



- (51) **International Patent Classification:**
H04N 21/441 (2011.01) *H04N 21/41* (2011.01)
- (21) **International Application Number:**
PCT/US2013/059940
- (22) **International Filing Date:**
16 September 2013 (16.09.2013)
- (25) **Filing Language:** English
- (26) **Publication Language:** English
- (30) **Priority Data:**
13/621,691 17 September 2012 (17.09.2012) US
- (72) **Inventors; and**
- (71) **Applicants :** **CHAN, Alistair K.** [US/US]; 9769 NE Morden Cove Dr., Bainbridge Island, Washington 98110 (US). **DUNCAN, William D.** [US/US]; 12204 NE 109th Way, Kirkland, Washington 98033 (US). **GATES, William** [US/US]; One Microsoft Way, Redmond, Washington 98052-6399 (US). **GERRITY, Daniel A.** [US/US]; 720 Queen Anne Ave N #510, Seattle, Washington 98109 (US). **HOLMAN, Paul** [US/US]; 2431 7th Ave N, Seattle, Washington 98119 (US). **HYDE, Roderick A.** [US/US]; 9915 - 161st Avenue N.E., Redmond, Washington 98052 (US). **JUNG, Edward K.Y.** [US/US]; 10091 Park Run Drive #200, Las Vegas, Nevada 89145 (US). **KARE, Jordin T.** [US/US]; 908 15th Ave. East, Seattle, Washington 98112 (US). **LEVIEN, Royce A.** [US/US]; 43 Somerset Road, Lexington, Massachusetts 02420-3519 (US). **LORD, Robert W.** [US/US]; 1410 41st Avenue East, Seattle, Washington 98112 (US). **LORD, Richard T.** [US/US]; 505 Broadway #405, Tacoma, Washington

98402 (US). **MALAMUD, Mark A.** [US/US]; 1508 Ninth Ave W, Seattle, Washington 98119 (US). **MYHRVOLD, Nathan P.** [US/US]; 11235 SE 6th Street, Suite 200, Bellevue, Washington 98004 (US). **ROSEMA, Keith D.** [US/US]; 501 Columbia Street NW Box H, Olympia, Washington 98501 (US). **TEGREENE, Clarence T.** [US/US]; 5910 E Mercer Way, Mercer Island, Washington 98040 (US). **WOOD, Lowell L., Jr.** [US/US]; 989 112th Avenue NE #2310, Bellevue, Washington 98004 (US).

(74) **Agents:** **CHAN, Alistair K.** et al.; 11235 SE 6th Street, Suite 200, Bellevue, Washington 98004-6841 (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, DK, DM, DO, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, GT, HN, HR, HU, ID, IL, IN, IS, JP, KE, KG, KN, KP, KR, KZ, LA, LC, LK, LR, LS, LT, LU, LY, MA, MD, ME, MG, MK, MN, MW, MX, MY, MZ, NA, NG, NI, NO, NZ, 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, 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,

[Continued on next page]

(54) **Title:** UNAUTHORIZED VIEWER DETECTION SYSTEM AND METHOD

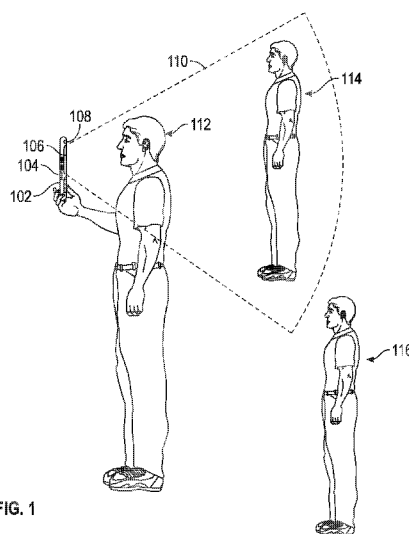


FIG. 1

(57) **Abstract:** A system for detecting intruding viewers of a display and responding to an intrusion by editing content. The system includes an electronic media display, a sensor, and a processing circuit. The processing circuit is configured to obtain information from the sensor, determine a visibility envelope of the electronic media display device, analyze the information from the sensor to determine a presence of an intruder within the visibility envelope, distinguish the intruder from an authorized user, and edit any displayed content.

WO 2014/043620 A1



TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, **Published:**
KM, ML, MR, NE, SN, TD, TG).

— *with international search report (Art. 21(3))*

UNAUTHORIZED VIEWER DETECTION SYSTEM AND METHOD

BACKGROUND

[0001] Many times a person is watching some video or viewing some content on an electronic display device that he does not want others to know he is viewing. However, due to the nature of viewing an electronic display device, he may never know when a collateral viewer is intruding on his content. Because he may not be aware that others are looking at his electronic display device, his sensitive content may be viewed by others without his permission. Thus, there is a need for improved systems and methods of detecting intruding viewers of electronic displays and automatically editing content accordingly.

SUMMARY

[0002] One exemplary embodiment relates to a system for detecting viewers of a display and responding to an intrusion. The system includes an electronic media display device configured to display content, a sensor, and a processing circuit. The processing circuit is configured to obtain information from the sensor, determine a visibility envelope of the electronic media display device, analyze the information from the sensor to determine a presence of an intruder within the visibility envelope, distinguish the intruder from an authorized user, and edit any displayed content.

[0003] Another exemplary embodiment relates to a method for detecting intruding viewers of a display and responding to an intrusion. The method includes displaying content on an electronic media display device, obtaining information from a sensor, determining a visibility envelope of the display device, analyzing the information to determine a presence of an intruder within the visibility envelope, distinguishing the intruder from an authorized user, and editing any displayed content.

[0004] Another exemplary embodiment relates to a method for detecting intruding viewers of a display of a camera-equipped mobile communication device and responding to an intrusion. The method includes obtaining input from a camera of the mobile communication device, determining an area within which a viewer can resolve any visual content, analyzing the input to determine a presence of an intruder within the area,

distinguishing the intruder from an authorized user, and responding to the presence of the intruder by editing the visual content.

[0005] Another exemplary embodiment relates to a non-transitory computer-readable medium having instructions stored thereon. The instructions include instructions to
5 interface with an electronic media display device that is configured to display content, instructions to obtain information from a sensor, instructions for determining an area within which a viewer can resolve any visual content, instructions to analyze the information to determine a presence of an intruder within the area, and instructions for editing the visual content if the presence of an intruder is detected.

10 [0006] The invention is capable of other embodiments and of being carried out in various ways. Alternative exemplary embodiments relate to other features and combinations of features as may be generally recited in the claims.

[0007] The foregoing is a summary and thus by necessity contains simplifications, generalizations and omissions of detail. Consequently, those skilled in the art will
15 appreciate that the summary is illustrative only and is not intended to be in any way limiting. Other aspects, inventive features, and advantages of the devices and/or processes described herein, as defined solely by the claims, will become apparent in the detailed description set forth herein and taken in conjunction with the accompanying drawings.

BRIEF DESCRIPTION OF THE FIGURES

20 [0008] The invention will become more fully understood from the following detailed description taken in conjunction with the accompanying drawings wherein like reference numerals refer to like elements, in which:

[0009] FIG. 1 is a schematic diagram of an electronic media display device and a visibility envelope, shown according to an exemplary embodiment.

25 [0010] FIG. 2 is a block diagram of an electronic media display device, a sensor, and a processing circuit, shown according to an exemplary embodiment.

[0011] FIG. 3 is a detailed block diagram of a processing circuit, shown according to an exemplary embodiment.

[0012] FIG. 4 is a schematic diagram of an electronic media display device, a sensor, and a processing circuit, shown according to an exemplary embodiment.

[0013] FIG. 5 is a schematic diagram of a visibility envelope, shown according to an exemplary embodiment.

5 [0014] FIG. 6 is a schematic diagram of a visibility envelope, shown according to an exemplary embodiment.

[0015] FIG. 7 is a schematic diagram of a visibility envelope, shown according to an alternative embodiment.

10 [0016] FIG. 8 is a schematic diagram of an electronic media display device, a sensor, a processing circuit, and a visibility envelope, shown according to an alternative embodiment.

[0017] FIG. 9 is a flowchart of a process for detecting and reacting to an intruding viewer of an electronic media display device, shown according to an exemplary embodiment.

15 [0018] FIG. 10 is a flowchart of a process for detecting and reacting to an intruding viewer of an electronic media display device, shown according to an alternative embodiment.

20 [0019] FIG. 11 is a flowchart of a general process for detecting and reacting to an intruding viewer of an electronic media display device, shown according to an exemplary embodiment.

[0020] FIG. 12 is a flowchart of a process for performing analysis of intruding viewers of an electronic media display device, shown according to an exemplary embodiment.

DETAILED DESCRIPTION

25 [0021] Before turning to the figures, which illustrate the exemplary embodiments in detail, it should be understood that the application is not limited to the details or methodology set forth in the description or illustrated in the figures. It should also be

understood that the terminology is for the purpose of description only and should not be regarded as limiting.

