

(19)日本国特許庁(JP)

(12)特許公報(B2)

(11)特許番号

特許第7221391号

(P7221391)

(45)発行日 令和5年2月13日(2023.2.13)

(24)登録日 令和5年2月3日(2023.2.3)

(51)国際特許分類

F I

G 0 6 F 21/62 (2013.01)

G 0 6 F 21/62

請求項の数 20 (全13頁)

(21)出願番号	特願2021-531810(P2021-531810)	(73)特許権者	508301087
(86)(22)出願日	令和1年12月16日(2019.12.16)		エーティーアイ・テクノロジーズ・ユー
(65)公表番号	特表2022-512122(P2022-512122		エルシー
	A)		ATI TECHNOLOGIES ULC
(43)公表日	令和4年2月2日(2022.2.2)		カナダ、オンタリオ エル3ティー 7
(86)国際出願番号	PCT/US2019/066615		エックス6、マーカム、コマス パリー
(87)国際公開番号	WO2020/131742		ドライブ イースト 1
(87)国際公開日	令和2年6月25日(2020.6.25)		One Commerce Valley
審査請求日	令和4年11月28日(2022.11.28)		Drive East, Markham
(31)優先権主張番号	16/228,349		, Ontario, L3T 7X6 C
(32)優先日	平成30年12月20日(2018.12.20)		anada
(33)優先権主張国・地域又は機関	米国(US)	(73)特許権者	591016172
早期審査対象出願			アドバンスト・マイクロ・デバイスズ
			・インコーポレイテッド
			ADVANCED MICRO DEVI
			最終頁に続く

(54)【発明の名称】 安全なコンピュータビジョン処理

(57)【特許請求の範囲】

【請求項1】

画像クラスタのコンピュータビジョンプロセッサにおいて、信頼メモリ領域(TMR)の一部に記憶された画像データへのアクセスを制御するフェンスメモリ領域(FMR)を定義することと、

前記コンピュータビジョンプロセッサにおいて、処理クラスタに実装された信頼できないアプリケーションから、前記TMRの前記一部の前記画像データにアクセスするためのFMR要求を受信することと、

前記コンピュータビジョンプロセッサにおいて、前記FMRが開いている場合に前記FMR要求を受信したことに応じて、前記信頼できないアプリケーションが前記画像データにアクセスすることを可能にすることと、を含む、

方法。

【請求項2】

前記コンピュータビジョンプロセッサを用いて、前記画像データを取得し、前記画像データを前記TMRの前記一部に記憶することをさらに含む、

請求項1の方法。

【請求項3】

前記TMRの前記一部へのアクセスを制御する前記FMRを定義することは、前記画像データを記憶するバッファのセットを前記TMR内に定義することを含む、

請求項1の方法。

10

20

【請求項 4】

前記コンピュータビジョンプロセッサにおいて、前記 FMR を開くことをさらに含む、請求項 1 の方法。

【請求項 5】

前記 FMR を開くことは、前記 FMR が開いていることを示す情報をセキュリティプロセッサに提供することを含み、前記セキュリティプロセッサは、前記画像クラスタと信頼関係を有しており、前記 FMR 要求を受信することは、前記 FMR が開いている間、前記 FMR 要求を前記セキュリティプロセッサから受信することを含む、請求項 4 の方法。

【請求項 6】

前記コンピュータビジョンプロセッサにおいて、前記 FMR を閉じ、前記 FMR が閉じられている間、前記画像データへの前記信頼できないアプリケーションのアクセスを拒否することを含む、請求項 5 の方法。

【請求項 7】

前記 FMR を閉じることは、前記 FMR が閉じられていることを示す情報を前記セキュリティプロセッサに提供することを含み、前記セキュリティプロセッサは、前記 FMR が閉じられている間、前記 FMR 要求を前記コンピュータビジョンプロセッサに転送しない、請求項 6 の方法。

【請求項 8】

前記画像クラスタにおいて、ユーザ入力に応じて、前記 FMR を開くか閉じるかを設定することをさらに含む、請求項 1 の方法。

【請求項 9】

処理クラスタの信頼できないアプリケーションから、画像クラスタのコンピュータビジョンプロセッサに、信頼メモリ領域 (TMR) の一部に記憶された画像データにアクセスするためのフェンスメモリ領域 (FMR) 要求を提供することと、

前記信頼できないアプリケーションにおいて、前記 FMR 要求を提供したことに応じて、前記コンピュータビジョンプロセッサが前記 TMR の一部の前記画像データにアクセスする許可を前記信頼できないアプリケーションに付与したかどうかを示す FMR 応答を受信することと、

前記 FMR が開いている場合に、前記 FMR 応答に基づいて、前記信頼できないアプリケーションから前記画像データにアクセスすることと、を含む、方法。

【請求項 10】

前記画像データは、前記コンピュータビジョンプロセッサによって取得され、前記コンピュータビジョンプロセッサは、前記画像データを前記 TMR の前記一部に記憶する、請求項 9 の方法。

【請求項 11】

前記画像データは、前記 TMR のバッファのセットに記憶され、前記 FMR は、前記 TMR の前記バッファのセットへのアクセスを制御するように定義される、請求項 10 の方法。

【請求項 12】

前記信頼できないアプリケーションは、前記コンピュータビジョンプロセッサが前記 FMR を開いたことに応じて、前記コンピュータビジョンプロセッサが前記画像データへのアクセスを許可したことを示す前記 FMR 応答を受信する、請求項 9 の方法。

【請求項 13】

前記 FMR 応答を受信することは、前記 FMR が開いている間、前記 FMR 応答をセキュリティプロセッサから受信することを含み、前記セキュリティプロセッサは、前記画像

