



(51) International Patent Classification:

G06F 21/53 (2013.01) G06F 21/71 (2013.01)
G06F 21/60 (2013.01)

(21) International Application Number:

PCT/US2019/066615

(22) International Filing Date:

16 December 2019 (16.12.2019)

(25) Filing Language:

English

(26) Publication Language:

English

(30) Priority Data:

16/228,349 20 December 2018 (20.12.2018) US

(71) Applicants: **ATI TECHNOLOGIES ULC** [CA/CA]; 1 Commerce Valley Drive East, Markham, Ontario L3T 7X6 (CA). **ADVANCED MICRO DEVICES, INC.** [US/US]; 2485 Augustine Drive, Santa Clara, California 95054 (US).

(72) Inventors: **CHAN, Benjamin Koon Pan**; 1 Commerce Valley Drive East, Markham, Ontario L3T 7X6 (CA). **ATKINSON, William Lloyd**; 1 Commerce Valley Drive East, Markham, Ontario L3T 7X6 (CA). **KWONG, Tung Chuen**; 1 Commerce Valley Drive East, Markham, Ontario L3T 7X6 (CA). **KRISHNAN, Guhan**; 2485 Augustine Drive, Santa Clara, California 95054 (US).

(74) Agent: **DAVIDSON, Ryan S.**; Davidson Sheehan LLP, 6836 Austin Center Blvd., Suite 320, Austin, Texas 78731 (US).

(81) Designated States (*unless otherwise indicated, for every kind of national protection available*): AE, AG, AL, AM, AO, AT, AU, AZ, BA, BB, BG, BH, BN, BR, BW, BY, BZ, CA, CH, CL, CN, CO, CR, CU, CZ, DE, DJ, DK, DM, DO, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, GT, HN, HR, HU, ID, IL, IN, IR, IS, JO, JP, KE, KG, KH, KN, KP, KR, KW, KZ, LA, LC, LK, LR, LS, LU, LY, MA, MD, ME, MG, MK, MN, MW, MX, MY, MZ, NA, NG, NI, NO, NZ,

(54) Title: SECURE COMPUTER VISION PROCESSING

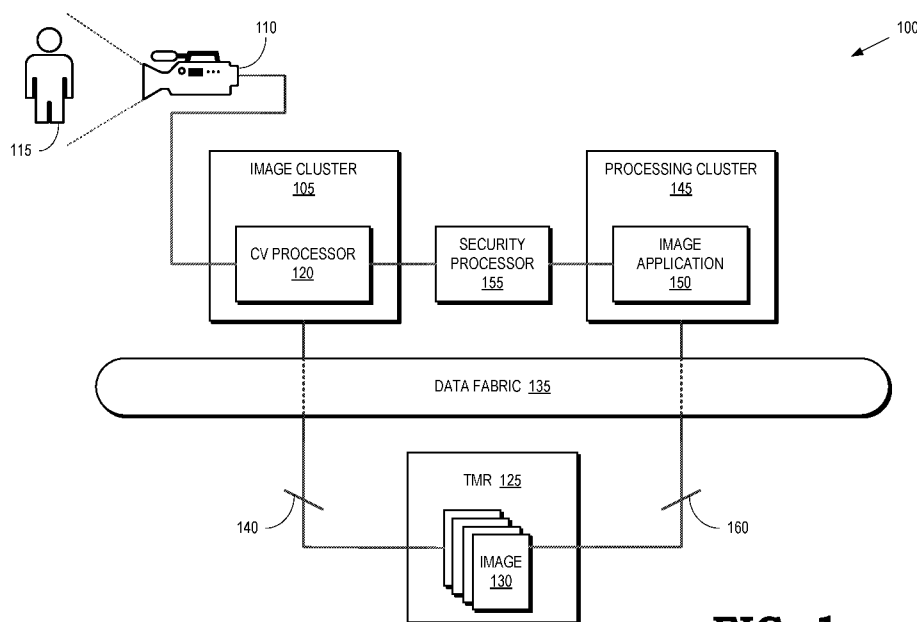


FIG. 1

(57) Abstract: A computer vision processor (120) in an image cluster (105) defines a fenced memory region (FMR) that controls access to image data stored in a first portion of a trusted memory region (TMR)(125). The computer vision processor receives FMR requests from an application (150) implemented in a processing cluster (145). The FMR requests are to access the image data (130) in the first portion of the TMR. The computer vision processor selectively allows the requesting application to access the image data. In some cases, the computer vision processor acquires the image data and stores the image data in the first portion of the TMR, such as buffers in the TMR. A data fabric (135) selectively permits the image processing application to access the data stored in the TMR based on whether the image cluster has opened or closed the FMR for the portion of the TMR.



OM, PA, PE, PG, PH, PL, PT, QA, RO, RS, RU, RW, SA, SC, SD, SE, SG, SK, SL, SM, ST, SV, SY, TH, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, ZA, ZM, ZW.

- (84) Designated States** (*unless otherwise indicated, for every kind of regional protection available*): ARIPO (BW, GH, GM, KE, LR, LS, MW, MZ, NA, RW, SD, SL, ST, SZ, TZ, UG, ZM, ZW), Eurasian (AM, AZ, BY, KG, KZ, RU, TJ, TM), European (AL, AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HR, HU, IE, IS, IT, LT, LU, LV, MC, MK, MT, NL, NO, PL, PT, RO, RS, SE, SI, SK, SM, TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, KM, ML, MR, NE, SN, TD, TG).

Published:

- with international search report (Art. 21(3))
- before the expiration of the time limit for amending the claims and to be republished in the event of receipt of amendments (Rule 48.2(h))

SECURE COMPUTER VISION PROCESSING

BACKGROUND

Computer vision allows computers to extract high-level information from digital images by automating tasks that correspond to similar tasks performed by a human visual system. Examples of computer vision tasks include object recognition, motion analysis, scene reconstruction, and image restoration. Computer vision techniques include two complementary tasks: (1) acquiring one or more digital images and (2) processing the acquired images to generate high dimensional data that represents an “understanding” of the information in the digital images. Image acquisition is performed by one or more image sensors or cameras, as well as range sensors, depth sensors, tomography devices, radar, ultrasonic cameras, and the like. The digital image can be an ordinary two-dimensional (2D) image, a three-dimensional (3D) volume, or a combination of one or more of the 2D images and 3D volumes. Image processing techniques including preprocessing the data to reduce noise or enhance image contrast, extracting features from the image data, detection or segmentation of the image data, image recognition or registration, and decision-making based on the extracted information.

