。ハードウェアアクセラレータ１０４はカーネルドライバ２０６に、タスクがシステムレジスタ１０８を介して終了したことを通知する。ユーザアプリケーション２０２は、カーネルドライバ２０６から復号したという通知及びハードウェアアクセラレータ１０４からデコーダ出力データを受信する。

【００２５】

上記のタスクを実行するためには、ハードウェアデコーダアクセラレータ１０４はある種の権限を有する。例えば、ハードウェアデコーダアクセラレータは、すべてのユーザのビデオ復号バッファを読み取り及び／または書き込むことができ得る。あるシステムでは

、デコーダはカーネルメモリ空間にアクセスし得る。ハードウェアデコーダアクセラレータは、あるシステムレジスタを読み取り及び／または書き込みすることも可能であり得る。あるシステムに加えて、ハードウェアアクセラレータ１０４がプログラム可能である場合には、プログラムの命令及びデータは、カーネルメモリ空間に保存される。

【００２６】

したがって、ハードウェアデコーダアクセラレータがハッカーによって損なわれた場合には、ハッカーはその他のデコーダアプリケーションからビデオコンテンツを盗み取ることができる可能性がある。例えば、ハッカーはブルーレイディスクの違法コピーを作成する可能性がある。さらに、ハッカーは侵害したデコーダアクセラレータを利用しシステムレジスタを読み取ることにより、暗号鍵などのシステムの機密を盗み得る。さらに、極端な場合には、侵害されたハードウェアデコーダアクセラレータは、システムカーネルを侵害し、ハッカーに全システム１００を乗っ取らせてしまう。

【００２７】

損傷の最小限化

システム１００は、ハードウェアデコーダアクセラレータ１０４が侵害された場合、損傷を最小限にするように構成し得る。このシステムの可能な構成の一つは、以下の通りである。

【００２８】

１．システム１００は、必要な場合にレジスタを読み込みまたは書き込む許可をハードウェアデコーダ１０４に与えるのみである。

２．ハードウェアアクセラレータがプログラム可能である場合、ハードウェアアクセラレータの命令及びデータは、カーネルメモリ空間及びユーザメモリ空間以外のメモリ空間に置くことが可能である。このようにして、ハードウェアアクセラレータ１０４は、命令を実行し、データを読み込み、メモリ空間に書き込むことが可能である。

３．もしユーザバッファがハードウェアデコーダのアクセスに開いている場合、バッファの必要な部分のみ開く。

【００２９】

設計によって制限されるが、すべてのハードウェアアクセラレータが上記の勧告に適合するとは限らない。例えば、ＰＣグラフィックカード内に統合されたハードウェアアクセラレータの大部分は、必要よりも多くのレジスタにアクセスすることができ、それに制約を課す可能性はない。したがって、ハードウェアアクセラレータをハッキングするのを困難にするために、追加の保護レイヤを実装する必要がある。

【００３０】

ビデオ復号

セキュリティソフトウェア１１４がいかに悪意のある攻撃からハードウェアデコーダアクセラレータを保護し得るのかを述べる前に、ビデオピクチャがどのように符号化するのかを理解することが有用である。一例として、限定するものではないが、図３に示すように、単一のピクチャ３００（例えば、デジタルビデオフレーム）は１以上のセクションに分解してもよい。本明細書で使用される用語「セクション」は、ピクチャ３００内の１以上のピクセルのグループを指すことができる。セクションはピクチャ内の単一のピクセルからピクチャ全体までの範囲とすることができる。セクションの限定しない例として、スライス３０２、マクロブロック３０４、サブマクロブロック３０６、ブロック３０８及び個々のピクセル３１０がある。図３に示すように、各スライス３０２は、マクロブロック３０４の１以上の行またはそのような１以上の行の部分を含む。ある行のマクロブロックの数は、マクロブロックのサイズとピクチャ３００のサイズ及び解像度に依存する。例えば、各マクロブロックに１６×１６ピクセルが含まれる場合、各行におけるマクロブロックの数は、ピクチャ３００の幅（ピクセル単位）を１６で割ることによって決定することができる。各マクロブロック３０４を一定数のサブマクロブロック３０６に分解してもよい。各サブマクロブロック３０６を一定数のブロック３０８に分解してもよく、各ブロックは一定数のピクセル３１０を含む。一例として、本発明を限定することなく、一般的な

ビデオ符号化方式では、各マクロブロック３０４は４つのサブマクロブロック３０６に分解される。各サブマクロブロックは４つのブロック３０８に分解され、各ブロックは、４×４配列の１６ピクセル３１０を含む。