10

20

30

40

50

クラスタと信頼関係を有している、

請求項 12 の方法。

【請求項 14】

前記信頼できないアプリケーションは、前記コンピュータビジョンプロセッサが前記 FMR を閉じたことに応じて、前記画像データへのアクセスを拒否する前記 FMR 応答を受信する、

請求項 13 の方法。

【請求項 15】

前記信頼できないアプリケーションは、前記 FMR が閉じている間、前記画像データへのアクセスを拒否する前記 FMR 応答を前記セキュリティプロセッサから受信し、前記セキュリティプロセッサは、前記 FMR が閉じられている間、前記 FMR 要求を前記コンピュータビジョンプロセッサに転送しない、

請求項 14 の方法。

【請求項 16】

データファブリックにおいて、信頼メモリ領域 (TMR) と信頼関係を有する画像クラスタによって前記 TMR の一部に記憶された画像データにアクセスする要求を画像処理アプリケーションから受信することであって、前記要求は、前記 TMR と信頼関係を有していないアプリケーションから受信される、ことと、

前記画像クラスタが前記 TMR の前記一部のためにフェンスメモリ領域 (FMR) を開いた場合に、前記画像処理アプリケーションが、前記 TMR に記憶された前記画像データにアクセスするのを許可することと、を含む、

方法。

【請求項 17】

前記要求を受信することは、前記 TMR 内の位置を示す情報を含む前記要求を受信することを含み、前記画像処理アプリケーションが前記画像データにアクセスするのを許可することは、前記要求において示された前記位置が、FMR 要求を介してアクセス可能な前記 TMR の前記一部に存在するかどうかを判別することを含む、

請求項 16 の方法。

【請求項 18】

前記画像処理アプリケーションが前記画像データにアクセスするのを許可することは、前記位置が、FMR 要求を介してアクセス可能な前記 TMR の前記一部に存在し、且つ、前記画像クラスタが前記 FMR を開いた場合に、前記画像処理アプリケーションが前記画像データにアクセスするのを許可することを含む、

請求項 17 の方法。

【請求項 19】

前記画像処理アプリケーションが前記画像データにアクセスするのを許可することは、前記位置が、FMR 要求を介してアクセス可能な前記 TMR の前記一部に存在しない場合に、メモリアクセスフォールトを前記画像処理アプリケーションに提供することを含む、

請求項 18 の方法。

【請求項 20】

前記画像クラスタが前記 FMR を閉じている間、前記 TMR の前記一部にアクセスするための要求に応じて、メモリアクセスフォールトを発行することを含む、

請求項 18 の方法。

【発明の詳細な説明】

【背景技術】

【0001】

コンピュータビジョンは、コンピュータが、人間の視覚系によって行われる類似のタスクに対応するタスクを自動化することによって、デジタル画像から高レベルの情報を抽出することを可能にする。コンピュータビジョンタスクの例は、オブジェクト認識、モーション分析、シーンの再構成、画像復元を含む。コンピュータビジョン技術は、2つの補完

10

20

30

40

50

タスク (complementary tasks) ((1) 1 つ以上のデジタル画像を取得すること、 (2) 取得した画像を処理して、デジタル画像内の情報の「理解 (understanding)」を表す高次元データを生成すること) を含む。画像取得は、1 つ以上の画像センサ又はカメラと、距離センサ、深度センサ、断層撮影装置、レーダ、超音波カメラ等とによって行われる。デジタル画像は、通常の 2 次元 (2 D) 画像、3 次元 (3 D) ポリウム、又は、1 つ以上の 2 D 画像及び 3 D ポリウムの組み合わせであり得る。画像処理技術は、ノイズを低減し又は画像コントラストを強調させるためにデータを前処理すること、画像データから特徴を抽出すること、画像データの検出又はセグメンテーション、画像認識又は画像記録、及び、抽出された情報に基づく意思決定を含む。

【発明の概要】

10

【課題を解決するための手段】

【 0 0 0 2 】

一態様によれば、方法は、画像クラスタのコンピュータビジョンプロセッサにおいて、信頼メモリ領域 (T M R) の第 1 の部分に記憶された画像データへのアクセスを制御するフェンスメモリ領域 (F M R : fenced memory region) を定義することを含む。方法は、コンピュータビジョンプロセッサにおいて、処理クラスタに実装されたアプリケーションから T M R の第 1 の部分の画像データにアクセスするための F M R 要求を受信することと、コンピュータビジョンプロセッサにおいて、F M R 要求を受信したことに応じて、アプリケーションが画像データにアクセスすることを選択的に可能にすることと、をさらに含む。T M R の第 1 の部分へのアクセスを制御するために F M R を定義することは、例えば、画像データを記憶する T M R のバッファのセットを定義することを含む。方法は、コンピュータビジョンプロセッサにおいて、F M R を開くことをさらに含むことができ、アプリケーションが画像データにアクセスすることを選択的に可能にすることは、F M R が開いている間、アプリケーションが画像データにアクセスすることを可能にすることを含む。いくつかの実施形態では、方法は、コンピュータビジョンプロセッサを使用して、画像データを取得することと、画像データを T M R の第 1 の部分に記憶することと、を含む。いくつかの実施形態では、F M R を開くことは、F M R が開いていることを示す情報をセキュリティプロセッサに提供することを含み、セキュリティプロセッサは、画像クラスタとの信頼関係を有し、F M R 要求を受信することは、F M R が開いている間、F M R 要求をセキュリティプロセッサから受信することを含む。方法は、コンピュータビジョンプロセッサにおいて、F M R を閉じることを含むことができ、アプリケーションが画像データにアクセスすることを選択的に可能にすることは、F M R が閉じている間、画像データへのアプリケーションのアクセスを拒否することを含む。例えば、F M R を閉じることは、F M R が閉じていることを示す情報をセキュリティプロセッサに提供することを含み、セキュリティプロセッサは、F M R が閉じている間、F M R 要求をコンピュータビジョンプロセッサに転送しない。方法は、画像クラスタにおいて、ユーザ入力に応じて、F M R を開く又は閉じるように設定することを含むことができる。