SUMMARY OF EMBODIMENTS

In accordance with one aspect, a method includes defining, at a computer vision processor in an image cluster, a fenced memory region (FMR) that controls access to image data stored in a first portion of a trusted memory region (TMR). The method further includes receiving, at the computer vision processor from an application implemented in a processing cluster, an FMR request to access the image data in the first portion of the TMR and selectively allowing, at the computer vision processor, the application to access the image data in response to receiving the FMR request. Defining the FMR to control access to the first portion of the TMR includes, for example, defining a set of buffers in the TMR that store the image data. The method further can include opening, at the computer vision processor, the FMR, and wherein selectively allowing the application to access the image data comprises allowing the application to access the image data while the FMR is open. The method, in some

embodiments, also includes acquiring, using the computer vision processor, the image data and storing the image data in the first portion of the TMR. In some embodiments, opening the FMR comprises providing information to a security processor that indicates that the FMR is open, wherein the security processor has a trusted relationship with the image cluster, and wherein receiving the FMR request comprises receiving the FMR request from the security processor while the FMR is open. The method also can include closing, at the computer vision processor, the FMR, and wherein selectively allowing the application to access the image data comprises denying the application access to the image data while the FMR is closed.

5 Closing the FMR comprises, for example, providing information to the security processor indicating that the FMR is closed, and wherein the security processor does not forward FMR requests to the computer vision processor while the FMR is closed. The method also can include setting, at the image cluster, the FMR as open or closed in response to user input.

15 In another aspect, a method includes providing, from an application in a processing cluster to a computer vision processor in an image cluster, a FMR request to access image data stored in a first portion of a TMR, receiving, at the application in response to providing the FMR request, an FMR response indicating whether the computer vision processor granted the application permission to access the image data in the first portion of the TMR, and selectively accessing, from the application, the image data based on the FMR response.

25 In accordance with yet another aspect, a method includes receiving, at a data fabric, a request from an image processing application to access image data stored in a portion of a TMR by an image cluster that has a trusted relationship with the TMR, wherein the request is received from an application in a processing cluster that does not have a trusted relationship with the TMR. The method further includes selectively permitting the image processing application to access the image data stored in the TMR based on whether the image cluster has opened or closed a fenced memory region (FMR) for the portion of the TMR.

30 In accordance with a further aspect, a computer system having at least one computer vision processor and is configured to perform one or more of the preceding methods.

BRIEF DESCRIPTION OF THE DRAWINGS

The present disclosure may be better understood, and its numerous features and advantages made apparent to those skilled in the art by referencing the accompanying drawings. The use of the same reference symbols in different
5 drawings indicates similar or identical items.

FIG. 1 is a block diagram of a processing system that supports secure computer vision processing according to some embodiments.

FIG. 2 is a message flow that includes messages used to selectively allow access to a trusted memory region (TMR) by untrusted applications according to
10 some embodiments.

FIG. 3 is a flow diagram of a method of selectively allowing untrusted applications to request access to portions of a TMR that are controlled by a fenced memory region (FMR) according to some embodiments.

DETAILED DESCRIPTION

15 In some computing architectures, separate clusters of processing elements are used to perform different computer vision tasks. An image cluster includes one or more processing elements (referred to herein as computer vision processors) that are configured to acquire the digital images for subsequent analysis. The image cluster receives data from image acquisition devices such as sensors, cameras, radar, and
20 the like. In some cases, the computer vision processor in the image cluster performs preprocessing on the acquired data such as resampling to a predetermined coordinate system, noise reduction, contrast enhancement, or scaling of the images. The image cluster then stores the acquired or postprocessed data in a memory region. A processing cluster accesses the acquired data from the memory region,
25 processes the acquired or postprocessed data, and stores the processing results in the memory region. The processing cluster is a user-facing cluster that also executes untrusted applications. Allowing untrusted applications to access computer vision data stored in the memory region could negatively impact user privacy. Requiring the image cluster to encrypt the data for storage in the memory region, e.g., using a
30 private key known only by the image cluster and the computer vision application in

the processing cluster, could provide privacy but this would significantly increase the processing overhead and reduce image processing throughput.

FIGs. 1-3 disclose a processing system in accordance with some embodiments that includes an image cluster and a processing cluster enforces security and privacy for computer vision data by allowing a computer vision processor in the image cluster to define a fenced memory region (FMR) that controls access to image data acquired or postprocessed by the image cluster. The computer vision processor in the image cluster stores the image data in a trusted memory region (TMR) that is accessible by trusted entities in the image cluster. The image cluster controls access to a portion of the TMR, such as a set of buffers in the TMR, that are associated with the FMR. The image cluster selectively allows the processing cluster to access information stored in the TMR in response to receiving an FMR request to access the information. Some embodiments of the image cluster receive FMR requests via a security processor, which acts as a trusted entity to control access to the image data in the TMR based on the FMR requests and responses. For example, the security processor receives an FMR request to access information in the TMR from an image processing application executing on the processing cluster and provides the request to the computer vision processor in the image cluster. The security processor grants access to the processing application if the image cluster grants the FMR request or denies access if the image cluster denies the FMR request. The image cluster only processes FMR requests if the FMR is opened by the image cluster. The security processor does not allow any untrusted application to access the TMR if image cluster closes the FMR.