[0022] Referring generally to the Figures, systems and methods for detecting intruding viewers of a display and editing content accordingly are shown and described. A person
5 may be operating an electronic media display device (e.g. a cellular phone, a tablet computer, a laptop computer, an eBook reading device, an ATM machine, a music player, a video player, a medical display, or any other device with an electronic display that is displaying content). The electronic media display device may be a fixed device or a mobile device. The person may be viewing sensitive content (e.g. private photographs,
10 private videos, financial records, medical records, or any other content that the person may not want other people to view). A collateral viewer may be behind the person, in a position to view the content, without the knowledge or permission of the person. Utilizing a sensor (e.g. a camera attached to the device, radar sensor, micropower impulse radar (MIR), light detection and ranging technology, microphone, ultrasonic sensor, infrared
15 sensor, near-infrared (NIR) sensor, or any other sensor that is capable of measuring the range and/or position of objects) the intruder may be detected, and action may be taken to prevent the content from being resolved.

[0023] The intruder may be detected by determining a visibility envelope of the electronic media display device, and the performing analysis to determine an intruder's
20 presence and location within the visibility envelope. Use of a visibility envelope can be advantageous in order to distinguish intruders who are capable of viewing and recognizing the contents of the display from ones who are capable of seeing the display but not of actually recognizing content displayed on it. By making this distinction, the display can take protective action (e.g., editing or modifying the display contents) only when
25 necessary to prevent content being recognized, and not for the case of intruders who are not within the visibility envelope of the display and do not pose a significant threat to the privacy of the displayed content. This reduction in the use of protective action can reduce the inconvenience to the user and disruption of the user's viewing activities that universal protective actions would entail. The intruder's presence may be based in part on his
30 distance from the electronic media display device. The visibility envelope may be generated by a processing circuit, which accepts information from a sensor. The information may be of the electronic media display device's surroundings. The processing

circuit may use the information to determine the presence of an intruder within the visibility envelope based on the distance and viewing angle of the intruder. The processing circuit may perform an analysis of the distance and viewing angle of the intruder and determine whether action needs to be taken to edit or change the content that the electronic media display device is displaying. According to an alternative embodiment, in determining the presence of the intruder, the processing circuit may also perform red eye detection analysis, resolution analysis, and display brightness analysis.

[0024] The system may be enabled or disabled by a user as the user desires. The threshold of when and what action should be taken may be specified by a preference file or by default values. The actions may include editing or changing of the content (e.g. turning off the display, switching the content to another content, degrading the visibility of the content, warning the user with an alert, or any other editing of the content).

[0025] For purposes of this disclosure, the term “coupled” means the joining of two members directly or indirectly to one another. Such joining may be stationary in nature or moveable in nature and such joining may allow for the flow of electricity, electrical signals, or other types of signals or communication between the two members. Such joining may be achieved with the two members or the two members and any additional intermediate members being integrally formed as a single unitary body with one another or with the two members or the two members and any additional intermediate members being attached to one another. Such joining may be permanent in nature or alternatively may be removable or releasable in nature.

[0026] Referring to FIG. 1, a visibility envelope 110 is shown. Visibility envelope 110 is generated by mobile device 102 having a sensor 108, electronic media display 106, and processing circuit 104. Sensor 108 may be a camera, or other appropriate sensor. Electronic media display 106 may be an LCD screen, an e-Paper screen, or any other electronic media display capable of displaying content. Mobile device 102 is shown as a cellular phone, but it may be a tablet computer, a portable movie player, or other mobile devices. The systems and methods of the present disclosure are not limited based on the type of mobile device, the type of the sensor, type of electronic media display, or the type of processing circuit.

[0027] User 112 is shown as operating mobile device 102. Electronic media display 106 may be showing textual content, video content, photographic content, or any other type of electronic content. The systems and methods of the present disclosure are not limited based on the type of electronic content being displayed.

5 [0028] Visibility envelope 110 is shown as being generated for a certain range. Viewer 116 and intruder 114 are shown. Viewer 116 is depicted as being too far away from the electronic media display 106 to resolve the content on the screen thereof, and thus outside of visibility envelope 110. Intruder 114 is depicted as being within visibility envelope 110. The systems and methods of the present disclosure are not limited based on the
10 number or position of viewers and intruders. As an example, an intruder may be within the visibility envelope, and thus any content being displayed by electronic media display 106 may be removed or edited to stop the intruder from viewing the content. However, in the same example, another viewer may be too far out of range, and not within the visibility envelope. The system may not react to the presence of the out of range viewer.

15 [0029] Referring to FIG. 2, a block diagram of a system 100 for executing the systems and methods of the present disclosure is shown. System 100 includes sensor 200 for detecting information about the environment around system 100. The information that sensor 200 detects may be provided to processing circuit 300. Processing circuit 300 may process the information, generate a visibility envelope, use the processed information to
20 determine the location and threat of any intruding viewers within the visibility envelope, and make a determination of whether or not to edit content on electronic media display 400. Sensor 200 may be coupled to electronic media display 400, and processing circuit 300 may be coupled to electronic media display 400. While depicted as separate modules in FIG. 2, sensor 200, processing circuit 300, and electronic media display 400 may be
25 part of one device. For example, sensor 200 may be the camera of a camera-equipped cellular phone, processing circuit 300 may be the processor or a separate module within the cellular phone, and electronic media display 400 may be the display of the cellular phone. As another example, sensor 200 may be the camera of a camera-equipped laptop, processing circuit 300 may be the processor within the laptop, and electronic media
30 display 400 may be the LCD display of the laptop.

[0030] Referring now to FIG. 3, a more detailed block diagram of processing circuit 300 for completing the systems and methods of the present disclosure is shown, according to an exemplary embodiment. Processing circuit 300 may be processing circuit 104 of FIG. 1. Processing circuit 300 is generally configured to accept input from an outside source (e.g. a sensor, a camera, etc.) in addition to other information (e.g. configuration data, preference data files, etc.). Input may be accepted continuously or periodically. Processing circuit 300 is then configured to use the accepted information to analyze information related to the environment, determine a visibility envelope, analyze the visibility envelope and determine intruders, determine if any content should be edited, and control the editing of content.

[0031] Processing circuit 300 includes processor 318. Processor 318 may be implemented as a general purpose processor, an application specific integrated circuit (ASIC), one or more field programmable gate arrays (FPGAs), a group of processing components, or other suitable electronic processing components. Processing circuit 300 also includes memory 302. Memory 302 is one or more devices (e.g., RAM, ROM, Flash Memory, hard disk storage, etc.) for storing data and/or computer code for facilitating the various processes described herein. Memory 302 may be or include non-transient volatile memory or non-volatile memory. Memory 302 may include database components, object code components, script components, or any other type of information structure for supporting the various activities and information structures described herein. Memory 302 may be communicably connected to the processor 318 and include computer code or instructions for executing the processes described herein (e.g., the processes shown in FIGS. 9-13).

[0032] Memory 302 includes memory buffer 304. Memory buffer 304 is configured to receive data from a sensor, (e.g. sensor 200) through input 320. The sensor data may include image or video data, or radar information, light detection and ranging information, infrared information, sonic or ultrasonic information, or content information (e.g., content information related to electronic media display 400). The image or video data, for example, may be photographs taken by sensor 108. The data receive through input 320 may be stored in memory buffer 304 until memory buffer 304 is accessed for data by the various modules of memory 302. For example, the visibility envelope module may access the image or video data that is stored in memory buffer 304.

[0033] The memory 302 further includes configuration data 312. Configuration data 312 includes data relating to processing circuit 300. For example, configuration data 312 may include information relating to interfacing with an electronic media display. This may include the command set needed to interface with graphic display components, for example a graphics processing unit (GPU). As another example, the configuration data 312 may include information as to how often input should be accepted from sensor 200 and how often the environment should be scanned for intruders. As another example, configuration data 312 may include data to configure the communication between the various components of processing circuit 300.

[0034] Memory 302 further includes user interface module 306. User interface module 306 is configured to receive input data through input 320. User interface module 306 is further configured to interpret the data for the other modules of processing circuit 300. For example, user interface module 306 may receive a cancel request, wherein a user requests an end to editing of the content, and user interface module 306 may be configured to receive that request and provide appropriate commands to edit generation module 316 to cease editing. User interface module 306 may also generate a user interface to allow a user to control edit generation module 316, as well as edit preference data 310. As another example, the user interface module may receive a request to begin scanning for intruders, and user interface module 306 may be configured to use that request and provide appropriate commands to enable the system.

[0035] Memory 302 further includes modules 308, 310, 314, and 316, for executing the systems and methods described herein. Modules 308, 310, 314, and 316 are configured to receive image and video data, sensor information, radar information, light detection and range information, infrared information, sonic or ultrasonic information, preference data, and other data as provided by processing circuit 300. Modules 308, 310, 314, and 316 are configured to analyze the data, generate a visibility envelope, determine viewers and their characteristics (range, location, etc.), determine whether intruders are present within the visibility envelope limits, and determine whether to edit content on an electronic media display.

[0036] Visibility envelope module 314 is configured to receive range and angle information. The information may be provided by configuration data 312, or by

preference data 310. Visibility envelope module 314 is configured to interpret the range and angle information and determine a visibility envelope based on the information. The visibility envelope may be a representation of a danger zone of the device. For example, any person(s) within the visibility envelope may be classified as intruders, and may have the potential of being able to resolve content of electronic media display 300.

[0037] In an exemplary embodiment, visibility envelope module 314 receives from configuration data 312 a range R_{m1} and a viewing angle θ_{m1} . Range R_{m1} represents a maximum range over which an electronic media display (e.g. electronic media display 400) may be viewed such that the electronic media display's contents may be resolved.