20

30

【 0 0 0 3 】

別の態様では、方法は、処理クラスタのアプリケーションから画像クラスタのコンピュータビジョンプロセッサに、T M R の第 1 の部分に記憶された画像データにアクセスするための F M R 要求を提供することと、アプリケーションにおいて、F M R 要求を提供したことに応じて、コンピュータビジョンプロセッサが T M R の第 1 の部分の画像データにアクセスする許可をアプリケーションに付与したかどうかを示す F M R 応答を受信することと、F M R 応答に基づいてアプリケーションから画像データに選択的にアクセスすることと、を含む。

40

【 0 0 0 4 】

さらに別の態様によれば、方法は、データファブリックにおいて、T M R と信頼関係を有する画像クラスタによって T M R の一部に記憶された画像データにアクセスするための画像処理アプリケーションからの要求を受信することを含み、この要求は、T M R と信頼関係を有していない処理クラスタのアプリケーションから受信される。方法は、画像クラ

50

スタが T M R の一部ののためにフェンスメモリ領域 (F M R) を開いている又は閉じているかどうかに基づいて、画像処理アプリケーションが T M R に記憶された画像データにアクセスすることを選択的に許可することを含む。

【 0 0 0 5 】

さらなる態様によれば、コンピュータシステムは、少なくとも 1 つのコンピュータビジョンプロセッサを有し、上述した方法の 1 つ以上を行うように構成されている。

【 0 0 0 6 】

本開示は、添付の図面を参照することによって良好に理解することができ、その多くの特徴及び利点が当業者に明らかになる。異なる図面において同じ符号を使用することは、類似又は同一の要素を示す。

【図面の簡単な説明】

【 0 0 0 7 】

【図 1】いくつかの実施形態による、安全なコンピュータビジョン処理をサポートする処理システムのブロック図である。

【図 2】いくつかの実施形態による、信頼されていないアプリケーションによる信頼メモリ領域 (T M R) へのアクセスを選択的に可能にするために使用されるメッセージを含むメッセージフローである。

【図 3】いくつかの実施形態による、信頼できないアプリケーションが、フェンスメモリ領域 (F M R) によって制御される T M R の一部へのアクセスを要求することを選択的に可能にする方法のフロー図である。

【発明を実施するための形態】

【 0 0 0 8 】

いくつかのコンピューティングアーキテクチャでは、処理要素の個別のクラスタを使用して、様々なコンピュータビジョンタスクを行う。画像クラスタは、その後の分析のためにデジタル画像を取得するように構成された 1 つ以上の処理要素 (本明細書では、コンピュータビジョンプロセッサと呼ばれる) を含む。画像クラスタは、センサ、カメラ、レーダ等の画像取得デバイスからデータを受信する。場合によっては、画像クラスタのコンピュータビジョンプロセッサは、取得したデータに対して、所定の座標系への再サンプリング、ノイズリダクション、コントラスト強調、又は、画像のスケーリング等の前処理を行う。次に、画像クラスタは、取得又は後処理されたデータをメモリ領域に記憶する。処理クラスタは、メモリ領域から取得したデータにアクセスし、取得又は後処理されたデータを処理し、処理結果をメモリ領域に記憶する。処理クラスタは、信頼できないアプリケーションも実行するユーザ向けクラスタである。信頼できないアプリケーションがメモリ領域に記憶されたコンピュータビジョンデータにアクセスするのを可能にすることで、ユーザのプライバシーに悪影響を及ぼす可能性がある。例えば、画像クラスタ及び処理クラスタのコンピュータビジョンアプリケーションのみが知っている秘密鍵を使用して、メモリ領域での記憶のためにデータを暗号化することを画像クラスタに要求することは、プライバシーを提供することができるが、これは、処理オーバーヘッドをかなり増加させ、画像処理のスループットを低下させる。

【 0 0 0 9 】

図 1 ~ 図 3 は、画像クラスタ及び処理クラスタを含むいくつかの実施形態による処理システムを開示し、処理クラスタは、画像クラスタのコンピュータビジョンプロセッサが、画像クラスタによって取得又は後処理された画像データへのアクセスを制御するフェンスメモリ領域 (F M R) を定義することを可能にすることによって、コンピュータビジョンデータのセキュリティ及びプライバシーを強化する。画像クラスタのコンピュータビジョンプロセッサは、画像クラスタの信頼できるエンティティによってアクセス可能な信頼メモリ領域 (T M R) に画像データを記憶する。画像クラスタは、 F M R に関連する T M R の一部 (T M R のバッファのセット等) へのアクセスを制御する。画像クラスタは、情報にアクセスするための F M R 要求を受信したことに応じて、処理クラスタが T M R に記憶された情報にアクセスすることを選択的に可能にする。画像クラスタのいくつかの実施形

10

20

30

40

50

態は、セキュリティプロセッサを介してFMR要求を受信し、セキュリティプロセッサは、FMR要求及び応答に基づいて、TMRの画像データへのアクセスを制御するための信頼できるエンティティとして機能する。例えば、セキュリティプロセッサは、処理クラスタで実行されている画像処理アプリケーションからTMRの情報にアクセスするためのFMR要求を受信し、その要求を画像クラスタのコンピュータビジョンプロセッサに提供する。セキュリティプロセッサは、画像クラスタがFMR要求を許可する場合には処理アプリケーションへのアクセスを許可し、画像クラスタがFMR要求を拒否する場合にはアクセスを拒否する。画像クラスタは、FMRが画像クラスタによって開かれている場合に、FMR要求のみ処理する。画像クラスタがFMRを閉じた場合、セキュリティプロセッサは、信頼できないアプリケーションがTMRにアクセスするのを許可しない。