【００３１】

なお、各ピクチャは、フレームまたはフィールドのいずれかであることに留意されたい。フレームは、完全な画像を指す。フィールドは、あるタイプのディスプレイデバイス上での画像の表示を容易にするために使用される画像の部分である。一般に、画像内のピクセルは、行単位に配置されている。表示を容易にするために、時には、ピクセルの行を交互に２つの異なるフィールドに置くことによって画像を分割することができる。そして、２つのフィールドのピクセルの行は、完全な画像を形成するためにインタレースされる。例えば、陰極線管（ＣＲＴ）ディスプレイなどのいくつかのディスプレイ装置では、２つのフィールドは単に、急速に連続して次々と表示される。蛍光体の残光または、ディスプレイ内のピクセルを点灯するのに使用されるその他の光を発する要素は、映像結果の持続性と組み合わされた結果、２つのフィールドが連続した画像として認識される。液晶ディスプレイなどのある表示装置については、表示する前に、単一のピクチャに２つのフィールドをインタレースする必要があるかもしれない。符号化された画像を表すストリーミングデータは、典型的には画像がフィールドであるかフレームであるかを示す情報を含む。このような情報は、画像に対するヘッダに含まれてもよい。

【００３２】

図４は、本開示の態様と関連して使用される、ストリーミングデータ４０１を復号する方法４００における可能な処理フローの一例を示す。この特定の例は、たとえばＡＶＣ（Ｈ．２６４）規格を使用したビデオ復号の処理フローを示す。符号化されたストリーミングデータ４０１は、最初にバッファに保存される。符号化されたストリーミングデータ４０１（例えば、ビデオデータビットストリーム）がネットワーク、例えば、インターネットで転送された場合、データ４０１は、符号４０２で示されるように、最初はネットワーク抽象化レイヤ（ＮＡＬ）復号と呼ばれる処理を経る。ＮＡＬ復号は、データを送信する際に補助するために追加された情報をデータ４０１から除去する。「ネットワークラッパー」と呼ばれるこのような情報は、データ４０１をビデオデータとして特定する、もしくはビットストリームの先頭または末尾、データの配置のビット、及び／またはビデオデータ自体に関するメタデータを示す。

【００３３】

また、例示的に、ネットワークラッパーは、スライスの開始または終了を示すデータなど、低レベルの復号に使用される情報に加えて、例えば、解像度、画像表示形式、データを表示するためのカラーパレット変換行列、各ピクチャのビット数に関する情報、スライスやマクロブロックに関する情報を含むデータ４０１に関する情報を含んでいてもよい。この情報は、単一のセクション内のタスクグループの各々に渡すべきマクロブロックの数を決定するために使用され得る。その複雑さのため、ＮＡＬ復号は、典型的にはピクチャとスライスのレベルで行われる。ＮＡＬ復号に対して使用される最小ＮＡＬバッファは、通常スライスのサイズのものである。

【００３４】

いくつかの実施の形態では、符号４０２におけるＮＡＬ復号後、図４で説明される残りの復号は、ここではビデオ符号化レイヤ（ＶＣＬ）復号４０４、動きベクトル（ＭＶ）再構築４１０及びピクチャ再構築４１４と呼ばれる３つの異なるスレッドグループまたはタスクグループにおいて実施される。ピクチャ再構築タスクグループ４１４は、ピクセル予測及び再構築４１６と後処理４２０を含み得る。本発明のいくつかの実施形態において、これらのタスクグループは、データ依存性に基づいて選択され、その結果、後続の処理のためにマクロブロックが次のタスクグループに送信される前に、各タスクグループがピクチャ（例えば、フレームまたはフィールド）またはセクション内のすべてのマクロブロックの処理を完了できるようになる。

【００３５】

特定のコーディング規約は、空間領域から周波数領域へのピクセル情報の変換を伴うデータ圧縮の形式を使用してもよい。そのような変換は、特に、離散コサイン変換（ＤＣＴ）として知られている。このような圧縮データの復号処理は、周波数領域から空間領域に戻す逆変換を伴う。ＤＣＴを使用して圧縮されたデータの場合、逆変換は逆離散コサイン変換（ＩＤＣＴ）として知られている。変換されたデータは、時々、離散変換されたデータの数値を表すのに使用されるビット数を減らすために量子化される。例えば、番号１、２、３を全て２にマッピングし、数字４，５，６を全て５にマッピングしてもよい。データを解凍するためには、周波数領域から空間領域への逆変換を行う前に逆量子化（ＩＱ）として知られる処理が用いられる。ＶＣＬ　ＩＱ／ＩＤＣＴ復号処理４０４のデータ依存関係は、典型的には、同じスライス内のマクロブロックに対するマクロブロックレベルにある。従ってＶＣＬ復号処理３０４によって生成される結果をマクロブロックレベルでバッファリングしてもよい。