Viewing angle θ_{m1} represents a maximum angle over which an electronic media display (e.g. electronic media display 400) may be viewed such that the electronic media display's contents may be resolved. Range R_{m1} and viewing angle θ_{m1} may correspond to the specifications of the electronic media display. Visibility envelope module 314 may provide the visibility envelope information R_{m1} and θ_{m1} to intruder analysis module 308.

While the discussion of the visibility envelope herein is generally in terms of independent bounds on range, R_{m1} , and viewing angle, θ_{m1} , in some embodiments, the visibility envelope can be given by a functional relationship, such as $R_{m1}(\theta_{m1})$, in which the range is a function of the viewing angle, θ_{m1} . For instance, R_{m1} can be larger for $\theta_{m1} = 0$, than for $\theta_{m1} = 20^\circ$. In some embodiments, the visibility envelope depends on a two dimensional viewing angle (e.g., on azimuth and elevation) relative to the display's axes, not simply on the polar angle from the display's normal vector, θ_{m1} .

[0038] In another exemplary embodiment, visibility envelope module 314 receives from preference data 310 a range R_{m2} and a viewing angle θ_{m2} . The viewing angle R_{m2} represents a maximum range specified by a user for analysis. The viewing angle θ_{m2} represents a maximum angle specified by a user for analysis. For example, a user may not be concerned about any viewers more than a certain angle to the side of his device, and can specify as such in the preferences. As another example, a user may not be concerned about viewers who are greater than a certain distance away from the device, and can specify as such in the preferences. Visibility envelope module 314 may provide the visibility envelope information R_{m2} and θ_{m2} to intruder analysis module 308.

[0039] In one embodiment, visibility envelope module 314 receives from configuration data 312 a range R_{m3} and a viewing angle θ_{m3} . Range R_{m3} represents a maximum range over which an electronic media display (e.g. electronic media display 400) may be viewed such that the electronic media display's contents may be resolved. Viewing angle θ_{m3} represents a maximum angle over which an electronic media display (e.g. electronic media display 400) may be viewed such that the electronic media display's contents may be resolved. Additionally, visibility envelope module 314 receives a brightness level B of the electronic media display's brightness level. Visibility envelope module 314 then adjusts R_{m3} and θ_{m3} according to brightness B . For example, if the electronic media display's brightness is at a maximum level, R_{m3} and θ_{m3} may be increased, and if the electronic media display's brightness is at a minimum level, R_{m3} and θ_{m3} may be decreased. Additionally, visibility envelope module 314 receives a brightness level B_a of the ambient environment's brightness level and/or its polarization. Visibility envelope module 314 then adjusts R_{m3} and θ_{m3} according to brightness B_a . For example, if the ambient brightness is at a maximum level, R_{m3} and θ_{m3} may be decreased, and if the ambient brightness is at a minimum level, R_{m3} and θ_{m3} may be increased. Visibility envelope module 314 may provide the adjusted visibility envelope information R_{m3}' and θ_{m3}' to intruder analysis module 308.

[0040] In one embodiment, visibility envelope module 314 receives from configuration data 312 a range R_{m4} and a viewing angle θ_{m4} . Range R_{m4} represents a maximum range over which an electronic media display (e.g. electronic media display 400) may be viewed such that the electronic media display's contents may be resolved. Viewing angle θ_{m4} represents a maximum angle over which an electronic media display (e.g. electronic media display 400) may be viewed such that the electronic media display's contents may be resolved. Additionally, visibility envelope module 314 receives a content type description of the primary content type that is being displayed on the electronic media display. Visibility envelope module 314 then adjusts R_{m4} and θ_{m4} according to the content type. For example, if the content type is photographic content, R_{m4} and θ_{m4} may be increased. If the content type is textual content, R_{m4} and θ_{m4} may be decreased. Visibility envelope module 314 may provide the adjusted visibility envelope information R_{m4}' and θ_{m4}' to intruder analysis module 308.

[0041] Intruder analysis module 308 receives visibility envelope information from visibility envelope module 314, and intruder analysis module 308 receives a user preference file from preference data 310. Additionally, intruder analysis module 308 receives sensor information, which is provided by the sensor (e.g. sensor 200) through input 320. Intruder analysis module 308 scans the input for viewers, and classifies them as either intruders or safe viewers. Intruder analysis module 308 may classify an object as a viewer using any number of detection algorithms. For example, intruder analysis module 308 may apply motion detection algorithms on the sensor information, and may classify any moving object as a viewer. As another example, intruder analysis module 308 may apply facial recognition algorithms on the sensor information, and may classify any detected faces as viewers.

[0042] Intruder analysis module 308 analyzes any detected viewers to determine each viewer's range and location information. A viewer's range and location information may be determined by any number of range-finding and location-finding algorithms. The systems and methods of the present disclosure are not limited based on the type of range-finding and location-finding algorithms. Intruder analysis module 308 may compare a viewer's range and location to the bounds of the visibility envelope. For example, if a viewer's range is greater than the visibility envelope's range, intruder analysis module 308 may not classify the viewer as an intruder. As another example, if a viewer's location is such that the viewer has a viewing angle greater than the visibility envelope's maximum viewing angle, intruder analysis module 308 may not classify the viewer as an intruder. As another example, if a viewer is located 20 ft. from the display device, and the visibility envelope has a maximum range of 15 ft., the viewer would not be classified as an intruder. For viewers that are within the bounds of the visibility envelope, intruder analysis module 308 may perform additional analysis as discussed below.

[0043] Intruder analysis module 308 may use any number of algorithms to determine that the user is not an intruder. As a simple example, intruder analysis module 308 may classify the closest viewer as a safe user. As another example, intruder analysis module 308 may classify a partially obscured viewer as an intruder. As another example, intruder analysis module 308 may determine demographics of the viewer (e.g., age, sex, race) and compare these to those of safe user demographics as specified by a user preferences file to classify the viewer as either a safe user or as an intruder; for instance all children within

the visibility envelope may be classified as intruders. As another example, intruder analysis module 308 may apply additional facial recognition algorithms on any detected viewers. Intruder analysis module 308 may compare a detected viewer's face to a set of safe user faces as specified by a user preferences file (e.g. preference data 310). Intruder analysis module 308 may then determine whether the detected viewer has a face that is within the set of safe user faces, if so, intruder analysis module 308 may not classify that viewer as an intruder. Intruder analysis module 308 may further use algorithms to detect the eye-state or red-eye response of a viewer. Intruder analysis module 308 may use the eye information to restrict classifying a viewer with closed eyes as an intruder. Intruder analysis module 308 may then provide the results of the analysis to edit generation module 316.

[0044] In one embodiment, intruder analysis module 308 may receive input via input 320 from a sensor that is a single camera. The input may be of image information, and may include the camera's focal length for the particular image. Intruder analysis module 308 may also receive information from configuration data 312 of the camera's specifications. Intruder analysis module 308 may detect viewers as discussed above, and then determine a viewer's range based on the angular size of the intruder (or portions thereof). For example, the size of some portions of the human body (e.g., facial width, or eye-to-eye separation) are relatively constant for most people. Accordingly, a priori knowledge of this physical size, combined with the angular size as measured by a camera, allows intruder analysis module 308 to infer a range estimate. Intruder analysis module 308 may detect viewers as discussed above, and then determine a viewer's range based on focusing algorithms. For example, intruder analysis module 308 may use the focal length necessary for focus in conjunction with the camera's specifications to calculate a distance. As another example, intruder analysis module may use contrast detection and phase detection algorithms to focus the image. Intruder analysis module 308 may use the calculated distance and the image information to determine a viewing angle of a viewer. Intruder analysis module 308 may then use the calculated distance and viewing angle in analyzing the viewer as discussed above. As another example, intruder analysis module 308 may use the ability of the camera to resolve features of the viewer in order to infer the ability of the viewer to resolve visual contents displayed on the screen, i.e., if the camera cannot clearly resolve the viewer, the intruder analysis module 308 may assume the

converse, and not classify him as an intruder. This analysis may involve a priori knowledge of typical human visual acuity (which may be dependent upon the ambient lighting conditions) as well as the imaging resolution capabilities of the camera and the quality of the image it obtains of the viewer.

5 [0045] In one embodiment, intruder analysis module 308 receives input via input 320 from a sensor that contains two cameras. The input may be of image or video information. Intruder analysis module 308 may also receive camera specification information from configuration data 312. Using the two camera input, intruder analysis module 308 may use stereoscopic algorithms to calculate the range of a viewer. Intruder analysis module
10 308 may use the calculated range and the image or video information to determine a viewing angle of a viewer. Intruder analysis module 308 may use the calculated range and viewing angle in analyzing the viewer as discussed above.

[0046] In one embodiment, intruder analysis module 308 may receive input via input 320 from a sensor that contains a cameras and distance measuring device (e.g., a sonic or
15 ultrasonic device, a microphone, an infrared device, a micropower impulse radar device, a light detection and ranging device etc.) The input may be of image or video information and distance information. Intruder analysis module 308 may also receive camera specification information from configuration data 312. Intruder analysis module 308 may use the distance information to determine a range of a viewer. Intruder analysis module
20 308 may then use the range and the image or video information to determine a viewing angle of a viewer. Intruder analysis module 308 may use the range and viewing angle in analyzing the viewer as discussed above.