10

【0010】

処理システムのデータファブリック（例えば、メモリコントローラ及び関連インフラストラクチャ）は、画像データにアクセスするための要求又は画像データを記憶するための要求を画像処理アプリケーションから受信する。データファブリックは、要求に示された位置が、画像クラスタによって定義されたFMR要求によってアクセス可能なTMRのバッファにあるかどうかを決定する。そのような場合であって、画像クラスタがFMRを開いた場合、画像処理アプリケーションは、バッファから画像データにアクセスするためのFMR要求を送信すること、又は、画像データをバッファに記憶することが許可される。画像クラスタがFMR要求を許可した場合、画像処理アプリケーションは、画像データにアクセスすることが可能になる。メモリ要求が、FMR要求によってアクセス不可能なTMRの一部に対するものである場合、又は、画像クラスタがFMRを閉じた場合、データファブリックは、メモリアクセスフォールトを発行し、画像処理アプリケーションは、TMRの画像データにアクセスすること又はその画像データを記憶することが許可されない。処理クラスタで実行されている他のアプリケーションは、画像クラスタがFMRを閉じた場合、FMRによって制御されるTMRのバッファにアクセスすることが許可されない。コンピュータビジョンプロセッサのいくつかの実施形態は、例えば、ユーザ入力に応じて、FMRポリシーを切り替える。例えば、ユーザが画像データの記録に同意した場合、コンピュータビジョンプロセッサは、FMRポリシーを切り替えて、処理クラスタがFMRポリシーによって制御されるTMRのバッファの外部の画像データにアクセスして、その画像データを記憶することを可能にする。

20

30

【0011】

図1は、いくつかの実施形態による、安全なコンピュータビジョン処理をサポートする処理システム100のブロック図である。処理システム100は、ビデオカメラ110等の画像取得デバイスからデータを収集、収集又は受信する画像クラスタ105を含む。画像クラスタ105のいくつかの実施形態は、センサ、カメラ、レーダ等の他のソースからデータを収集、収集又は受信する。ビデオカメラ110は、ビデオカメラ110の視野内にあるユーザ115の映像等の画像を記録する。ビット又はフレームのストリーム等の画像を表す情報は、ビデオカメラ110で生成され、画像クラスタ105に提供される。図示した実施形態では、画像クラスタ105は、コンピュータビジョンプロセッサ120等の1つ以上の処理要素を含む。単一のコンピュータビジョンプロセッサ120が図1に示されているが、画像クラスタ105のいくつかの実施形態は、追加の画像又はビデオソースからデータを収集、収集又は受信する複数の処理要素を含む。

40

【0012】

画像クラスタ105は、取得したデータを、画像クラスタ105と信頼関係のあるメモリ領域125に記憶する。したがって、メモリ領域125は、信頼メモリ領域（TMR）125と呼ばれる。信頼関係は、ハンドシェイクプロトコル、認証プロトコル、鍵交換、ハードウェア分離等の技術を使用して、画像クラスタ105とTMR125との間で確立される。例えば、コンピュータビジョンプロセッサ120は、画像を表す情報をTMR125のバッファ130に記憶し、バッファ130は、他の画像又はデータを記憶するための追加バッファを含む。画像クラスタ105のコンピュータビジョンプロセッサ120の

50

いくつかの実施形態は、取得したデータに対して、所定の座標系への再サンプリング、ノイズリダクション、コントラスト強調、画像のスケーリング等の前処理を行う。次に、後処理された画像データは、TMR 125のバッファ130に記憶される。バッファ130に記憶された画像データは、画像クラスタ105とTMR 125との間の信頼関係によって安全であると見なされる。したがって、ユーザ115のセキュリティ及びプライバシーは、画像クラスタ105とTMR 125との信頼関係によって保護される。しかしながら、処理システム100の全てのエンティティがTMR 125と信頼関係を有するわけではない。

【0013】

画像クラスタ105は、処理システム100に実装されたデータファブリック135を介してTMR 125と情報を交換する。データファブリック135のいくつかの実施形態は、画像クラスタ105とTMR 125との間のインターフェース140をサポートするためのメモリコントローラ及び関連インフラストラクチャを含む。関連インフラストラクチャは、1つ以上のバス、ブリッジ、スイッチ、ルーター、ワイヤ、トレース等を含むことができる。インターフェース140は、画像クラスタ105とTMR 125との間の信頼関係により、これらのエンティティ間の安全な通信を提供する。例えば、データファブリック135又はインターフェース140は、コンピュータビジョンプロセッサ120からの要求を受信して、情報をTMR 125に記憶することができる。データファブリック135又はインターフェース140は、コンピュータビジョンプロセッサ120が（例えば、キー又はパスワードを使用して）TMR 125にアクセスすることが許可されたことを検証し、したがって、TMR 125へのアクセスをコンピュータビジョンプロセッサ120に提供する。TMR 125へのアクセスが許可されていないエンティティからのメモリアクセス要求は、拒否又は拒絶される。例えば、データファブリック135は、許可されていないエンティティからのアクセス要求に応じて、メモリアクセスフォールトを発行することができる。