A data fabric in the processing system, e.g., a memory controller and associated infrastructure, receives requests from the image processing application to access or store image data. The data fabric determines whether the locations indicated in the request are in buffers of the TMR that are accessible via FMR requests defined by the image cluster. If so and the image cluster has opened the FMR, the image processing application is permitted to send FMR requests to access the image data from the buffer or store the image data in the buffer. The image processing application is then able to access the image data if the image cluster grants the FMR request. If the memory request is to a portion of the TMR that is not accessible via

FMR requests, or if the image cluster has closed the FMR, the data fabric issues a memory access fault and the image processing application is not permitted to access or store the image data in the TMR. Other applications executing on the processing cluster are not permitted to access buffers in the TMR that are controlled by the FMR if the image cluster has closed the FMR. Some embodiments of the computer vision processor toggle the FMR policy, e.g., in response to user input. For example, if the user consents to recording of the image data, the computer vision processor toggles the FMR policy to allow the processing cluster to access and store image data outside the buffers in the TMR that are controlled by the FMR policy.

FIG. 1 is a block diagram of a processing system 100 that supports secure computer vision processing according to some embodiments. The processing system 100 includes an image cluster 105 that gathers, collects, or receives data from image acquisition devices such as a video camera 110. Some embodiments of the image cluster 105 gather, collect, or receive data from other sources such as sensors, cameras, radar, and the like. The video camera 110 records images such as a video of a user 115 that is in the field-of-view of the video camera 110. Information representative of the images, such as a stream of bits or frames, is generated in the video camera 110 and provided to the image cluster 105. In the illustrated embodiment, the image cluster 105 includes one or more processing elements such as the computer vision processor 120. A single computer vision processor 120 is shown in FIG. 1, although some embodiments of the image cluster 105 include more than one processing element that gathers, collects, or receives data from additional image or video sources.

The image cluster 105 stores the acquired data in a memory region 125 that has a trusted relationship with the image cluster 105. The memory region 125 is therefore referred to as a trusted memory region (TMR) 125. The trust relationship is established between the image cluster 105 and the TMR 125 using techniques such as handshaking protocols, authentication protocols, key exchange, hardware isolation, and the like. For example, the computer vision processor 120 stores information representing the image in a buffer 130 of the TMR 125, which also includes additional buffers for storing other images or data. Some embodiments of the computer vision processor 120 in the image cluster 105 perform preprocessing on

the acquired data such as resampling to a predetermined coordinate system, noise reduction, contrast enhancement, scaling of the images, and the like. The postprocessed image data is then stored in the buffer 130 of the TMR 125. The image data stored in the buffer 130 is considered secure because of the trusted relationship between the image cluster 105 and the TMR 125. The security and privacy of the user 115 is therefore protected by the trusted relationship between the image cluster 105 and the TMR 125. However, not all entities in the processing system 100 have a trusted relationship with the TMR 125.

The image cluster 105 exchanges information with the TMR 125 via a data fabric 135 implemented in the processing system 100. Some embodiments of the data fabric 135 include a memory controller and associated infrastructure to support an interface 140 between the image cluster 105 and the TMR 125. The associated infrastructure can include one or more buses, bridges, switches, routers, wires, traces, and the like. The interface 140 provides secure communication between the image cluster 105 and the TMR 125 due to the trusted relationship between these entities. For example, the data fabric 135 or the interface 140 can receive requests from the computer vision processor 120 to store information in the TMR 125. The data fabric 135 or the interface 140 verifies that the computer vision processor 120 is authorized to access the TMR 125 (e.g., using a key or password) and therefore provides the computer vision processor 120 with access to the TMR 125. Memory access requests from entities that are not authorized to access the TMR 125 are denied or rejected. For example, the data fabric 135 can issue a memory access fault in response to an access request from an unauthorized entity.

The processing system 100 includes a processing cluster 145 that executes applications such as the image processing application 150. The processing cluster 145 does not have a trusted relationship with the TMR 125. The image processing application 150 is therefore referred to as an untrusted application. Allowing untrusted applications to access computer vision data stored in the TMR 125 could negatively impact user privacy. However, preventing all untrusted applications from accessing data stored in the TMR 125, such as the images in the buffer 130, would severely limit the ability of the processing system 100 to utilize the image data stored in the TMR 125. Some embodiments of the image processing application 150 are

executed in the processing cluster 145 to extract high-level information from the images in the buffer 130 by automating tasks such as object recognition, motion analysis, scene reconstruction, and image restoration. Denying the image processing application 150 access to the images in the buffer 135 would therefore
5 limit the ability of the processing system 100 to process the images to generate high dimensional data that represents an “understanding” of the information in the images acquired by the image cluster 105.

In order to ensure the privacy and security of the user 115 while also allowing the processing cluster 145 to perform valuable operations on data stored in the TMR
10 125, the image cluster 105 selectively provides access to the TMR 125 by defining a fenced memory region (FMR) associated with a portion of the TMR 125. In the illustrated embodiment, the FMR defined by the image cluster 105 includes the buffers 130 that store the images acquired (and in some cases preprocessed) by the computer vision processor 120.

The image cluster 105 uses the FMR to control access to the image data stored in the portion of the TMR 125 that is associated with the FMR. Some embodiments of the computer vision processor 120 receive FMR requests from applications executing in the processing cluster 145 such as the image processing application 150. The FMR requests include requests to access image data in the buffers 130 in
20 the TMR 125. For example, the FMR request can include information such as an address indicating a location in the TMR 125. The computer vision processor 120 uses the address to determine that the FMR request is attempting to access the buffers 130 that are controlled by the FMR. The computer vision processor 120 selectively allows the image processing application 150 to access the image data in
25 the buffer 130, e.g., depending on whether the image cluster 105 or the computer vision processor 120 has opened or closed the FMR. Some embodiments of the image cluster 105 store (or have access to) a white list that indicates applications that should be given access to the buffers 130. The image cluster 105 can also provide access to the buffers 130 in response to the user 115 authorizing access or providing
30 an indication that the images in the buffer is 130 can be made publicly available.