[0047] In one embodiment, intruder analysis module 308 may receive content information, in addition to input from a sensor. The content information may be of a
25 content type that is being primarily displayed. For example, a content type may be of “text” or “video.” Intruder analysis module may use the content type information in addition to analyzing the viewer as discussed above. For example, if the content being displayed on an electronic media display is text of a small font, the range in which a viewer is considered an intruder may be decreased due to the difficulty of reading small
30 text at a distance. As another example, if the content being displayed is an image, the

range in which a viewer is considered an intruder may be increased due to the ease of viewing an image.

[0048] Edit generation module 316 is configured to receive data from intruder analysis module 308. Edit generation module 316 is further configured to provide communication capabilities with an electronic media display via input 320 and output 322. The data may include results from any analysis performed by intruder analysis module 308. Edit generation module 316 may determine whether to perform edits to content on an electronic media display (e.g., electronic media display 400). For example, the data may indicate the presence of intruders, and edit generation module 316 may then determine that content must be edited. Edit generation module 316 may accept information corresponding to the contents displayed on an electronic media display. Edit generation module may then provide the commands for editing the content and transmit the commands via output 322.

[0049] As an example, edit generation module 316 may provide commands to degrade the visibility of the electronic media display content (e.g. blurring the content of the electronic media display, dimming the brightness of the content of the electronic media display, reducing the font size of the content of the electronic media display, switching the content of the electronic media display to a new content, stopping (or refusing to start) the display of the content of the electronic media display device, etc.) As another example, edit generation module 316 may provide commands necessary for warning the user with an alert message, by playing an alert sound, or by muting the sound. As another example, the alert may involve haptic feedback (e.g., a vibration), or visual alert indication (e.g., flashes, color changes). As another example, the data from intruder analysis module 308 may indicate the lack of any intruders, and edit generation module 316 may then determine that the content should be displayed unedited and may not send any commands to edit content, or may send commands to cease any editing that is occurring.

[0050] In one embodiment, edit generation module 316 may generate commands to switch content displayed on an electronic media display (e.g., electronic media display 400) to new content in real time. For example, electronic media display 400 may be the display of a cellular phone, and a user may be watching a film that is not appropriate for children on the cellular phone. A child may walk up behind the display, and edit generation module 316 may send commands to switch the film to a blank stream of white

frames with no audio. In another example edit generation module 316 may send commands to pause the film and blur the display. In another example edit generation module 316 may send commands to pause the film and dim the brightness of the display.

[0051] In one embodiment, edit generation module 316 may generate commands to mute the audio of an electronic media display device (e.g., electronic media display device 402 of FIG. 4). For example, electronic media display device 402 may be a camera equipped cellular phone, and a user may be making a video call with speakerphone enabled. An intruder may walk up behind the device, and edit generation module 316 may produce commands to mute the audio output of the cellular phone. In this fashion, the audio of the video call would be muted before the intruder can actively hear the discussion.

[0052] In an alternative embodiment, edit generation module 316 may generate commands to freeze the current content displayed on an electronic media display (e.g., electronic media display 400). This may be useful as part of a parental control system. For example, electronic media display 400 may be the display of a laptop computer, and a parent may set the user preferences to freeze the screen if an intruder is detected. The parent may have not added his or her face to a list of safe users. The parent may walk up behind the display when the display is being used by a child, and edit generation module 316 may send commands to freeze the contents of the display. In this fashion, the parent may see what the child was viewing before the child can actively change the content.

[0053] Preference data 310 may be stored in a database local to or remotely from processing circuit 300, or may be received via a preference file transmitted to processing circuit 300 via input 320. Preference data 310 relates to user preferences for the visibility envelope module 314, intruder analysis module 308, and edit generation module 316. Using a preference file stored in preference data 310, the constraints of a visibility envelope may be customized for a user. Additionally, a safe user may be specified for use in determining an intruder. A user's preferred content editing methods (e.g. blurring the screen, etc.) may also be specified and stored in the preference file. For example, if a user is in a particularly sensitive environment, the user may increase the range in which a viewer is considered an intruder.

[0054] Processing circuit 300 further includes an input 320 and an output 322. Input 320 may be configured to receive image information, video information, content information,

preference file information, and other information relating to the determination of a visibility envelope, performing intruder analysis, and editing content as described above. Output 322 may be configured to provide an output to a client, electronic display, or other electronic device as described above. Outputs may include commands, data including image sequences, preference file information, and other information related to editing content as described above. Outputs may involve recording the time and/or location of an intrusion event, an image of the intruder, the position of the intruder relative to the device, the determination of the viewer as either a safe viewer or as an intruder, the editing action taken, or other information related to the event.

10 **[0055]** Referring generally to FIGS. 4-13, various schematic diagrams and processes are shown and described that may be implemented using the systems and methods described herein. The schematic diagrams and processes may be implemented using the system 100 of FIG. 2 and processing circuit 300 of FIG. 3.

15 **[0056]** Referring to FIG. 4, a schematic diagram of an electronic media display device, a sensor, and a processing circuit is shown according to one embodiment. Electronic media display device 402 is shown as camera-equipped cellular phone. Sensor 404 is shown as a camera that is coupled to electronic media display device 402. Processing circuit 300 is shown as internal processing components. Processing circuit 300 contains modules and components as describe above. While FIG. 4 only shows one camera as a sensor, it should be understood that sensor 402 may be any of the sensors discussed above. Coupling sensor 402 and processing circuit to electronic media display device 402 allows for portability of the system.

25 **[0057]** As an exemplary embodiment, electronic media display device 402 may be a tablet computing device. Sensor 404 may be an onboard camera that is coupled to the tablet computer. Processing circuit 300 may be the processing components of the tablet computer that are configured to implement the systems and methods described herein.

30 **[0058]** Referring to FIG. 5, a schematic diagram of a sensor 502 and corresponding visibility envelope 500 is shown. Analysis performed by intruder analysis module 308 of processing circuit 300 is depicted as angle 504 and distance 506. An intruder 508, maximum viewing angle 510, and maximum viewing range 512 are also depicted. According to an exemplary embodiment, angle 510 and range 512 may correspond to the

specifications of an electronic media display device. For example, a particular mobile LCD display may have a maximum viewing angle of 160° and a maximum resolvable viewing distance of 15 ft. According to an alternative embodiment, angle 510 and range 512 may be offset with values as specified by a user preferences file. According to an exemplary embodiment, angle 504 is be calculated as the angle between a center axis and the position of a viewer 508. The center axis may be positioned midway within the maximum viewing angle.

[0059] Referring to FIG. 6, a schematic diagram of a sensor 602 and corresponding visibility envelope 600 is shown. Analysis performed by intruder analysis module 308 of processing circuit 300 is depicted as angles 606, 608, and 610, and distances 614, 616, and 618. User 620, viewers 622, 624 and 626, maximum viewing angle 604, and maximum viewing range 612 are also depicted. According to an exemplary embodiment, angle 604 and range 612 correspond to the specifications of an electronic media display device. According to an alternative embodiment, angle 604 and range 612 may be offset with values as specified by a user preferences file. As shown in FIG. 6, viewer 626 is shown as having a range 616 that is greater than the maximum resolvable viewing range 612. For example, viewer 626 may be positioned 25 ft. from sensor 602, which is coupled to an electronic media display that has a maximum viewing range of 15 ft. In this example, viewer 626 would not be considered an intruder. Similarly, viewer 624 may be positioned at an angle that is greater than half of the display's maximum viewing angle. Viewer 624 would not be considered an intruder. However, viewer 622 is a positioned at a range that is less than maximum viewing range 612, and at an angle that is less than half of the maximum viewing angle 612. Viewer 622 would be considered an intruder.

[0060] Referring to FIG. 7, a schematic diagram of a sensor 702 and corresponding visibility envelope 700 is shown. Analysis performed by intruder analysis module 308 of processing circuit 300 (as is shown in FIG. 3) is depicted as angles 706, and 710, and distances 708 and 712. Additionally, analysis related to eye detection is also depicted at 718. Viewers 716 and 720, maximum viewing angle 704 and maximum viewing range 714 are also depicted. According to an exemplary embodiment, angle 704 and range 714 correspond to the specifications of an electronic media display device. Both viewers 716 and 720 are shown as within viewing envelope 700. However, viewer 720 has his or her eyes 722 closed, or may be turned around looking the other way. For example, a viewer

may be sleeping. Viewer 716 has his or her eyes 718 open. In an alternative embodiment, an intruder analysis module such as intruder analysis module 308 may use this information in determining if a viewer is an intruder. For example, if a red eye response cannot be determined for a viewer, that viewer may not be classified as an intruder. As shown in
5 FIG. 7, viewer 716 would be classified as an intruder, but viewer 720 would not. As an example, algorithms that may be used to detect open eyes include red-eye response algorithms, and other facial recognition algorithms.

[0061] Referring to FIG. 8, a schematic diagram of shows electronic media display device 802, sensor 806, processing circuit 300 (as is shown in FIG. 3), and visibility
10 envelope 800. According to an exemplary embodiment, the electronic media display device is part of an ATM machine. Sensor 806 may be a camera that is coupled to the ATM machine, and processing circuit 300 may be the processing components of the ATM machine. User 810 is shown as operating the ATM machine, and viewer 812 is shown as being within visibility envelope 800. Contents of electronic media display device 802 are
15 shown as blurred 814. By automatically blurring the contents of the display, sensitive content can be protected from being viewed by unauthorized viewers. Similar embodiments are also useful in situations where sensitive content is displayed. For example, a medical display device that displays or gathers information about a user's medical history.