【0014】

処理システム100は、画像処理アプリケーション150等のアプリケーションを実行する処理クラスタ145を含む。処理クラスタ145は、TMR 125と信頼関係がない。したがって、画像処理アプリケーション150は、信頼されないアプリケーションと呼ばれる。信頼されないアプリケーションが、TMR 125に記憶されたコンピュータビジョンデータにアクセスするのを可能にすることによって、ユーザのプライバシーに悪影響を及ぼす可能性がある。しかしながら、信頼されない全てのアプリケーションが、TMR 125に記憶されたデータ（バッファ130の画像等）にアクセスするのを抑制することは、処理システム100が、TMR 125に記憶された画像データを利用する能力を大幅に制限することになる。画像処理アプリケーション150のいくつかの実施形態は、処理クラスタ145で実行され、オブジェクト認識、動作分析、シーン再構成、画像復元等のタスクを自動化することによって、バッファ130の画像から高レベル情報を抽出する。したがって、画像処理アプリケーション150がバッファ130の画像にアクセスすることを拒否すると、処理システム100が、画像を処理して、画像クラスタ105によって取得された画像の情報の「理解」を表す高次元データを生成する能力が制限される。

【0015】

ユーザ115のプライバシー及びセキュリティを確保すると同時に、処理クラスタ145が、TMR 125に記憶されたデータに対して重要な操作を行うことを可能にするために、画像クラスタ105は、TMR 125の一部に関連するフェンスメモリ領域（FMR）を定義することによって、TMR 125へのアクセスを選択的に提供する。図示した実施形態では、画像クラスタ105によって定義されるFMRは、コンピュータビジョンプロセッサ120によって取得された（場合によっては、前処理された）画像を記憶するバッファ130を含む。

【0016】

画像クラスタ105は、FMRを使用して、FMRに関連するTMR 125の一部に記

10

20

30

40

50

憶された画像データへのアクセスを制御する。コンピュータビジョンプロセッサ 120 のいくつかの実施形態は、画像処理アプリケーション 150 等の処理クラスタ 145 で実行されるアプリケーションからの FMR 要求を受信する。FMR 要求は、TMR 125 のバッファ 130 の画像データにアクセスするための要求を含む。例えば、FMR 要求は、TMR 125 内の位置を示すアドレス等の情報を含むことができる。コンピュータビジョンプロセッサ 120 は、アドレスを使用して、FMR 要求が、FMR によって制御されるバッファ 130 にアクセスするのを試みていることを決定する。コンピュータビジョンプロセッサ 120 は、例えば、画像クラスタ 105 又はコンピュータビジョンプロセッサ 120 が FMR を開いている又は閉じているかどうかによって、画像処理アプリケーション 150 がバッファ 130 の画像データにアクセスするのを選択的に可能にする。画像クラスタ 105 のいくつかの実施形態は、バッファ 130 へのアクセスが与えられるアプリケーションを示すホワイトリストを記憶する（又は、ホワイトリストにアクセスする）。また、画像クラスタ 105 は、ユーザ 115 がアクセスを許可するか、バッファ 130 の画像がパブリックに利用可能であるという指標を提供したことに応じて、バッファ 130 へのアクセスを提供することができる。

10

【0017】

処理システム 100 のいくつかの実施形態は、信頼されたエンティティであるセキュリティプロセッサ 155 を含む。セキュリティプロセッサ 155 は、処理クラスタ 145 によって生成された FMR 要求及び画像クラスタ 105 によって提供された FMR 応答に基づいて、TMR 125 のバッファ 130 へのアクセスを制御する。例えば、画像クラスタ 105 は、画像クラスタ 105 が FMR を開いたことを、セキュリティプロセッサ 155 に通知することができる。セキュリティプロセッサ 155 は、FMR が開いている間に、TMR 125 の情報にアクセスするための FMR 要求を画像処理アプリケーション 150 から受信した場合に、FMR 要求を画像クラスタ 105（例えば、コンピュータビジョンプロセッサ 120）に提供する。画像クラスタ 105 は、FMR 要求を受信したことに応じて、セキュリティプロセッサ 155 に提供される FMR 応答に示されるように、TMR へのアクセスを選択的に許可する。セキュリティプロセッサ 155 は、画像クラスタ 105 が FMR 要求を許可する場合には、画像処理アプリケーション 150 へのアクセスを許可し、画像クラスタ 105 が FMR 要求を拒否する場合には、アクセスを拒否する。画像クラスタ 105 は、FMR が画像クラスタ 105 によって開かれている場合、FMR 要求のみを処理する。画像クラスタ 105 が FMR を閉じた場合、セキュリティプロセッサ 155 は、信頼されていないアプリケーションが TMR 125 にアクセスするのを許可しない。

20

30

【0018】

データファブリック 135 は、処理クラスタ 145 と TMR 125 との間のインターフェース 160 をサポートする。データファブリック 135 のいくつかの実施形態は、処理クラスタ 145（又は、画像処理アプリケーション 150）が、処理クラスタ 145 又は画像処理アプリケーション 150 によって生成されたメモリアクセス要求に基づいて、TMR 125 の一部へのアクセスを要求するのを選択的に可能にする。データファブリック 135 は、要求に示された位置が、画像クラスタ 105 によって定義されるように、FMR 要求によってアクセス可能な TMR 125 のバッファ 130 にあるかどうかを決定する。このような場合であって、画像クラスタ 105 が FMR を開いている場合、画像処理クラスタ 145 又は画像処理アプリケーション 150 は、バッファ 130 から画像データにアクセスするための FMR 要求を送信すること、又は、画像データをバッファ 130 に記憶することが許可される。画像クラスタ 105 が FMR 要求を許可する場合には、画像処理クラスタ 145 又は画像処理アプリケーション 150 は、画像データにアクセスすることが可能になる。メモリ要求が、FMR 要求によってアクセス不可能な TMR 125 の一部に対するものである場合、又は、画像クラスタ 105 が FMR を閉じた場合には、データファブリック 135 は、メモリアクセスフォールトを発行する。この場合、処理クラスタ 145 又は画像処理アプリケーション 150 は、TMR 125 の画像データにアクセス