Some embodiments of the processing system 100 include a security processor 155 that is a trusted entity. The security processor 155 controls access to the buffers

130 in the TMR 125 based on FMR requests generated by the processing cluster 145 and FMR responses provided by the image cluster 105. For example, the image cluster 105 can inform the security processor 155 that the image cluster 105 has opened the FMR. If the security processor 155 receives an FMR request to access information in the TMR 125 from the image processing application 150 while the FMR is open, the security processor 155 provides the FMR request to the image cluster 105, e.g., to the computer vision processor 120. In response to receiving the FMR request, the image cluster 105 selectively allows access to the TMR as indicated in an FMR response provided to the security processor 155. The security processor 155 grants access to the image processing application 150 if the image cluster 105 grants the FMR request or denies access if the image cluster 105 denies the FMR request. The image cluster 105 only processes FMR requests if the FMR is opened by the image cluster 105. The security processor 155 does not allow any untrusted application to access the TMR 125 if the image cluster 105 closes the FMR.

The data fabric 135 supports an interface 160 between the processing cluster 145 and the TMR 125. Some embodiments of the data fabric 135 selectively allow the processing cluster 145 (or the image processing application 150) to request access to portions of the TMR 125 based on the memory access request generated by the processing cluster 145 or the image processing application 150. The data fabric 135 determines whether the locations indicated in the request are in the buffer 130 of the TMR 125 that is accessible via FMR requests, as defined by the image cluster 105. If so and the image cluster 105 has opened the FMR, the processing cluster 145 or the image processing application 150 is permitted to send FMR requests to access the image data from the buffer 130 or store the image data in the buffer 130. The processing cluster 145 or the image processing application 150 is then able to access the image data if the image cluster 105 grants the FMR request. The data fabric 135 issues a memory access fault if the memory request is to a portion of the TMR 125 that is not accessible via FMR requests, or if the image cluster 105 has closed the FMR. In that case, the processing cluster 145 or the image processing application 150 is not permitted to access or store the image data in the TMR 125. Other applications executing on the processing cluster 145 are not permitted to access the buffer 130 in the TMR 125 that is controlled by the FMR if the image cluster 105 has closed the FMR.

The policy that controls access to the TMR 125 based on the FMR is modified based on user input in some cases. For example, the user 115 can make the image data in the buffer 130 publicly available by providing consent to an operator of the processing system 100. Some embodiments of image processor 105 or the
5 computer vision processor 120 toggle the FMR policy in response to user input. For example, if the user consents to recording of the image data, the computer vision processor 120 toggles the FMR policy to allow the processing cluster 145 to access and store image data outside the buffers 130 in the TMR 125 that are controlled by the FMR policy.

FIG. 2 is a message flow 200 that includes messages used to selectively allow access to a trusted memory region (TMR) by untrusted applications according to some embodiments. The message flow 200 includes messages exchanged between a computer vision processor (CV) in an image cluster, a secure processor (SEC), a processing cluster 205 that includes two applications (APP1, APP2), and the TMR,
15 which has a trusted relationship with the image cluster. The message flow 200 is therefore implemented in some embodiments of the processing system 100 shown in FIG. 1. The image cluster has defined an FMR associated with a portion of the TMR, such as a set of buffers implemented in the TMR.

At block 210, the computer vision processor in the image cluster opens the FMR
20 to allow untrusted applications to request access to the portion of the TMR controlled by the FMR. Although not shown in FIG. 2 in the interest of clarity, the computer vision processor notifies the secure processor and a data fabric such as the data fabric 135 shown in FIG. 1 that the image cluster has opened the FMR.

The first application (APP1) transmits an FMR request 215 to the computer
25 vision processor to request access to the FMR-controlled portion of the TMR. The FMR request includes information identifying the location of the requested portion of the TMR. In response to receiving the FMR request 215, the computer vision processor determines whether to grant the first application access to the buffers of the TMR. In the illustrated embodiment, the computer vision processor grants access
30 to the first application at block 225. For example, the first application can be on a white list of applications that are granted access to the TMR. The computer vision processor returns an FMR response 230 to the secure processor that indicates that

the computer vision processor has granted access to the first application. The secure processor forwards the FMR response 235 to the first application. In response to receiving the FMR response 235, the first application accesses the region in the TMR, e.g., over an interface supported by the data fabric, as indicated by the double-headed arrow 240.

The second application (APP2) transmits an FMR request 245 to the computer vision processor to request access to the FMR-controlled portion of the TMR. The FMR request includes information identifying the location of the requested portion of the TMR. In response to receiving the FMR request 245, the computer vision processor determines whether to grant the second application access to the buffers of the TMR. In the illustrated embodiment, the computer vision processor denies access to the second application at block 255. For example, the second application can be on a black list of applications that are not granted access to the TMR or the second application may not be on a white list of applications that are granted access to the TMR. The computer vision processor returns an FMR response 260 that indicates that the request is denied. The secure processor forwards the FMR response 265 to the second application to inform the second application that the request was denied. No interface is established between the second application and the TMR, thereby securing the information stored in the TMR from undesired or malicious access by the second application.

FIG. 3 is a flow diagram of a method 300 of selectively allowing untrusted applications to request access to portions of a TMR that are controlled by a fenced memory region (FMR) according to some embodiments. The method 300 is implemented in some embodiments of the data fabric 135 in the processing system 100 shown in FIG. 1.

At block 305, the data fabric receives a request from an untrusted application in a processing cluster to access images collected by an image cluster that has a trusted relationship with a TMR. For example, an image processing application in the processing cluster can transmit a memory access request including information indicating an address in memory that the image processing application would like to access.

At block 310, the data fabric determines whether the requested images are in the TMR. In some embodiments, the data fabric compares an address in the memory access request to an address range that corresponds to locations within the TMR. If the requested images are in the TMR, *e.g.*, as indicated by the address
5 being within the address range corresponding to the TMR, the method 300 flows to decision block 315. If the requested images are not in the TMR, *e.g.*, as indicated by the address being outside the address range corresponding to the TMR, the method 300 flows to block 320 and the data fabric allows the untrusted application to request or receive access to the images.