【００３６】

ＶＣＬ復号４０４は、多くの場合、ＶＣＬ構文を復号するために使用されるエントロピー復号４０６と呼ばれる処理を含む。ＡＶＣ（Ｈ．２６４）のような多くのコーデックは、エントロピー符号化と呼ばれる符号化レイヤを使用する。エントロピー符号化は、符号長が信号の確率に一致するように、信号に符号を割り当てる符号化方式である。典型的には、エントロピーエンコーダは、等しい長さの符号で表されるシンボルを、確率の負の対数に比例した符号で表されるシンボルで置き換えることによってデータを圧縮するために使用される。ＡＶＣ（Ｈ．２６４）は、２つのエントロピー符号化方式、コンテキスト適応可変長符号化（ＣＡＶＬＣ）、及びコンテキスト適応バイナリ算術符号化（ＣＡＢＡＣ）をサポートする。ＣＡＢＡＣはＣＡＶＬＣよりも約１０％以上の圧縮を提供する傾向があるため、ＣＡＢＡＣは、ＡＶＣ（Ｈ．２６４）ビットストリームを生成する際に多くのビデオエンコーダで好んで利用されている。ＡＶＣ（Ｈ．２６４）符号化されたデータストリームのエントロピーレイヤを復号することは計算量が大きくなるため、汎用マイクロプロセッサを使用してＡＶＣ（Ｈ．２６４）符号化されたビットストリームを復号する装置に対しては困難な課題があるであろう。このような理由から、多くのシステムはハードウェアデコーダアクセラレータを使用している。

【００３７】

エントロピー復号４０６に加えて、ＶＣＬ復号処理４０４は、符号４０８で示すように逆量子化（ＩＱ）及び／または逆離散コサイン変換（ＩＤＣＴ）を含み得る。これらの処理は、ヘッダ４０９とマクロブロックからのデータを復号する。復号されたヘッダ４０９は、隣接マクロブロックのＶＣＬ復号を補助するために用いられ得る。

【００３８】

ＶＣＬ復号４０４は、マクロブロックレベルのデータ依存頻度で実施され得る。具体的には、同じスライス内の異なるマクロブロックが並列にＶＣＬ復号を受け、その結果は、さらなる処理のために動きベクトル再構成タスクグループ４１０に送信され得る。

【００３９】

続いて、ピクチャまたはセクション内のすべてのマクロブロックは、動きベクトル再構築４１０を受け得る。ＭＶ再構築処理４１０は、所与のマクロブロック４１１及び／または同位置のマクロブロックヘッダ４１３からのヘッダを用いた動きベクトル再構築４１２を含み得る。動きベクトルは、ピクチャ内で明白な動きを表す。このような動きベクトルは、以前のピクチャのピクセルとピクチャからピクチャへのそれらのピクセルの相対運動の知識に基づいたピクチャ（またはその一部）の再構築を可能にする。いったん動きベクトルが回復されると、ピクセルは、符号４１６において、ＶＣＬ復号処理４０４からの残留ピクセルとＭＶ再構築処理４１０からの動きベクトルに基づいたプロセスを使用して再構築することができる。ＭＶに対するデータ依存頻度（及び並列処理のレベル）は、ＭＶ再構築処理４１０が他のピクチャからの同位置のマクロブロックに関係するかどうかに依存する。他のピクチャからの同位置のＭＢヘッダに関係しないＭＶ再構築に対しては、ＭＶ再構築処理４１０は、スライスレベルまたはピクチャレベルで並列に実装することがで

きる。同位置のＭＢヘッダに関係するＭＶ再構築に対しては、データ依存頻度はピクチャレベルであり、ＭＶ再構築処理４１０はスライスレベルで並列処理を実装することができる。

【００４０】

動きベクトル再構築４１０の結果は、ピクチャの頻度レベルで並列化することができるピクチャ再構築タスクグループ４１４に送られる。ピクチャ再構築タスクグループ４１４内では、ピクチャまたはセクション内のすべてのマクロブロックは、デブロッキング４２０と併せてピクセル予測及び再構築４１６を受け得る。ピクセル予測及び再構成タスク４１６とデブロッキングタスク４２０は復号効率を高めるために並列化することができる。これらのタスクは、データ依存関係に基づいて、マクロブロックレベルでピクチャ再構築タスクグループ４１４内で並列化され得る。例えば、ピクセル予測及び再構築４１６は１つのマクロブロックに対して行われ、デブロッキング４２０がその後に続く。デブロッキング４２０により得られた復号されたピクチャからの参照ピクセルは、後続のマクロブロック上のピクセル予測及び再構築４１６で使用され得る。ピクセル予測及び再構築４１８は復号されたセクション４１９（例えば、復号されたブロックまたはマクロブロック）を生成する。セクション４１９は、後続のマクロブロックに対するピクセル予測及び再構築処理４１８への入力として使用される近傍ピクセルを含む。ピクセル予測と再構築４１６に対するデータ依存関係のゆえに、同じスライス内のマクロブロックに対するマクロレベルでの並列処理がある程度可能になる。

【００４１】

ブロック符号化技術が使用されるブロック間で形成される鋭いエッジを平滑化することによって画質と予測性能を向上させるために、後処理タスクグループ４２０は、復号されたセクション４１９内のブロックに適用されるデブロッキングフィルタ４２２を含み得る。デブロッキングフィルタ４２２は、得られたデブロックされたセクション４２４の外観を改善するために使用することができる。