40

50

すること又は画像データを記憶することが許可されない。処理クラスタ 1 4 5 で実行されている他のアプリケーションは、画像クラスタ 1 0 5 が F M R を閉じた場合に、F M R によって制御される T M R 1 2 5 のバッファ 1 3 0 にアクセスすることが許可されない。

【 0 0 1 9 】

F M R に基づいて T M R 1 2 5 へのアクセスを制御するポリシーは、場合によっては、ユーザ入力に基づいて変更される。例えば、ユーザ 1 1 5 は、処理システム 1 0 0 のオペレータに同意を提供することによって、バッファ 1 3 0 の画像データをパブリックに利用可能にすることができる。画像クラスタ 1 0 5 又はコンピュータビジョンプロセッサ 1 2 0 のいくつかの実施形態は、ユーザ入力に応じて、F M R ポリシーを切り替える。例えば、ユーザが画像データの記録に同意した場合には、コンピュータビジョンプロセッサ 1 2 0 は、F M R ポリシーを切り替えて、処理クラスタ 1 4 5 が、F M R ポリシーによって制御される T M R 1 2 5 のバッファ 1 3 0 の外部の画像データにアクセスして、その画像データを記憶するのを可能にする。

10

【 0 0 2 0 】

図 2 は、いくつかの実施形態による、信頼されていないアプリケーションによる信頼メモリ領域 (T M R) へのアクセスを選択的に可能にするために使用されるメッセージを含むメッセージフロー 2 0 0 である。メッセージフロー 2 0 0 は、画像クラスタのコンピュータビジョンプロセッサ (C V)、セキュアプロセッサ (S E C)、2 つのアプリケーション (A P P 1 , A P P 2) を含む処理クラスタ 2 0 5、及び、画像クラスタと信頼関係を有する T M R との間で交換されるメッセージを含む。したがって、メッセージフロー 2 0 0 は、図 1 に示される処理システム 1 0 0 のいくつかの実施形態で実施される。画像クラスタは、T M R の一部 (T M R に実装されるバッファのセット等) に関連する F M R を定義している。

20

【 0 0 2 1 】

ブロック 2 1 0 において、画像クラスタのコンピュータビジョンプロセッサは、F M R を開き、信頼されていないアプリケーションが、F M R によって制御される T M R の一部へのアクセスを要求するのを可能にする。分かりやすくするために図 2 に示されていないが、コンピュータビジョンプロセッサは、画像クラスタが F M R を開いていることを、セキュアプロセッサと、データファブリック (図 1 に示すデータファブリック 1 3 5 等) と、に通知する。

30

【 0 0 2 2 】

第 1 のアプリケーション (A P P 1) は、F M R 要求 2 1 5 をコンピュータビジョンプロセッサに送信して、T M R の F M R 制御部へのアクセスを要求する。F M R 要求は、T M R の要求された部分の位置を識別する情報を含む。F M R 要求 2 1 5 を受信したことに応じて、コンピュータビジョンプロセッサは、T M R のバッファへの第 1 のアプリケーションのアクセスを許可するかどうかを決定する。図示した実施形態では、ブロック 2 2 5 において、コンピュータビジョンプロセッサは、第 1 のアプリケーションのアクセスを許可する。例えば、第 1 のアプリケーションは、T M R へのアクセスが許可されているアプリケーションのホワイトリストに含まれ得る。コンピュータビジョンプロセッサは、コンピュータビジョンプロセッサが第 1 のアプリケーションのアクセスを許可したことを示す F M R 応答 2 3 0 を、セキュアプロセッサ (secure processor) に返す。セキュアプロセッサは、F M R 応答 2 3 5 を、第 1 のアプリケーションに転送する。F M R 応答 2 3 5 を受信したことに応じて、第 1 のアプリケーションは、例えば、両矢印 2 4 0 によって示すように、データファブリックによってサポートされたインターフェースを介して、T M R の領域にアクセスする。

40

【 0 0 2 3 】

第 2 のアプリケーション (A P P 2) は、F M R 要求 2 4 5 をコンピュータビジョンプロセッサに送信して、T M R の F M R 制御部へのアクセスを要求する。F M R 要求は、T M R の要求された部分の位置を識別する情報を含む。F M R 要求 2 4 5 を受信したことに応じて、コンピュータビジョンプロセッサは、第 2 のアプリケーションが T M R のバッ

50

ァにアクセスするのを許可するかどうかを決定する。図示した実施形態では、ブロック 255 において、コンピュータビジョンプロセッサは、第 2 のアプリケーションのアクセスを拒否する。例えば、第 2 のアプリケーションは、TMR へのアクセスが許可されていないアプリケーションのブラックリストに含まれていてもよく、第 2 のアプリケーションは、TMR へのアクセスが許可されているアプリケーションのホワイトリストに含まれていなくてもよい。コンピュータビジョンプロセッサは、要求が拒否されたことを示す FMR 応答 260 を返す。セキュアプロセッサは、FMR 応答 265 を第 2 のアプリケーションに転送して、要求が拒否されたことを第 2 のアプリケーションに通知する。第 2 のアプリケーションと TMR との間にインターフェースが確立されないため、TMR に記憶された情報は、第 2 のアプリケーションによる望ましくないアクセス又は悪意のあるアクセスから保護される。

10

【0024】

図 3 は、いくつかの実施形態による、信頼されていないアプリケーションが、フェンスメモリ領域 (FMR) によって制御される TMR の一部へのアクセスを要求することを選択的に可能にする方法 300 のフロー図である。方法 300 は、図 1 に示す処理システム 100 のデータファブリック 135 のいくつかの実施形態で実施される。