[0062] Referring to FIG. 9, a flow diagram of a process 900 for detecting an intruding
20 viewer of a camera-equipped electronic media display device and editing content is shown, according to an exemplary embodiment. Process 900 includes capturing an image of the electronic media display device's surroundings using a camera (step 902), determining a visibility envelope (step 904), and analyzing the captured image and
25 visibility envelope information to determine if an intruder is present (step 906). If a viewer is present (step 908), and the viewer is within the visibility envelope (step 910), and the content on the screen is not already edited (step 912), the content on the electronic media display device is edited or changed (step 914). However, if the viewer is not determined to be an intruder, and the content is already edited (step 918), it is safe to reset
30 any previous edits and display unedited content again (step 916). If an intruder is detected and the content is already edited, no further action needs to be taken (step 912).

[0063] Referring to FIG. 10, a flow diagram of a process 1000 for detecting an intruding viewer of camera-equipped electronic media display device and editing content according to a user preference file is shown, according to an exemplary embodiment. Process 1000 includes receiving a user preference data file (step 1002), capturing an image of the electronic media display device's surrounding using the camera (step 1004), determining a visibility envelope (step 1006), and analyzing the captured image and visibility envelope information to determine if an intruder is present (step 1008). If a viewer is present (step 1010), and the viewer is within the visibility envelope (step 1012), and the content on the screen is not already edited (step 1014), content on the electronic media display device is edited or changed (step 1016). However, if the viewer is not determined to be an intruder, and the content is already edited (step 1020), it is safe to reset any previous edits and display unedited content again (step 1018). If an intruder is detected and the content is already edited, no further action needs to be taken (step 1014).

[0064] Referring to FIG. 11, a flow diagram of a general process 1100 for detecting and reacting to an intruding viewer of an electronic media display device is shown according to an exemplary embodiment. Process 1100 includes obtaining information from a sensor (step 1102), determining a visibility envelope based on the sensor and input information (step 1104), performing analysis to determine a presence of an intruder within the visibility envelope, and editing or changing content on a display device if an intruder is detected (step 1108).

[0065] Referring to FIG. 12, a flow diagram of a process 1200 for performing intruder analysis is shown, according to an exemplary embodiment. Process 1200 includes detecting all viewers of a display device (step 1202) and performing the following steps for each detected viewer: determining the viewers range from the display device (step 1204), determining the viewer's angle with respect to the display device (step 1206), performing additional analysis (step 1208), and comparing the analyzed information to a visibility envelope to determine if the viewer is an intruder and is a threat to the display device's content (step 1210). Step 1208 may include performing additional operations in addition to those performed in steps 1204 and 1206. For example, a system may be configured to perform red eye analysis to determine if a viewer can see the display. As another example, a system may be configured to adjust a visibility envelope according to user preferences. As another example, a system may be configured to take the display's

brightness or content type into consideration. As another example, a system may be configured to take the display's size and the average quality of human eyesight into consideration.

[0066] The present disclosure contemplates methods, systems and program products on any machine-readable media for accomplishing various operations. The embodiments of the present disclosure may be implemented using existing computer processors, or by a special purpose computer processor for an appropriate system, incorporated for this or another purpose, or by a hardwired system. Embodiments within the scope of the present disclosure include program products comprising machine-readable media for carrying or having machine-executable instructions or data structures stored thereon. Such machine-readable media can be any available media that can be accessed by a general purpose or special purpose computer or other machine with a processor. By way of example, such machine-readable media can comprise RAM, ROM, EPROM, EEPROM, CD-ROM or other optical disk storage, magnetic disk storage or other magnetic storage devices, or any other medium which can be used to carry or store desired program code in the form of machine-executable instructions or data structures and which can be accessed by a general purpose or special purpose computer or other machine with a processor. When information is transferred or provided over a network or another communications connection (either hardwired, wireless, or a combination of hardwired or wireless) to a machine, the machine properly views the connection as a machine-readable medium. Thus, any such connection is properly termed a machine-readable medium. Combinations of the above are also included within the scope of machine-readable media. Machine-executable instructions include, for example, instructions and data which cause a general purpose computer, special purpose computer, or special purpose processing machines to perform a certain function or group of functions.

[0067] Although the figures may show a specific order of method steps, the order of the steps may differ from what is depicted. Also two or more steps may be performed concurrently or with partial concurrence. Such variation will depend on the software and hardware systems chosen and on designer choice. All such variations are within the scope of the disclosure. Likewise, software implementations could be accomplished with standard programming techniques with rule based logic and other logic to accomplish the various connection steps, processing steps, comparison steps and decision steps.

WHAT IS CLAIMED IS:

1. A system for detecting viewers of a display and responding to an intrusion, comprising:
 - an electronic media display device having a screen configured to display content;
 - a sensor; and
 - a processing circuit configured to:
 - obtain information from the sensor;
 - determine a visibility envelope of the electronic media display device;
 - analyze the information to determine a presence of an intruder within the visibility envelope;
 - distinguish the intruder from an authorized user; and
 - edit any displayed content.
2. The system of claim 1, wherein the sensor is coupled to the electronic media display device.
3. The system of claim 1, wherein the processing circuit is further configured to determine a distance of the intruder from the screen based on the information
4. The system of claim 3, wherein the distance determination is based upon an angular size of at least a portion of the intruder.
5. The system of claim 3, wherein the presence of an intruder is determined using the distance.
6. The system of claim 1, wherein the processing circuit is further configured to determine an angle of the intruder relative to an axis orthogonal to the screen based on the information.
7. The system of claim 6, wherein the presence of an intruder is determined using the angle.

8. The system of claim 1, wherein the visibility envelope is determined using a brightness of the screen.
9. The system of claim 1, wherein the visibility envelope is determined using externally provided information characterizing the visual performance of the screen.
10. The system of claim 1, wherein the visibility envelope is determined using information concerning the displayed content.
11. The system of claim 1, wherein the visibility envelope is based upon an ability to resolve displayed content.
12. The system of claim 11, wherein the presence of an intruder is determined using the ability to resolve displayed content.
13. The system of claim 1, wherein the sensor is further configured to sense the intruder according to characteristics of human vision.
14. The system of claim 13, wherein the presence of an intruder is determined according to characteristics of human vision.
15. The system of claim 1, wherein the sensor includes a passive imager.
16. The system of claim 15, wherein the passive imager includes a range-sensitive camera.
17. The system of claim 16, wherein the processing circuit is further configured to perform calculations using a focal length.
18. The system of claim 1, wherein the sensor includes a set of two cameras.
19. The system of claim 18, wherein the processing circuit is further configured to perform calculations based on stereoscopic information.
20. The system of claim 1, wherein the sensor includes an active imager.
21. The system of claim 1, wherein the sensor uses a radar.

22. The system of claim 21, wherein the radar includes a micropower impulse radar (MIR).

23. The system of claim 1, wherein the sensor includes light detection and ranging technology (LIDAR).

24. The system of claim 1, wherein the sensor includes a microphone.

25. The system of claim 1, wherein the sensor includes an ultrasonic sensor.

26. The system of claim 1, wherein the sensor includes an infrared sensor.

27. The system of claim 26, wherein the infrared sensor includes a near-infrared (NIR) sensor.

28. The system of claim 26, wherein the processing circuit is further configured to determine a red-eye response.

29. The system of claim 28, wherein the processing circuit is further configured to determine whether the intruder is looking at the screen using the red-eye response.

30. The system of claim 29, wherein the processing circuit is further configured to edit the displayed content only when the intruder is determined to be looking at the screen.

31. The system of claim 1, wherein the processing circuit is further configured to determine the location of the intruder's eyes.

32. The system of claim 31, wherein the processing circuit is further configured to determine whether the intruder is looking at the screen.

33. The system of claim 32, wherein the processing circuit is further configured to respond to the presence of the intruder only when the intruder is looking at the screen.

34. The system of claim 1, wherein the processing circuit is further configured to alert a user if the presence of an intruder is determined.

35. The system of claim 34, wherein the alert includes playing a sound.

36. The system of claim 34, wherein the alert includes displaying a flashing content on a portion of the screen.
37. The system of claim 34, wherein the alert includes a vibration.
38. The system of claim 34, wherein the alert includes a change to a color of a portion of content displayed on the screen.
39. The system of claim 34, wherein the alert includes displaying a message on the screen.
40. The system of claim 34, wherein the alert is defined by a user's settings.
41. The system of claim 1, wherein the editing comprises turning off the screen.
42. The system of claim 1, wherein the editing comprises replacing the displayed content with a different content.
43. The system of claim 1, wherein the editing comprises freezing the displayed content.
44. The system of claim 1, wherein the editing comprises adjusting a brightness of the screen.
45. The system of claim 1, wherein editing comprises disabling a displaying of new content.
46. The system of claim 1, wherein the editing comprises muting any audio.
47. The system of claim 1, wherein the editing comprises temporarily disabling any input.
48. The system of claim 1, wherein the editing comprises degrading the displayed content.
49. The system of claim 48, wherein the degrading comprises blurring.
50. The system of claim 48, wherein the degrading comprises dimming.