【００４２】

復号化されたセクション４１９またはデブロックされたセクション４２４は、隣接マクロブロックをデブロッキングする際に使用するための隣接ピクセルを提供し得る。さらに、現在復号中のピクチャからのセクションを含む復号されたセクション４１９は、後続のマクロブロックに対するピクセル予測及び再構築４１８のための参照ピクセルを提供し得る。ピクチャ（またはそのサブセクション）がインター符号化であるかイントラ符号化であるかにかかわらず、現在のピクチャ内からのピクセルが上述したように同じ現在のピクチャ内のピクセル予測のために任意に使用されるのは、この段階である。デブロッキング４２０は、同じピクチャ内のマクロブロックに対してマクロブロックレベルで並列化することができる。

【００４３】

後処理４２０の前に生成した復号されたセクション４１９及び後処理されたセクション４２４は、同じバッファ、たとえば、関係した特定のコーデックに応じた出力ピクチャバッファに保存され得る。なお、デブロッキングは、Ｈ．２６４における後処理フィルタであることに留意されたい。Ｈ．２６４は、デブロッキング前のマクロブロックを、隣接するマクロブロックのイントラ予測と、未来のピクチャマクロブロックのインター予測に対するデブロッキング後のマクロブロックの参照として、使用するからである。デブロッキング前とデブロッキング後の両方のピクセルが予測に用いられるため、デコーダまたはエンコーダは、デブロッキング前のマクロブロックとデブロッキング後のマクロブロックの両方をバッファリングする必要がある。たいていの低コストの民生用アプリケーションでは、メモリ使用量を減らすために、デブロッキング前のピクチャとデブロッキング後のピクチャは同じバッファを共有する。ＭＰＥＧ２またはＭＰＥＧ４　ｐａｒｔ　１０（注：Ｈ．２６４もＭＰＥＧ４パート１０と呼ばれる）を除くＭＰＥＧ４などの以前のＨ．２６４規格に対しては、後処理の前のマクロブロック（例えば、デブロッキング前のマクロブロック）だけが、他のマクロブロックの予測のための参照として使用される。そのような

コーデックでは、フィルタ処理前のピクチャは、フィルタ処理後のピクチャと同じバッファを共有しなくてよい。

【００４４】

したがって、Ｈ．２６４に対しては、ピクセル復号の後、復号化されたセクション４１９は、出力ピクチャバッファに保存される。その後、後処理されたセクション４２４は、出力ピクチャバッファにある復号化されたセクション４１９を置き換える。非Ｈ．２６４の場合は、デコーダは出力ピクチャバッファに復号化されたセクション４１９を保存するだけである。後処理は、表示時に行われており、後処理の出力はデコーダ出力ピクチャバッファと同じバッファを共有することはない。

【００４５】

少なくとも復号処理４００の一部のいくつかは、ハードウェアデコーダ１０４上で実施され得る。ハッカーが悪質なコードまたはデータを、システム１００によって受信された符号化されたストリーミングデータ４０１に挿入することが可能である。このような悪質なコードまたはデータは、ハードウェアデコーダ１０４を権限なく使用することによってシステムを攻撃するために使用され得る。ハードウェアデコーダアクセラレータのセキュリティレイヤ１１４は、ハードウェアデコーダ１０４をこのような悪意のある攻撃から保護するよう構成されることが可能である。

【００４６】

ハードウェアデコーダの保護

ハードウェアアクセラレータ１０４を保護するためには、ユーザアプリケーション２０２及びアクセラレータ１０４のインターフェースは、十分なメモリアクセス情報を伝送しなければならない。ユーザアプリケーション２０２がハードウェアデコーダアクセラレータ１０４に要求をサブミットする場合、その要求は、デコーダ１０４によってアクセスされたすべてのユーザバッファ２０８のアドレスを伝送しなければならない。また、ハードウェアアクセラレータ１０４のメモリ使用量を計算するために必要な、すべての情報を伝送する必要がある。異なるコーディング規約用にハードウェアアクセラレータ１０４によって使用される、このようなバッファのいくつかの例は、下記の表１中にて示す。

【００４７】

【表１】

表Ｉ

	ビデオビットストリーム	参照ピクセル	参照マクロブロックヘッダ	復号されたピクセル	テンポラルマクロブロック	テンポラルループフィルタ	ビット平面
Ｈ．２６４	あり	あり	あり	あり	可能	可能	なし
ＭＰＥＧ２	あり	あり	なし	あり	可能	なし	なし
ＭＰＥＧ４	あり	あり	あり	あり	可能	なし	なし
ＶＣ１	あり	あり	あり	あり	可能	可能	可能

【００４８】

現在のビデオ符号化規格としては、これらのバッファサイズに関する情報は、マクロブロックレベルより上のビデオストリームで符号化される。表ＩＩは、バッファサイズの情報が異なるビデオ規格にあわせてストリーム中でいかに符号化されるのかを示す。