【0025】

ブロック 305 において、データファブリックは、処理クラスタの信頼されていないアプリケーションから、TMR と信頼関係を有する画像クラスタによって収集された画像にアクセスするための要求を受信する。例えば、処理クラスタの画像処理アプリケーションは、画像処理アプリケーションがアクセスしたいメモリのアドレスを示す情報を含むメモリアクセス要求を送信することができる。

20

【0026】

ブロック 310 において、データファブリックは、要求された画像が TMR にあるかどうかを決定する。いくつかの実施形態では、データファブリックは、メモリアクセス要求のアドレスを、TMR の範囲内の位置に対応するアドレス範囲と比較する。例えば、アドレスが、TMR に対応するアドレスの範囲内にあることによって示されるように、要求された画像が TMR にある場合には、方法 300 は、決定ブロック 315 に進む。例えば、アドレスが、TMR に対応するアドレス範囲外にあることによって示されるように、要求された画像が TMR にない場合には、方法 300 は、ブロック 320 に進み、データファブリックは、信頼されていないアプリケーションが画像へのアクセスを要求又は受信することを可能にする。

30

【0027】

決定ブロック 315 において、データファブリックは、メモリアクセス要求が、画像クラスタによって定義された FMR によって制御される TMR の一部に向けられているかどうかを決定する。画像処理アプリケーションからのメモリアクセス要求が、FMR によって制御されていない TMR の一部に向けられた場合には、画像処理アプリケーションは、TMR と信頼関係を有していない処理クラスタで実行されているので、データファブリックは、メモリアクセス要求を拒否する。方法 300 は、ブロック 325 に進み、データファブリックは、信頼されていない画像処理アプリケーションに対してメモリアクセスフォールトを発行する。メモリアクセス要求が、FMR によって制御される TMR の一部に向けられた場合には、方法 300 は、決定ブロック 335 に進む。

40

【0028】

決定ブロック 335 において、データファブリックは、画像クラスタ (又は、コンピュータビジョンプロセッサ) が、FMR によって制御される TMR の一部にアクセスするための FMR 要求を受信するために FMR を開いたかどうかを決定する。そうではない場合、方法 300 は、ブロック 325 に進み、データファブリックは、信頼されていない画像処理アプリケーションに対してメモリアクセスフォールトを発行する。FMR が開いている場合、方法 300 は、ブロック 340 に進み、データファブリックは、信頼されていない画像処理アプリケーションが、FMR によって制御される TMR の一部の画像へのアク

50

セスを要求することを可能にする。したがって、画像処理アプリケーションは、データファブリックを介してFMR要求を画像クラスタに送信することができる。

【0029】

コンピュータ可読記憶媒体は、命令及び/又はデータをコンピュータシステムに提供するために、使用中にコンピュータシステムによってアクセス可能な任意の非一時的な記憶媒体又は非一時的な記憶媒体の組み合わせを含む。このような記憶媒体には、限定されないが、光学媒体（例えば、コンパクトディスク（CD）、デジタル多用途ディスク（DVD）、ブルーレイ（登録商標）ディスク）、磁気媒体（例えば、フロッピー（登録商標）ディスク、磁気テープ、磁気ハードドライブ）、揮発性メモリ（例えば、ランダムアクセスメモリ（RAM）若しくはキャッシュ）、不揮発性メモリ（例えば、読取専用メモリ（ROM）若しくはフラッシュメモリ）、又は、微小電気機械システム（MEMS）ベースの記憶媒体が含まれ得る。コンピュータ可読記憶媒体（例えば、システムRAM又はROM）はコンピューティングシステムに内蔵されてもよいし、コンピュータ可読記憶媒体（例えば、磁気ハードドライブ）はコンピューティングシステムに固定的に取り付けられてもよいし、コンピュータ可読記憶媒体（例えば、光学ディスク又はユニバーサルシリアルバス（USB）ベースのフラッシュメモリ）はコンピューティングシステムに着脱可能に取り付けられてもよいし、コンピュータ可読記憶媒体（例えば、ネットワークアクセス可能ストレージ（NAS））は有線又は無線ネットワークを介してコンピュータシステムに結合されてもよい。

【0030】

いくつかの実施形態では、上記の技術のいくつかの態様は、ソフトウェアを実行するプロセッシングシステムの1つ以上のプロセッサによって実装されてもよい。ソフトウェアは、非一時的なコンピュータ可読記憶媒体に記憶され、又は、非一時的なコンピュータ可読記憶媒体上で有形に具現化された実行可能命令の1つ以上のセットを含む。ソフトウェアは、1つ以上のプロセッサによって実行されると、上記の技術の1つ以上の態様を実行するように1つ以上のプロセッサを操作する命令及び特定のデータを含むことができる。非一時的なコンピュータ可読記憶媒体は、例えば、磁気若しくは光ディスク記憶デバイス、例えばフラッシュメモリ、キャッシュ、ランダムアクセスメモリ（RAM）等のソリッドステート記憶デバイス、又は、他の1つ以上の不揮発性メモリデバイス等を含むことができる。非一時的なコンピュータ可読記憶媒体に記憶された実行可能命令は、ソースコード、アセンブリ言語コード、オブジェクトコード、又は、1つ以上のプロセッサによって解釈若しくは実行可能な他の命令フォーマットであってもよい。

【0031】

上述したものに加えて、概要説明において説明した全てのアクティビティ又は要素が必要とされているわけではなく、特定のアクティビティ又はデバイスの一部が必要とされない場合があり、1つ以上のさらなるアクティビティが実行される場合があり、1つ以上のさらなる要素が含まれる場合があることに留意されたい。さらに、アクティビティが列挙された順序は、必ずしもそれらが実行される順序ではない。また、概念は、特定の実施形態を参照して説明された。しかしながら、当業者であれば、特許請求の範囲に記載されているような本発明の範囲から逸脱することなく、様々な変更及び変形を行うことができるのを理解するであろう。したがって、明細書及び図面は、限定的な意味ではなく例示的な意味で考慮されるべきであり、これらの変更形態の全ては、本発明の範囲内に含まれることが意図される。