51. The system of claim 48, wherein the degrading comprises reducing the size of displayed content.

52. The system of claim 1, wherein editing comprises edits as specified by a user's settings.

53. The system of claim 1, wherein the electronic media display device includes a television.

54. The system of claim 1, wherein the electronic media display device includes a computer terminal.

55. The system of claim 1, wherein the electronic media display device includes a medical device.

56. The system of claim 1, wherein the electronic media display device includes an automated teller machine.

57. The system of claim 1, wherein the electronic media display device includes a video-conferencing device.

58. The system of claim 1, wherein the electronic media display device includes a mobile device.

59. The system of claim 58, wherein the mobile device includes a cellular phone.

60. The system of claim 58, wherein the mobile device includes a tablet computer.

61. The system of claim 58, wherein the mobile device includes a laptop computer.

62. The system of claim 58, wherein the mobile device includes an eBook reading device.

63. The system of claim 58, wherein the mobile device includes a music player.

64. The system of claim 58, wherein the mobile device includes a video player.

65. A method for detecting viewers of a display and responding to an intrusion, comprising:

displaying content on an electronic media display device having a screen;
obtaining information from a sensor;
determining a visibility envelope of the display device;
analyzing the information to determine a presence of an intruder within the visibility envelope;
distinguishing the intruder from an authorized user; and
editing the displayed content if the presence of an intruder is determined.

66. The method of claim 65, wherein the sensor is coupled to the electronic media display device.

67. The method of claim 65, further comprising determining an angle of the intruder relative to an axis orthogonal to the screen based on the information.

68. The method of claim 67, further comprising determining a distance of the intruder from the screen based on the information.

69. The method of claim 68, wherein the distance determination is based upon an angular size of at least a portion of the intruder.

70. The method of claim 68, wherein the presence of an intruder is determined using the distance and angle.

71. The method of claim 65, wherein the visibility envelope is determined using a brightness of the screen.

72. The method of claim 65, wherein the visibility envelope is determined using externally provided information characterizing the visual performance of the screen.

73. The method of claim 65, wherein the visibility envelope is determined using information concerning the displayed content.

74. The method of claim 65, wherein the visibility envelope is determined based upon an ability to resolve displayed content.

75. The method of claim 74, wherein the presence of an intruder is determined using the ability to resolve displayed content.

76. The method of claim 65, further comprising determining an ability to image the intruder according to characteristics of human vision.

77. The method of claim 76, wherein the presence of an intruder is determined according to characteristics of human vision.

78. The method of claim 65, wherein the sensor includes a passive imager.

79. The method of claim 78, wherein the passive imager includes a range-sensitive camera.

80. The method of claim 79, further comprising performing calculations using a focal length.

81. The method of claim 65, wherein the sensor includes a set of two cameras.

82. The method of claim 81, further comprising performing calculations based on stereoscopy.

83. The method of claim 65, wherein the sensor includes an active imager.

84. The method of claim 65, wherein the sensor uses a radar.

85. The method of claim 84, wherein the radar includes a micropower impulse radar (MIR).

86. The method of claim 65, wherein the sensor includes light detection and ranging technology (LIDAR).

87. The method of claim 65, wherein the sensor includes a microphone.

88. The method of claim 65, wherein the sensor includes an ultrasonic sensor.

89. The method of claim 65, wherein the sensor includes an infrared sensor.

90. The method of claim 89, wherein the infrared sensor includes a near-infrared (NIR) sensor.

91. The method of claim 89, further comprising determining a red-eye response.

92. The method of claim 91, further comprising determining whether the intruder is looking at the screen based on the red-eye response.

93. The method of claim 92, further comprising editing the displayed content only when the intruder is determined to be looking at the screen.

94. The method of claim 65, further comprising locating an intruder's eyes.

95. The method of claim 94, further comprising determining whether the intruder is looking at the screen.

96. The method of claim 95, further comprising editing the displayed content only when the intruder is looking at the screen.

97. The method of claim 65, further comprising notifying a user with an alert.

98. The method of claim 97, wherein the alert includes playing a sound.

99. The method of claim 97, wherein the alert includes displaying a flashing content on a portion of the screen.

100. The method of claim 97, wherein the alert includes a vibration.

101. The method of claim 97, wherein the alert includes a change to a color of a portion of content displayed on the screen.

102. The method of claim 97, wherein the alert includes displaying a message on the screen.

103. The method of claim 97, wherein the alert is defined by a user's settings.

104. The method of claim 65, wherein the editing comprises turning off the screen.

105. The method of claim 65, wherein the editing comprises replacing the displayed content with a different content.

106. The method of claim 65, wherein the editing comprises freezing the displayed content.

107. The method of claim 65, wherein the editing comprises adjusting a brightness of the screen.

108. The method of claim 65, wherein editing comprises disabling displaying new content.

109. The method of claim 65, wherein the editing comprises muting any audio.

110. The method of claim 65, wherein editing comprises temporarily disabling any input.

111. The method of claim 65, wherein the editing comprises degrading the displayed content.

112. The method of claim 111, wherein the degrading comprises blurring.

113. The method of claim 111, wherein the degrading comprises dimming.

114. The method of claim 111, wherein the degrading comprises reducing the size of displayed content.

115. The method of claim 65, wherein editing comprises edits as specified by a user's settings.

116. The method of claim 65, wherein the electronic media display device includes a television.

117. The method of claim 65, wherein the electronic media display device includes a computer terminal.

118. The method of claim 65, wherein the electronic media display device includes a medical display.

119. The method of claim 65, wherein the electronic media display device includes an automated teller machine.

120. The method of claim 65, wherein the electronic media display device includes a video-conferencing device.

121. The method of claim 65, wherein the electronic media display device includes a mobile device.

122. The method of claim 121, wherein the mobile device includes a cellular phone.

123. The method of claim 121, wherein the mobile device includes a tablet computer.

124. The method of claim 121, wherein the mobile device includes a laptop computer.

125. The method of claim 121, wherein the mobile device includes an eBook reading device.

126. The method of claim 121, wherein the mobile device includes a music player.

127. The method of claim 121, wherein the mobile device includes a video player.

128. A method for detecting viewers of a display of a camera-equipped mobile communication device and responding to an intrusion, comprising:

- obtaining input from a camera;
- determining an area within which a viewer can resolve any visual content;
- analyzing the input to determine a presence of an intruder within the area;
- distinguishing the intruder from an authorized user; and
- responding to the presence of the intruder by editing the visual content.

129. The method of claim 128, wherein the input includes an image.

130. The method of claim 128, wherein the input includes a set of images.

131. The method of claim 128, wherein the input includes a video clip.
132. The method of claim 128, wherein the input includes a live video stream.
133. The method of claim 128, where in the camera includes a front-facing camera.
134. The method of claim 128, wherein the mobile communication device includes a cellular phone.
135. The method of claim 128, wherein the mobile communication device includes a tablet computer.
136. The method of claim 128, wherein the mobile communication device includes a laptop computer.
137. The method of claim 128, wherein the mobile communication device includes an eBook reading device.
138. The method of claim 128, further comprising obtaining additional input from a second camera of the mobile communication device.
139. The method of claim 138, further comprising determining the presence of an intruder based on the input and the additional input.
140. A non-transitory computer-readable medium having instructions stored thereon for execution by a processing circuit, the instructions comprising:
- instructions for interfacing with an electronic media display device having a screen for visual content;
 - instructions for obtaining information from a sensor;
 - instructions for determining an area within which a viewer can resolve any visual content;
 - instructions for analyzing the information to determine a presence of an intruder within the area;
 - instructions for distinguishing the intruder from an authorized user; and
 - instructions for editing the visual content if the presence of an intruder is detected.

141. The non-transitory computer-readable medium of claim 140, wherein the instructions for analyzing the information further comprise instructions to calculate an angular size of at least a portion of the intruder.

142. The non-transitory computer-readable medium of claim 140, wherein the instructions for analyzing the information further comprise instructions to use externally provided information characterizing the visual performance of the screen.

143. The non-transitory computer-readable medium of claim 140, wherein the instructions for analyzing the information further comprise instructions to use information concerning the visual content.

144. The non-transitory computer-readable medium of claim 140, wherein the instructions for editing the visual content comprise instructions for turning off the screen.

145. The non-transitory computer-readable medium of claim 140, wherein the instructions for editing the visual content comprise instructions for replacing the visual content with a different visual content.

146. The non-transitory computer-readable medium of claim 140, wherein the instructions for editing the visual content comprise instructions for freezing the visual content.

147. The non-transitory computer-readable medium of claim 140, wherein the instructions for editing the visual content comprise instructions for adjusting a brightness of the screen.

148. The non-transitory computer-readable medium of claim 140, wherein the instructions for editing the visual content comprise instructions for disabling the display of any new visual content.

149. The non-transitory computer-readable medium of claim 140, wherein the instructions for editing the visual content comprise instructions for muting any audio.

150. The non-transitory computer-readable medium of claim 140, wherein the instructions for editing the visual content comprise instructions for muting any input.

151. The non-transitory computer-readable medium of claim 140, wherein the instructions for editing the visual content comprise instructions for degrading the visual content.

152. The non-transitory computer-readable medium of claim 140, wherein the instructions for editing the visual content comprise instructions for blurring the visual content.

153. The non-transitory computer-readable medium of claim 140, wherein the instructions for editing the visual content comprise instructions for changing a font size.