【００４９】

【表２】

表ＩＩ

スタンダード	バッファ名：ビデオビットストリームサイズ
全スタンダード	ビデオエレメンタリストリーム上部のレイヤで符号化される。またはビデオエレメンタリストリーム中のスタートコード間のバイト数
	バッファ名：参照ピクセルバッファサイズ
ＡＶＣ	インプットしたストリームプロフィール、レベル、最大ＤＥＣフレームバッファリング及びフレーム解像度
ＭＰＥＧ２	プロフィール及びフレーム解像度
ＭＰＥＧ４	プロフィール及びフレーム解像度
ＶＣ１	プロフィール及びフレーム解像度
	バッファ名：参照マクロブロックヘッダバッファサイズ
ＡＶＣ	インプットしたストリームプロフィール、レベル、最大ＤＥＣフレームバッファリング及びフレーム解像度
ＶＣＬ	プロフィール及びフレーム解像度
	バッファ名：復号したピクセルバッファ、マクロブロック中間データバッファ、参照マクロブロックヘッダバッファ、ループフィルタ中間データバッファ及びビット平面バッファサイズ
全スタンダード	フレーム解像度及カレントピクチャのフレーム／フィールドフラッグ

【００５０】

ユーザの要求を受信後、デコーダ保護レイヤ１１４は、各バッファの必要サイズを計算し、範囲内のすべてのメモリが有効であるか確かめる。セキュリティをより強固にするため、ユーザはメッセージを要求し、一旦、タスクがサブミットされたら、任意のユーザ処理アクセスから、ビデオストリームバッファ及び復号したピクセルバッファ以外の、表ＩＩのすべてのバッファが保護されるべきである。さもなければ、その要求が確認された後、ハッカーは有効な要求を無効な要求に置き換える機会を有するかも知れず、ハッカーは、アクセラレータがこれらのバッファを処理している間に、これらのデータバッファ中のコンテンツを変更する可能性がある。

【００５１】

これらのバッファを悪意のある使用から守る、可能な方法のいくつかの例には、下記のものが含まれるがこれらに限定されない。

【００５２】

１．バッファをユーザメモリ空間から安全なメモリ空間へとコピーする。

２．データ範囲内のメモリページをロックし、ユーザ処理によって書き込みできないようにする。注：バッファサイズは、タスクの要求をサブミットするユーザアプリケーションのメモリ使用量情報により計算される。

【００５３】

通常は、復号したピクセルバッファは、アクセラレータ１０４に「読取りのみ」である。したがって、通常はこのバッファを保護する必要はない。一般的にいくつかの理由から、ビデオストリームバッファを保護するのは実用的ではないと思われる。第１に、このバッファのサイズは、非常に大きく、このバッファ内のすべてのデータをもう一つのメモリ空間にコピーするのは実用的ではないと思われるからである。第二に、ユーザアプリケー

ションは、他のピクチャのために、まだビットストリームバッファで動いている可能性がある。符号化したピクチャサイズは予想ができない。ピクチャバウンダリをメモリページバウンダリの境界に並べるのは困難である。したがって、あるページをロックしてバッファにユーザアクセスをさせないのは実用的ではない。

【００５４】

ハードウェアアクセラレータ１０４が、マクロブロックレベルよりも高く符号化したストリームを復号する場合、ストリーム４０１で符号化したパラメータに関連するバッファサイズが、ユーザの要求のこれらのパラメータに不一致であるため、保護レイヤ１１４は任意の入力したビットストリームを拒否し得る。これはハードウェアデコーダアクセラレータ１０４をバッファオーバフロー攻撃から保護する。

【００５５】

各符号化したスライス中のすべてのビデオ符号化規格のため、スライスヘッダはスライスの開始位置を示す情報を伝送する。ある実装においては、デコーダ保護レイヤ１１４は、スライス位置が現在のピクチャバウンダリ内であるかチェックし得る。もしスライスが現在のピクチャバウンダリ内でないと結論付けた場合、このスライスは悪質なコードまたは悪質なデータを含んでいる可能性があるため破棄されるべきである。

【００５６】

さらに、それぞれの符号化したマクロブロックのため、保護レイヤ１１４は、現在のマクロブロックが現在のピクチャバウンダリ内であるかをチェックし、現在のマクロブロックが現在のピクチャバウンダリの範囲外である場合、この保護レイヤ１１４はこのマクロブロックを破棄し得る。

【００５７】

Ｈ．２６４、ＭＰＥＧ４またはＶＣ１ストリーム復号の場合には、各マクロブロックのため、保護レイヤ１１４は、関連した同位置の参照マクロブロックヘッダが参照マクロブロックヘッダバッファと一緒であるかチェックし得る。もし参照マクロブロックヘッダバッファ内になければ、このマクロブロックは破棄するべきである。

【００５８】

ＭＰＥＧ２ストリーム復号の場合には、保護レイヤ１１４は、動きベクトルが参照ピクチャバウンダリ内にあるかチェックするべきである。もし参照ピクチャバウンダリ内になければ、このマクロブロックは破棄するべきである。

【００５９】

上述したように、インプットしたストリームバッファを保護するのは困難なため、すべてのビットストリームは上記をチェックするため、データ値はデータが使用されるときにチェックするべきであることに留意する。さもなければ、ハッカーは、アクセラレータがデータを確かめる時間とデータを使用する時間との間に、ビットストリームコンテンツを変える機会を有するだろう。