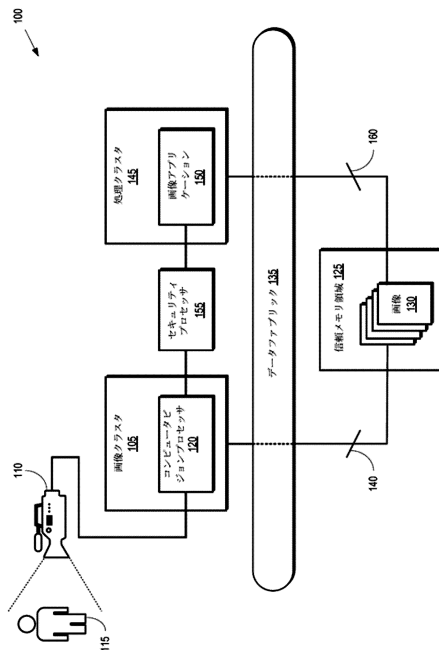
【0032】

利益、他の利点及び問題に対する解決手段を、特定の実施形態に関して上述した。しかし、利益、利点、問題に対する解決手段、及び、何かしらの利益、利点若しくは解決手段が発生又は顕在化する可能性のある特徴は、何れか若しくは全ての請求項に重要な、必須の、又は、不可欠な特徴と解釈されない。さらに、開示された発明は、本明細書の教示の利益を有する当業者には明らかな方法であって、異なっているが同様の方法で修正され実施され得ることから、上述した特定の実施形態は例示にすぎない。添付の特許請求の範囲

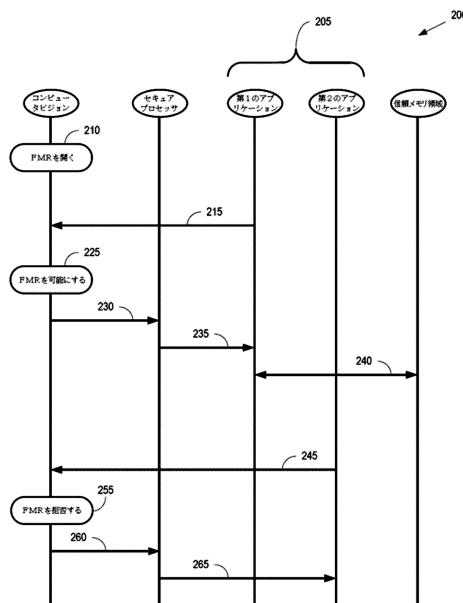
に記載されている以外に本明細書に示されている構成又は設計の詳細については限定がない。したがって、上述した特定の実施形態は、変更又は修正されてもよく、かかる変更形態の全ては、開示された発明の範囲内にあると考えられることが明らかである。したがって、ここで要求される保護は、添付の特許請求の範囲に記載されている。

【図面】

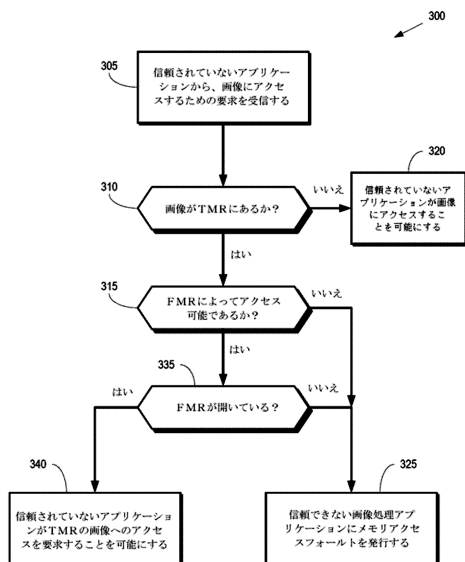
【図 1】



【図 2】



【図 3】



10

20

30

40

50

フロントページの続き

CES INCORPORATED

アメリカ合衆国 9 5 0 5 4 カリフォルニア州、 サンタ クララ、 オーガスティン ドライブ 2
4 8 5

(74)代理人 100108833

弁理士 早川 裕司

(74)代理人 100111615

弁理士 佐野 良太

(74)代理人 100162156

弁理士 村雨 圭介

(72)発明者 ベンジャミン クーン パン チャン

カナダ国 L 3 T 7 X 6 オンタリオ州、 マーカム、 ワン コマース バリー ドライブ イースト

(72)発明者 ウィリアム ロイド アトキンソン

カナダ国 L 3 T 7 X 6 オンタリオ州、 マーカム、 ワン コマース バリー ドライブ イースト

(72)発明者 トゥン チュアン クォン

カナダ国 L 3 T 7 X 6 オンタリオ州、 マーカム、 ワン コマース バリー ドライブ イースト

(72)発明者 グアン クリシュナン

アメリカ合衆国 9 5 0 5 4 カリフォルニア州、 サンタ クララ、 オーガスティン ドライブ 2 4 8 5

審査官 平井 誠

(56)参考文献 米国特許出願公開第 2 0 1 3 / 0 3 0 5 3 4 2 (U S , A 1)

米国特許出願公開第 2 0 0 8 / 0 1 0 9 6 6 2 (U S , A 1)

特開 2 0 0 7 - 2 5 8 9 5 7 (J P , A)

米国特許出願公開第 2 0 1 3 / 0 0 5 7 3 8 4 (U S , A 1)

(58)調査した分野 (Int.Cl. , D B 名)

G 0 6 F 2 1 / 6 2