At decision block 315, the data fabric determines whether the memory access request is directed to a portion of the TMR that is controlled by an FMR defined by the image cluster. If the memory access request from the image processing application is directed to a portion of the TMR that is not controlled by an FMR, the data fabric denies the memory access request because the image processing
15 application is executing on the processing cluster, which does not have a trusted relationship with the TMR. The method 300 flows to block 325 and the data fabric issues a memory access fault to the untrusted image processing application. If the memory access request is directed to a portion of the TMR that is controlled by an FMR, the method 300 flows to decision block 330.

At decision block 335, the data fabric determines whether the image cluster (or computer vision processor) has opened the FMR to receive FMR requests to access the portion of the TMR that is controlled by the FMR. If not, the method 300 flows to block 325 and the data fabric issues a memory access fault to the untrusted image processing application. If the FMR is open, the method 300 flows to block 340 and
25 the data fabric allows the untrusted image processing application to request access to the images in the portion of the TMR that is controlled by the FMR. The image processing application can therefore transmit FMR requests to the image cluster via the data fabric.

A computer readable storage medium may include any non-transitory storage
30 medium, or combination of non-transitory storage media, accessible by a computer system during use to provide instructions and/or data to the computer system. Such storage media can include, but is not limited to, optical media (*e.g.*, compact disc

(CD), digital versatile disc (DVD), Blu-Ray disc), magnetic media (e.g., floppy disc, magnetic tape, or magnetic hard drive), volatile memory (e.g., random access memory (RAM) or cache), non-volatile memory (e.g., read-only memory (ROM) or Flash memory), or microelectromechanical systems (MEMS)-based storage media.

5 The computer readable storage medium may be embedded in the computing system (e.g., system RAM or ROM), fixedly attached to the computing system (e.g., a magnetic hard drive), removably attached to the computing system (e.g., an optical disc or Universal Serial Bus (USB)-based Flash memory), or coupled to the computer system via a wired or wireless network (e.g., network accessible storage (NAS)).

10 In some embodiments, certain aspects of the techniques described above may be implemented by one or more processors of a processing system executing software. The software includes one or more sets of executable instructions stored or otherwise tangibly embodied on a non-transitory computer readable storage medium. The software can include the instructions and certain data that, when
15 executed by the one or more processors, manipulate the one or more processors to perform one or more aspects of the techniques described above. The non-transitory computer readable storage medium can include, for example, a magnetic or optical disk storage device, solid state storage devices such as Flash memory, a cache, random access memory (RAM) or other non-volatile memory device or devices, and
20 the like. The executable instructions stored on the non-transitory computer readable storage medium may be in source code, assembly language code, object code, or other instruction format that is interpreted or otherwise executable by one or more processors.

Note that not all of the activities or elements described above in the general
25 description are required, that a portion of a specific activity or device may not be required, and that one or more further activities may be performed, or elements included, in addition to those described. Still further, the order in which activities are listed are not necessarily the order in which they are performed. Also, the concepts have been described with reference to specific embodiments. However, one of
30 ordinary skill in the art appreciates that various modifications and changes can be made without departing from the scope of the present disclosure as set forth in the claims below. Accordingly, the specification and figures are to be regarded in an

illustrative rather than a restrictive sense, and all such modifications are intended to be included within the scope of the present disclosure.

Benefits, other advantages, and solutions to problems have been described above with regard to specific embodiments. However, the benefits, advantages, solutions to problems, and any feature(s) that may cause any benefit, advantage, or
5 solution to occur or become more pronounced are not to be construed as a critical, required, or essential feature of any or all the claims. Moreover, the particular embodiments disclosed above are illustrative only, as the disclosed subject matter may be modified and practiced in different but equivalent manners apparent to those
10 skilled in the art having the benefit of the teachings herein. No limitations are intended to the details of construction or design herein shown, other than as described in the claims below. It is therefore evident that the particular embodiments disclosed above may be altered or modified and all such variations are considered within the scope of the disclosed subject matter. Accordingly, the protection sought
15 herein is as set forth in the claims below.

WHAT IS CLAIMED IS:

1. A method comprising:
 - defining, at a computer vision processor in an image cluster, a fenced memory region (FMR) that controls access to image data stored in a first portion of a trusted memory region (TMR);
 - 5 receiving, at the computer vision processor from an application implemented in a processing cluster, an FMR request to access the image data in the first portion of the TMR; and
 - selectively allowing, at the computer vision processor, the application to access the image data in response to receiving the FMR request.
- 10 2. The method of claim 1, wherein defining the FMR to control access to the first portion of the TMR comprises defining a set of buffers in the TMR that store the image data.
3. The method of claim 1, further comprising:
 - opening, at the computer vision processor, the FMR, and wherein selectively
 - 15 allowing the application to access the image data comprises allowing the application to access the image data while the FMR is open.
4. The method of any of claims 1 to 3, further comprising:
 - acquiring, using the computer vision processor, the image data and storing the image data in the first portion of the TMR.
- 20 5. The method of claim 4, wherein opening the FMR comprises providing information to a security processor that indicates that the FMR is open, wherein the security processor has a trusted relationship with the image cluster, and wherein receiving the FMR request comprises receiving the FMR request from the security processor while the FMR is open.
- 25 6. The method of claim 5, further comprising:
 - closing, at the computer vision processor, the FMR, and wherein selectively allowing the application to access the image data comprises denying the application access to the image data while the FMR is closed.

7. The method of claim 6, wherein closing the FMR comprises providing information to the security processor indicating that the FMR is closed, and wherein the security processor does not forward FMR requests to the computer vision processor while the FMR is closed.

5 8. The method of any of the preceding claims, further comprising:
setting, at the image cluster, the FMR as open or closed in response to user input.

9. A computer system having at least one computer vision processor to perform the method of any of claims 1 to 8.

10 10. A method comprising:
providing, from an application in a processing cluster to a computer vision processor in an image cluster, a fenced memory region (FMR) request to access image data stored in a first portion of a trusted memory region (TMR);
15 receiving, at the application in response to providing the FMR request, an FMR response indicating whether the computer vision processor granted the application permission to access the image data in the first portion of the TMR; and
selectively accessing, from the application, the image data based on the FMR
20 response.