【００６０】

いくつかの特別な保護ケース

すべてのハードウェアが、ユーザ処理アクセスからある種のバッファをロックする能力を有するとは限らない。例えば、ユーザアプリケーションがマクロブロック中間データバッファにアクセスが可能な場合、ハッカーはアクセラレータに命令して、動きベクトルまたは参照ピクセルを参照してシステムの機密情報を読み取りバッファ内のコンテンツを変更することができる。したがって、マクロブロック中間データバッファ及び参照マクロブロックヘッダバッファのコンテンツによっては、あるメモリアクセス操作のために更なる保護が加えられるべきである。以下は、これらの追加の保護を実装することができる推奨の最良の方法のいくつかの例である。

【００６１】

１．すべてのビデオの規格のため、動きベクトルがマクロブロック中間データバッファに保存される場合には、アクセラレータは参照ピクセル指数の前に、各動きベクトルをチェックしなければならない。

２．Ｈ．２６４及びＶＣＬストリームのため、同位置のマクロブロック動きベクトルが参照マクロブロックヘッダバッファに保存される場合、アクセラレータセキュリティレイヤ１１４は各参照ピクセル指数の前に動きベクトル参照ＩＤをチェックしなければならない。

３．Ｈ．２６４、ＭＰＥＧ４及びＶＣ１ストリームのため、隣接するマクロブロックバリッドフラグがマクロブロック中間データバッファに保存される場合、アクセラレータセキュリティレイヤ１１４は、隣接するマクロブロックが、任意の隣接するマクロブロックがアクセスする前に、現在のピクチャバウンダリ内であるかチェックしなければならない。

【００６２】

本開示の態様には、上記の様々な種類のハードウェアデコーダアクセラレータセキュリティレイヤを実装するよう構成されたシステムが含まれる。一例として、限定するものではないが、図５は、本開示の態様に係るビデオ符号化を実装するために用いられるコンピュータシステム５００のブロック図を示す。システム５００は一般に、メインのプロセッサモジュール５０１、メモリ５０２及びハードウェアデコーダ５０５を含み得る。プロセッサモジュール５０１には、例えば、シングルコア、デュアルコア、クアドコア、プロセッサ－コプロセッサ、セルプロセッサ、アーキテクチャなどの１つ以上のプロセッサコアを含み得る。

【００６３】

メモリ５０２は、例えば、ＲＡＭ、ＤＲＡＭ、ＲＯＭなどの集積回路の形態を取ってもよい。そのメモリはまた、プロセッサモジュール５０１内のすべてのプロセッサコアによってアクセス可能なメインメモリであってもよい。いくつかの実施形態では、プロセッサモジュール５０１は、１つ以上のプロセッサコアまたは１つ以上のコプロセッサに関連するローカルメモリを有し得る。ソフトウェアコーダプログラム５０３は、プロセッサモジュール５０１上で実行することができるプロセッサ読み取り可能な命令の形態でメインメモリ５０２に保存されてもよい。コーダプログラム５０３は、例えば、前述したように、ピクチャをハードウェアデコーダアクセラレータ５０５とともに圧縮したシグナルデータに復号するよう構成し得る。ハードウェアデコーダアクセラレータのセキュリティレイヤ５０３Ａは、メモリ５０２内に保存し、プロセッサモジュール５０１上で実行される。セキュリティレイヤ５０３Ａは、上述のように、ハードウェアコーダアクセラレータのために追加のセキュリティを実装するよう構成されている。コーダプログラム５０３及びハードウェアデコーダアクセラレータセキュリティレイヤ５０３Ａは、任意の適切なプロセッサ読み取り可能な言語、たとえば、Ｃ、Ｃ＋＋、ＪＡＶＡ（登録商標）、アセンブリ、ＭＡＴＬＡＢ、フォートラン、及び他の様々な言語で書かれ得る。

【００６４】

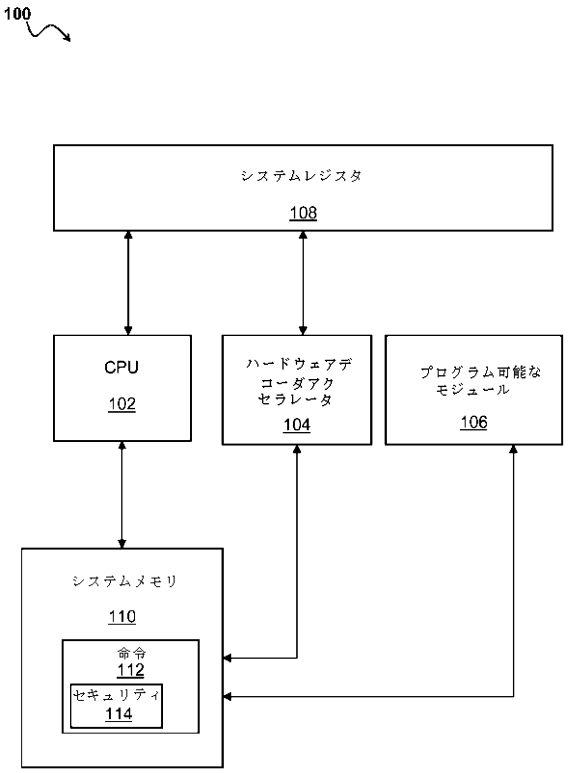
入力データ５０７はメモリ５０２に保存されてもよい。コーダプログラム５０３及び／またはセキュリティレイヤ５０３Ａの実行中、プログラムコード及び／またはデータ５０７の一部は、メモリ５０２またはプロセッサ５０１に対するプロセッサコアのローカルストアにロードされる。一例であり、限定しないが、入力データ８０７は、符号化／復号前または符号化／復号の中間段階におけるビデオピクチャまたはそのセクションを含み得る。符号化の場合、データ５０７は、バッファされたストリーミングデータの一部、たとえば、未符号化ビデオピクチャまたはそのセクションを含み得る。復号の場合、データ５０７は、未復号のセクション、復号されたが後処理がなされていないセクション、及び復号され後処理がなされたセクションの形式の入力データを含み得る。そのような入力データは、１つ以上のデジタルピクチャの１つ以上の符号化されたセクションを表すデータを有するデータパケットを含んでもよい。一例として、限定するものではないが、そのようなデータパケットは、変換係数の集合及び予測パラメータの部分集合を含んでもよい。これらの様々なセクションは１以上のバッファに保存されてもよい。特に、復号され、及び／または、後処理されたセクションは、メモリ５０２に実装された出力ピクチャバッファに保存されてもよい。

【００６５】
システム５００はさらに、入出力（Ｉ／Ｏ）要素５１１、電源（Ｐ／Ｓ）５１２、クロック（ＣＬＫ）５１３及びキャッシュ５１４などの周知のサポート機能５１０を含み得る。装置５００は任意に、プログラム及び／またはデータを保存するためのディスクドライブ、ＣＤ－ＲＯＭドライブ、テープドライブなどの大容量記憶装置５１５を備えてもよい。装置８００はまた、任意に、装置５００とユーザの相互作用を容易にするために、ディスプレイユニット５１６及びユーザインタフェースユニット５１８を含み得る。ディスプレイユニット５１６は、テキスト、数値、グラフィカルシンボルや画像を表示する陰極線管（ＣＲＴ）、またはフラットパネルスクリーンの形態であってもよい。ユーザインタフェース５１８は、キーボード、マウス、ジョイスティック、ライトペンや他の装置を含んでもよく、これらは、グラフィカルユーザインタフェース（ＧＵＩ）と併せて使われてもよい。装置５００はまた、ネットワークインターフェース５２０を含み、これにより、当該装置がインターネットのようなネットワーク５２２上で他の装置と通信することが可能になる。システム５００は、ネットワークインターフェース５２０を介して、ネットワーク５２２に接続されたその他の装置から、符号化したストリーミングデータ（例えば、１つ以上の符号化したビデオフレーム）のフレームを１つ以上受信し得る。これらの構成要素はハードウェア、ソフトウェア、ファームウェアまたはこれらの２以上の組み合わせによって実装される。

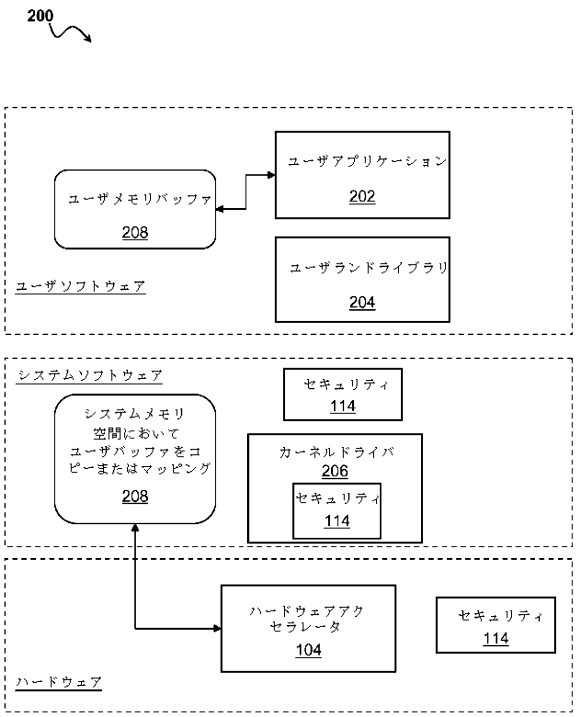
【００６６】
本開示の態様は、ハードウェアデコーダアクセラレータのセキュリティレイヤ５０３Ａの使用を通じて、システム５００上での悪意のある攻撃に対する追加の保護を提供する。