11. The method of claim 10, wherein the image data is acquired by the computer vision processor and the computer vision processor stores the image data in the first portion of the TMR.

12. The method of claim 11, wherein the image data is stored in a set of buffers in the TMR, and wherein the FMR is defined to control access to the set of buffers in the TMR.
25

13. The method of any of claims 10 to 12, wherein the application receives the FMR response indicating that the computer vision processor granted access to the image data in response to the computer vision processor opening the FMR.

14. The method of claim 13, wherein receiving the FMR response comprises receiving the FMR response from a security processor while the FMR is open, wherein the security processor has a trusted relationship with the image cluster.

15. The method of claim 14, wherein the application receives the FMR response denying access to the image data in response to the computer vision processor closing the FMR.

16. The method of claim 15, wherein the application receives the FMR response denying access to the image data from the security processor while the FMR is closed, and wherein the security processor does not forward FMR requests to the computer vision processor while the FMR is closed.

17. A computer system having at least one computer vision processor to perform the method of any of claims 11 to 17.

18. A method comprising:

receiving, at a data fabric, a request from an image processing application to access image data stored in a portion of a trusted memory region (TMR) by an image cluster that has a trusted relationship with the TMR, wherein the request is received from an application in a processing cluster that does not have a trusted relationship with the TMR; and selectively permitting the image processing application to access the image data stored in the TMR based on whether the image cluster has opened or closed a fenced memory region (FMR) for the portion of the TMR.

19. The method of claim 18, wherein receiving the request comprises receiving the request including information indicating a location in the TMR, and wherein selectively permitting the image processing application to access the image data comprises determining whether the location indicated in the request is in the portion of the TMR that is accessible via FMR requests.

20. The method of claim 19, wherein selectively permitting the image processing application to access the image data comprises permitting the image processing application to access the image data if the location is in the portion of the TMR that is accessible via FMR requests and the image cluster has opened the FMR.

21. The method of claim 20, wherein selectively permitting the image processing application to access the image data comprises providing a memory access fault to the image processing application if the location is not in the portion of the TMR that is accessible via FMR requests.

- 5 22. The method of claim 20, further comprising:
issuing memory access faults in response to requests to access the portion of
the TMR while the image cluster has closed the FMR.

23. A computer system having at least one computer vision processor to perform the method of any of claims 18 to 22.

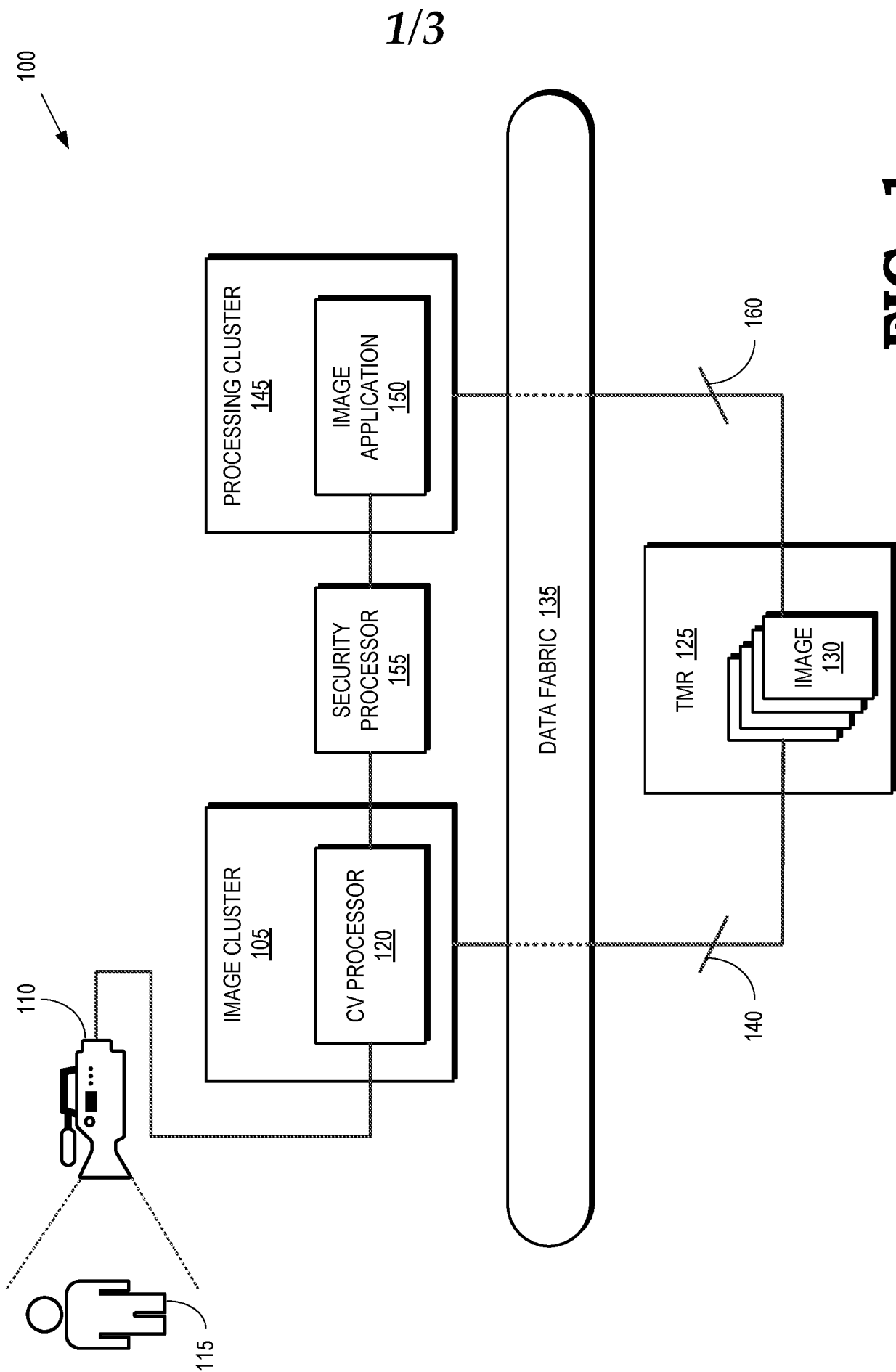
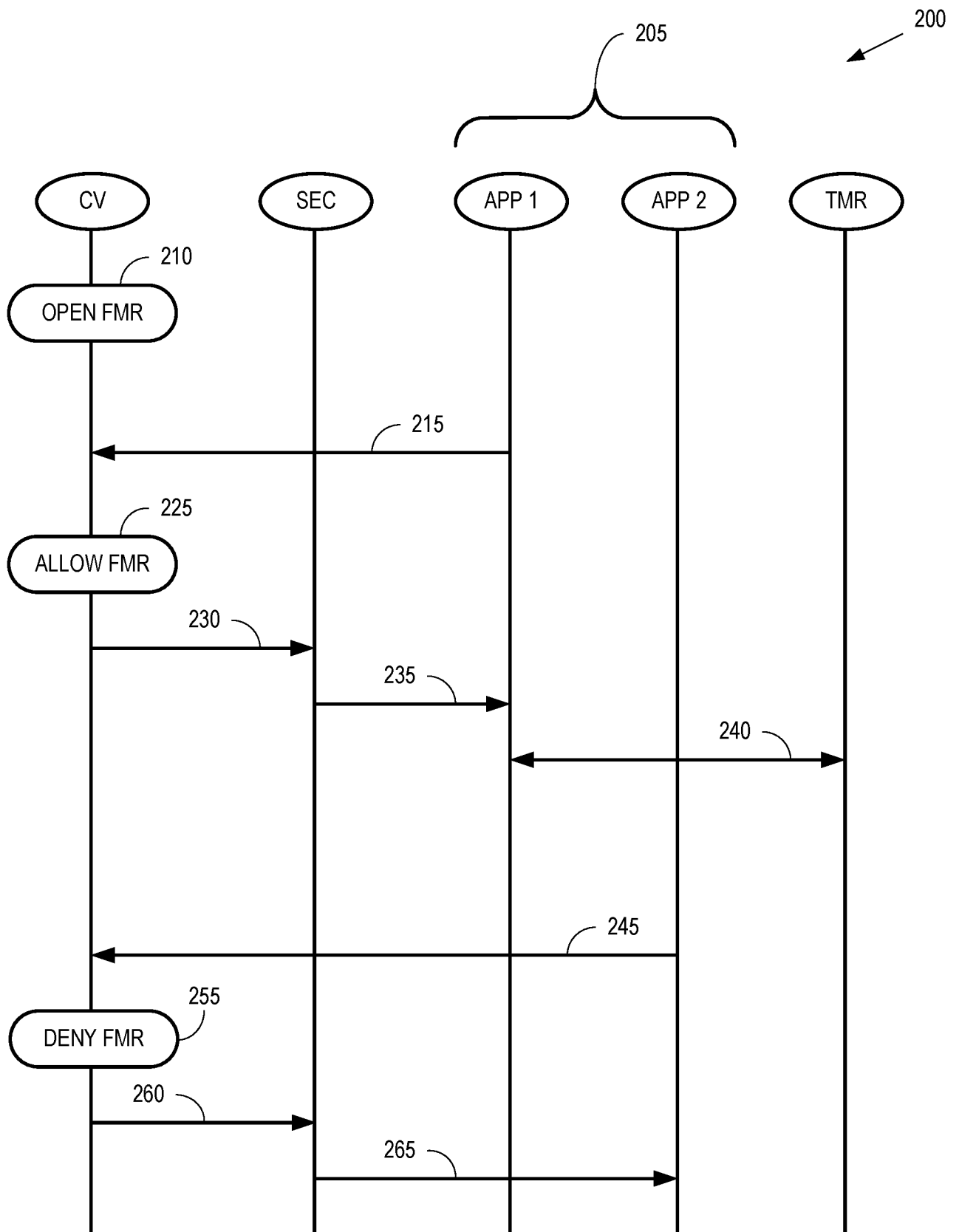
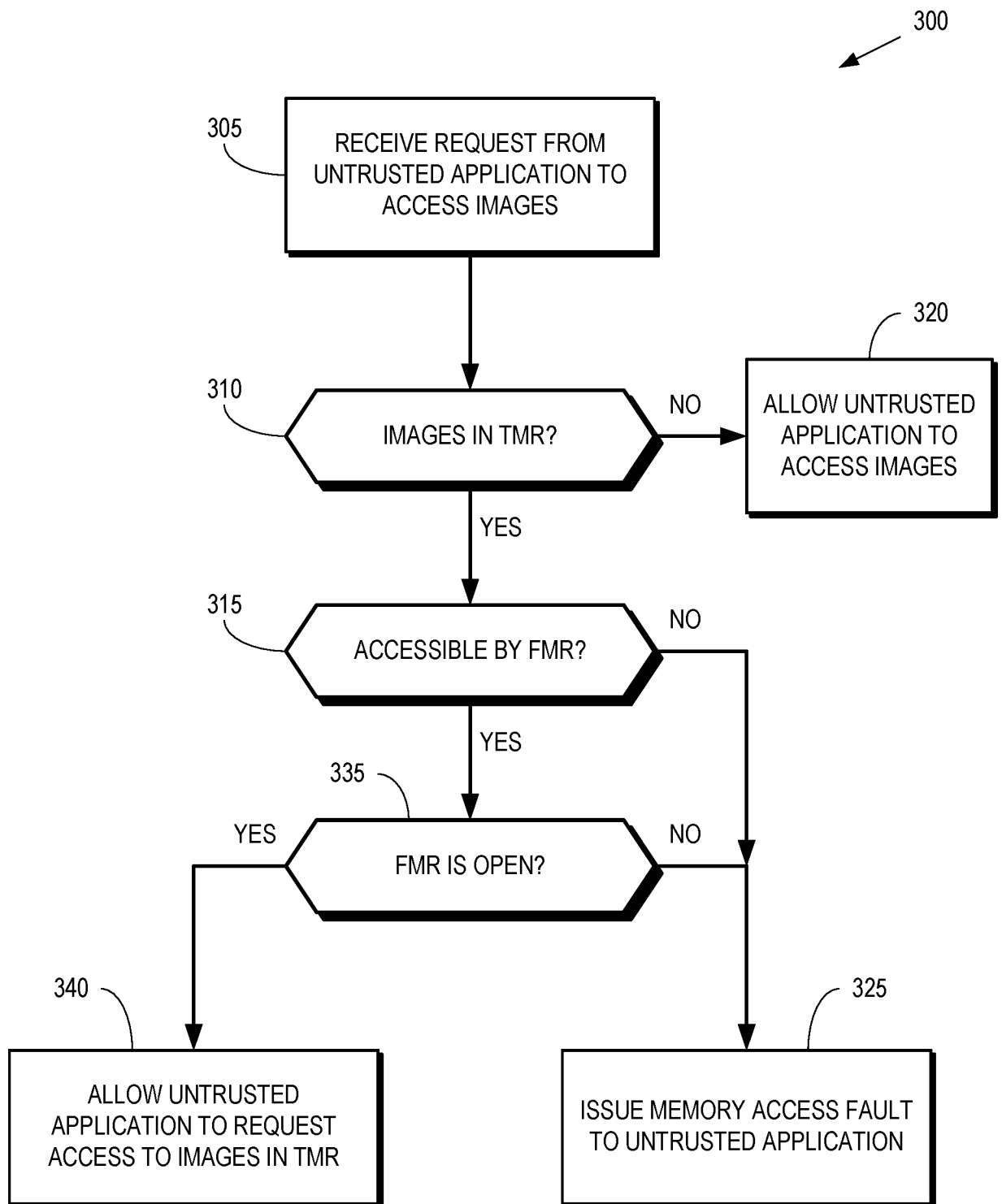