【００６７】
本発明の好ましい実施の形態を完全な形で説明してきたが、いろいろな代替物、変形、等価物を用いることができる。したがって、本発明の範囲は、上記の説明を参照して決められるものではなく、請求項により決められるべきであり、均等物の全範囲も含まれる。ここで述べた特徴はいずれも、好ましいかどうかを問わず、本明細書で記載される他の特徴と組み合わせてもよい。下記の請求項において、明示的に断らない限り、各項目は１またはそれ以上の数量である。請求項において「～のための手段」のような語句を用いて明示的に記載する場合を除いて、請求項がミーンズ・プラス・ファンクションの限定を含むものと解してはならない。

【図１】



【図２】



【図３】

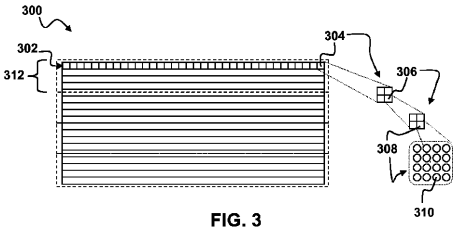
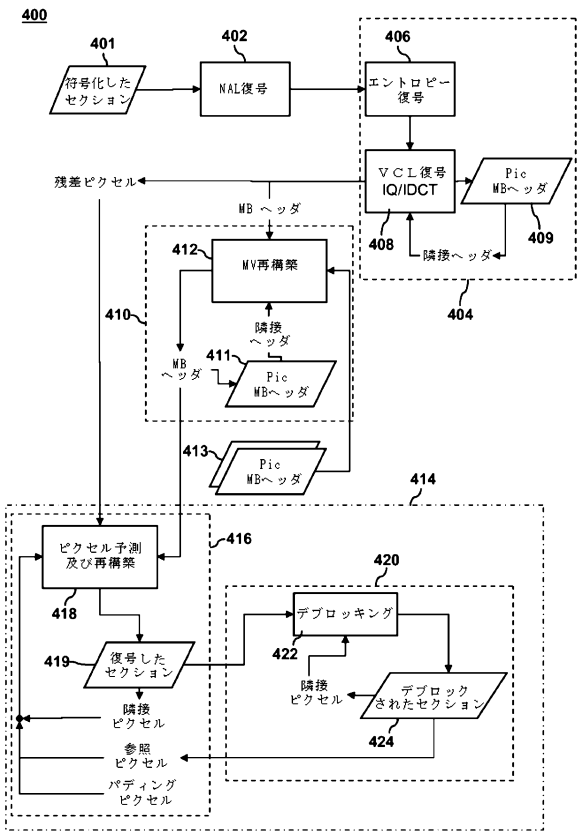
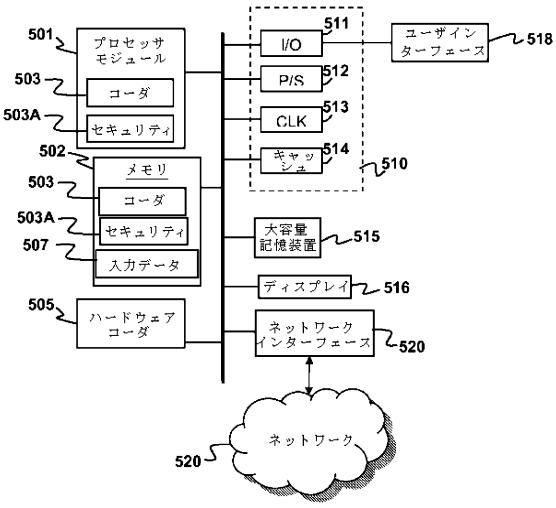


FIG. 3

【図４】



【図５】


500
501
プロセッサモジュール
503
コーダ
503A
セキュリティ
502
メモリ
503
コーダ
503A
セキュリティ
507
入力データ
505
ハードウェアコーダ
511
I/O
512
P/S
513
CLK
514
キャッシュ
510
518
ユーザインターフェース
515
大容量記憶装置
516
ディスプレイ
520
ネットワークインターフェース
520
ネットワーク

フロントページの続き

(72)発明者　フアン、チェン
アメリカ合衆国、カリフォルニア州　９４４０４、サン　マテオ、ブリッジポイント　パークウェイ　２２０７、ソニー　コンピュータ　エンタテインメント　アメリカ内

審査官　岸野　徹

(56)参考文献　特表２００９－５３３０００（ＪＰ，Ａ）
特表２０１２－５０８４８５（ＪＰ，Ａ）
米国特許出願公開第２００８／００１０５３８（ＵＳ，Ａ１）
特表２００８－５３７４２７（ＪＰ，Ａ）
特開２０００－１２４８９４（ＪＰ，Ａ）
特開２００２－０４４６５８（ＪＰ，Ａ）

(58)調査した分野(Int.Cl.，ＤＢ名)
Ｇ０６Ｆ　２１／５４
Ｇ０６Ｆ　２１／７１
Ｈ０４Ｎ　１９／４２
Ｈ０４Ｎ　２１／４３８
Ｈ０４Ｎ　２１／４４３