FIG. 1

2/3

**FIG. 2**

3/3

**FIG. 3**

A. CLASSIFICATION OF SUBJECT MATTER**G06F 21/53(2013.01)i, G06F 21/60(2013.01)i, G06F 21/71(2013.01)i**

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)

G06F 21/53; G06F 12/14; G06F 21/62; G06F 21/78; G06T 1/60; H04L 9/32; G06F 21/60; G06F 21/71

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Korean utility models and applications for utility models

Japanese utility models and applications for utility models

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)

eKOMPASS(KIPO internal) & keywords: fenced memory region (FMR), trusted memory region (TMR), access, selectively allowing, address, open/close**C. DOCUMENTS CONSIDERED TO BE RELEVANT**

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	US 2013-0305342 A1 (QUALCOMM INCORPORATED) 14 November 2013 paragraphs [0037], [0053]-[0054], [0101]; claims 1, 5; and figures 2A, 6A, 12	1-2,4,9-12,17
Y		3,5-8,13-16,18-23
Y	US 2008-0109662 A1 (VENKAT NATARAJAN et al.) 08 May 2008 paragraph [0036]; claims 1-2, 6; and figure 4	3,5-8,13-16,18-23
A	US 2018-0307867 A1 (LANCE W. DOVER) 25 October 2018 paragraphs [0025]-[0031]; claims 1, 7, 9; and figure 1	1-23
A	US 2014-0230067 A1 (RAVI L. SAHITA et al.) 14 August 2014 paragraphs [0022]-[0056]; claims 1-3; and figures 1-3	1-23
A	US 2011-0289294 A1 (MANABU MAEDA et al.) 24 November 2011 paragraphs [0022], [0202]-[0207], [0238]-[0250]; claims 1, 9; and figures 14, 21	1-23



Further documents are listed in the continuation of Box C.



See patent family annex.

* Special categories of cited documents:

"A" document defining the general state of the art which is not considered to be of particular relevance

"D" document cited by the applicant in the international application

"E" earlier application or patent but published on or after the international filing date

"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)

"O" document referring to an oral disclosure, use, exhibition or other means

"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art

"&" document member of the same patent family

Date of the actual completion of the international search

22 April 2020 (22.04.2020)

Date of mailing of the international search report

23 April 2020 (23.04.2020)

Name and mailing address of the ISA/KR

International Application Division

Korean Intellectual Property Office

189 Cheongsa-ro, Seo-gu, Daejeon, 35208, Republic of Korea

Facsimile No. +82-42-481-8578

Authorized officer

KIM, Sung Hee

Telephone No. +82-42-481-3516



INTERNATIONAL SEARCH REPORT

Information on patent family members

International application No.

PCT/US2019/066615

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
US 2013-0305342 A1	14/11/2013	CN 104272752 A CN 104272752 B EP 2847703 A1 EP 2847703 B1 US 8910307 B2 WO 2013-169446 A1	07/01/2015 15/12/2017 18/03/2015 18/12/2019 09/12/2014 14/11/2013
US 2008-0109662 A1	08/05/2008	TW 200844787 A TW I370983 B US 8190919 B2 WO 2008-058152 A2 WO 2008-058152 A3	16/11/2008 21/08/2012 29/05/2012 15/05/2008 17/07/2008
US 2018-0307867 A1	25/10/2018	CN 110651261 A WO 2018-195433 A1	03/01/2020 25/10/2018
US 2014-0230067 A1	14/08/2014	BR 102014003201 A2 CN 103984894 A CN 103984894 B EP 2765530 A1 EP 2765530 B1 US 9158942 B2	04/08/2015 13/08/2014 13/10/2017 13/08/2014 17/01/2018 13/10/2015
US 2011-0289294 A1	24/11/2011	EP 2515239 A1 EP 2515239 B1 JP 5631334 B2 WO 2011-074168 A1	24/10/2012 29/03/2017 26/11/2014 23/06/2011