154. The non-transitory computer-readable medium of claim 140, wherein the instructions for editing the visual content comprise instructions for changing a size of the visual content.

155. The non-transitory computer-readable medium of claim 140, wherein the instructions for editing the visual content comprise instructions for performing edits as specified by a user's settings.

156. The non-transitory computer-readable medium of claim 140, wherein the instructions for editing the visual content comprise instructions for alerting a user.

157. The non-transitory computer-readable medium of claim 156, wherein the instructions for alerting a user comprise instructions for playing a sound.

158. The non-transitory computer-readable medium of claim 156, wherein the instructions for alerting a user comprise instructions for flashing content on a portion of the screen.

159. The non-transitory computer-readable medium of claim 156, wherein the instructions for alerting a user comprise instructions for initiating a vibration.

160. The non-transitory computer-readable medium of claim 156, wherein the instructions for alerting a user comprise instructions for changing a color on a portion of the screen.

161. The non-transitory computer-readable medium of claim 156, wherein the instructions for alerting a user comprise instructions for displaying a message.

162. The non-transitory computer-readable medium of claim 156, wherein the instructions for alerting a user comprise instructions for alerting as defined by a user's settings.

1/8

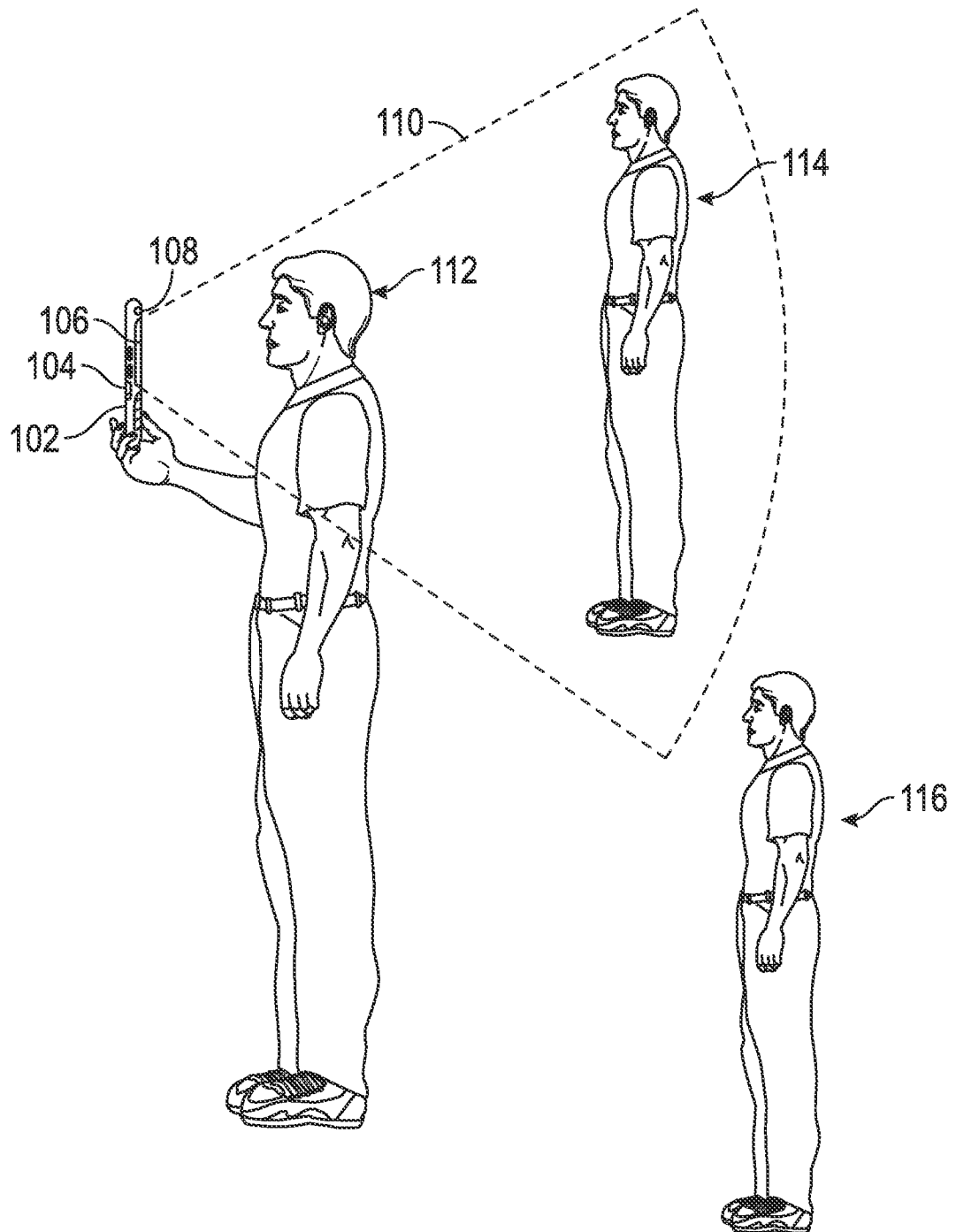


FIG. 1

2/8

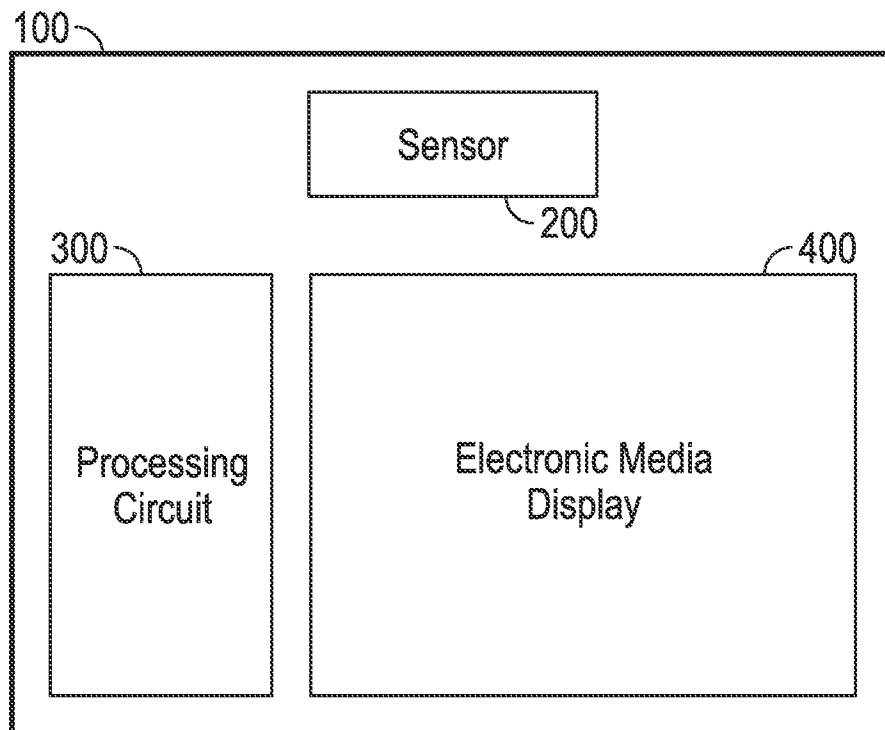


FIG. 2

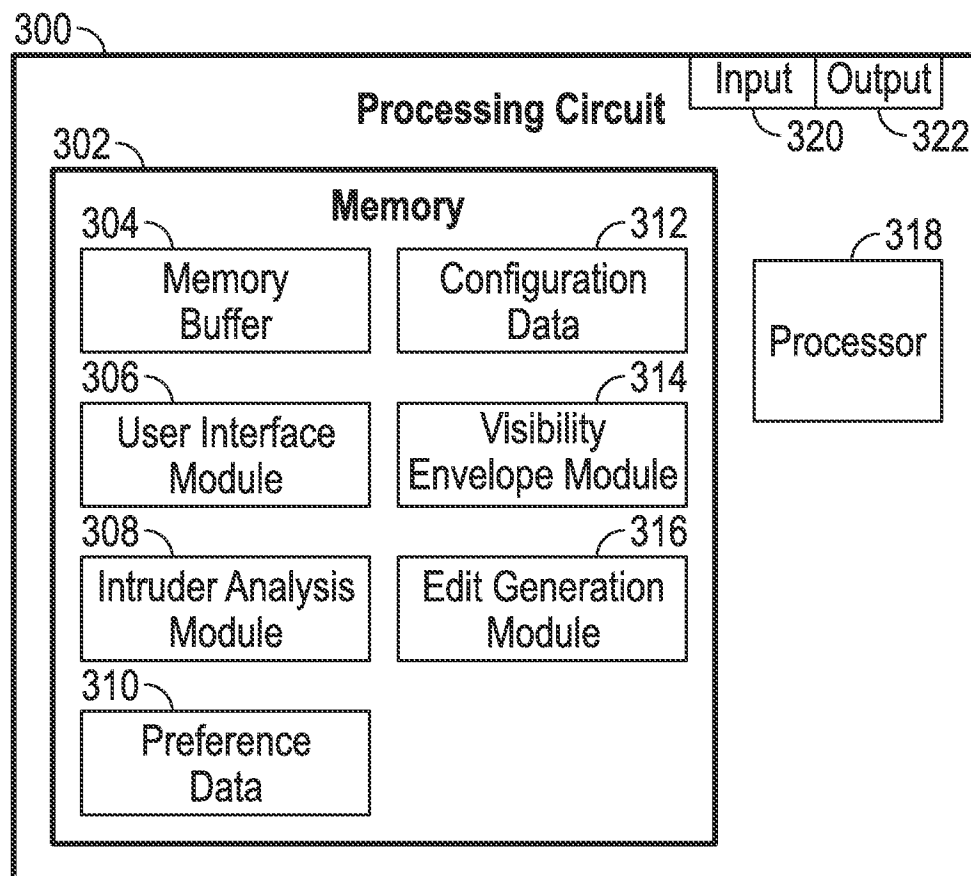


FIG. 3

3/8

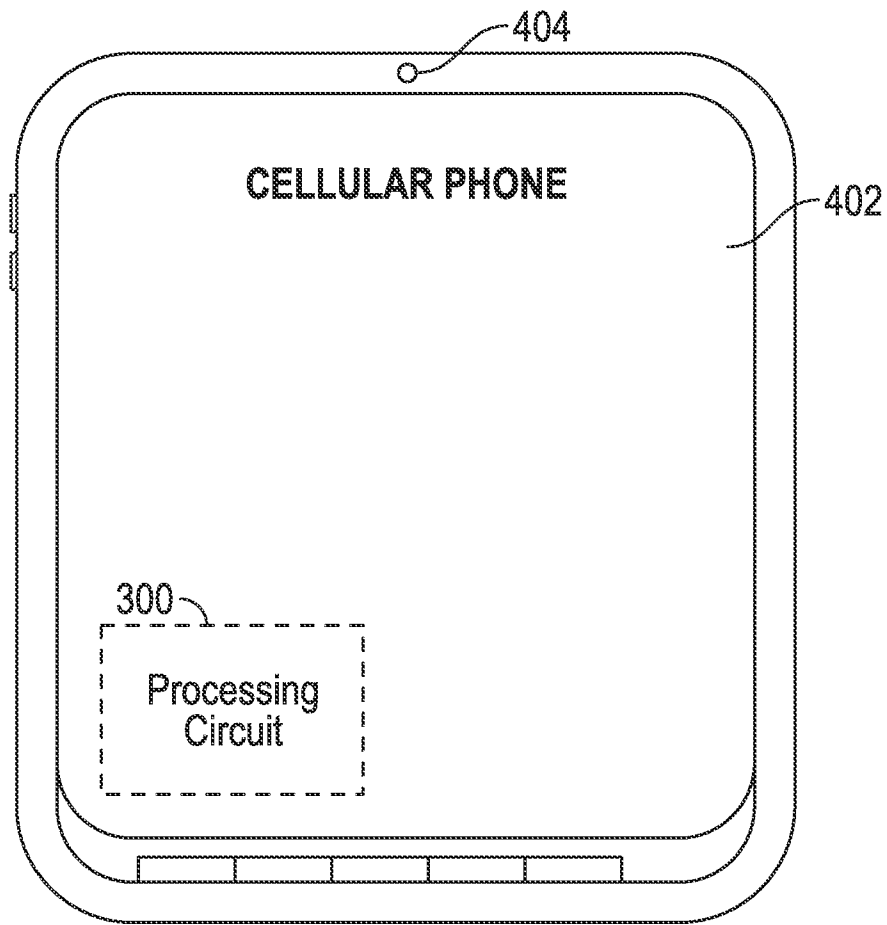


FIG. 4

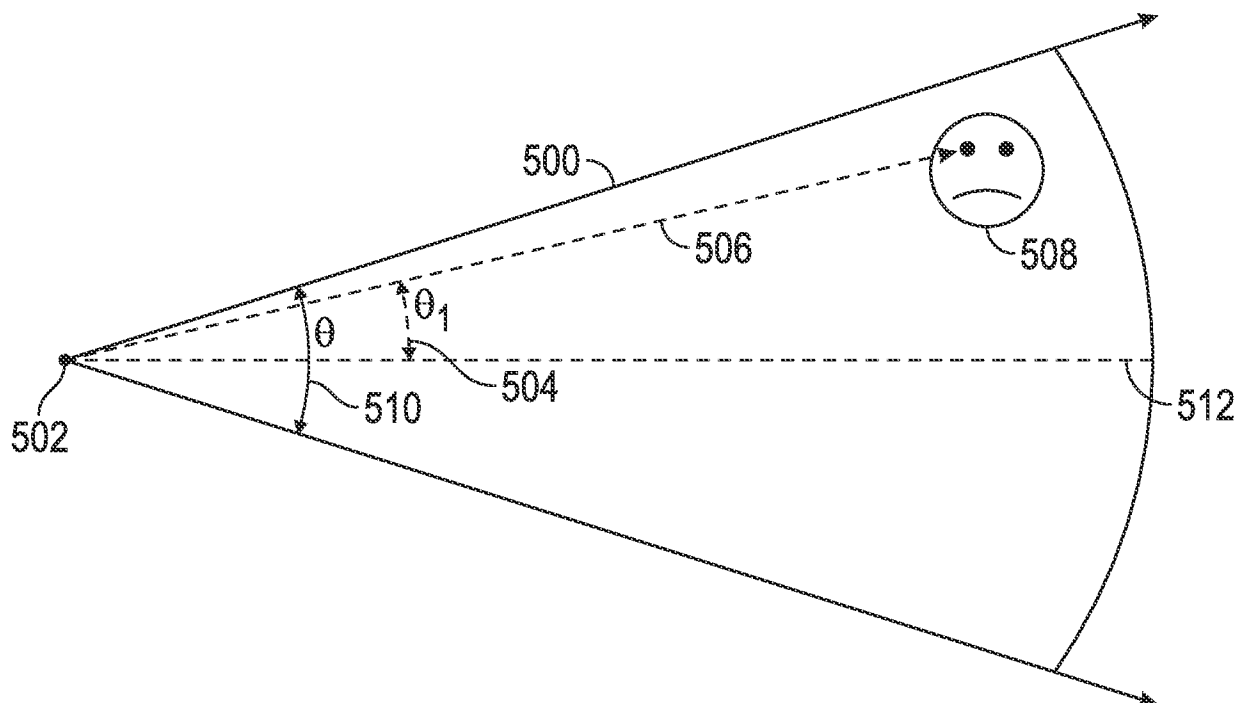


FIG. 5

4/8

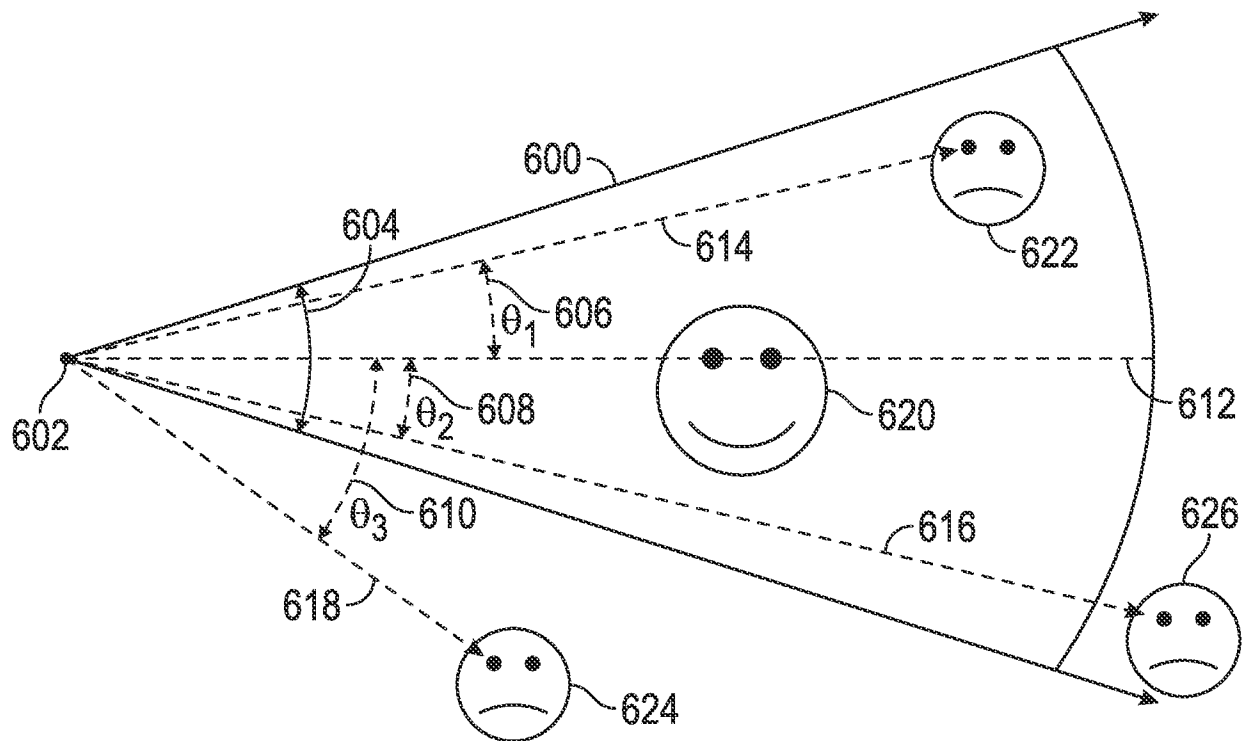


FIG. 6

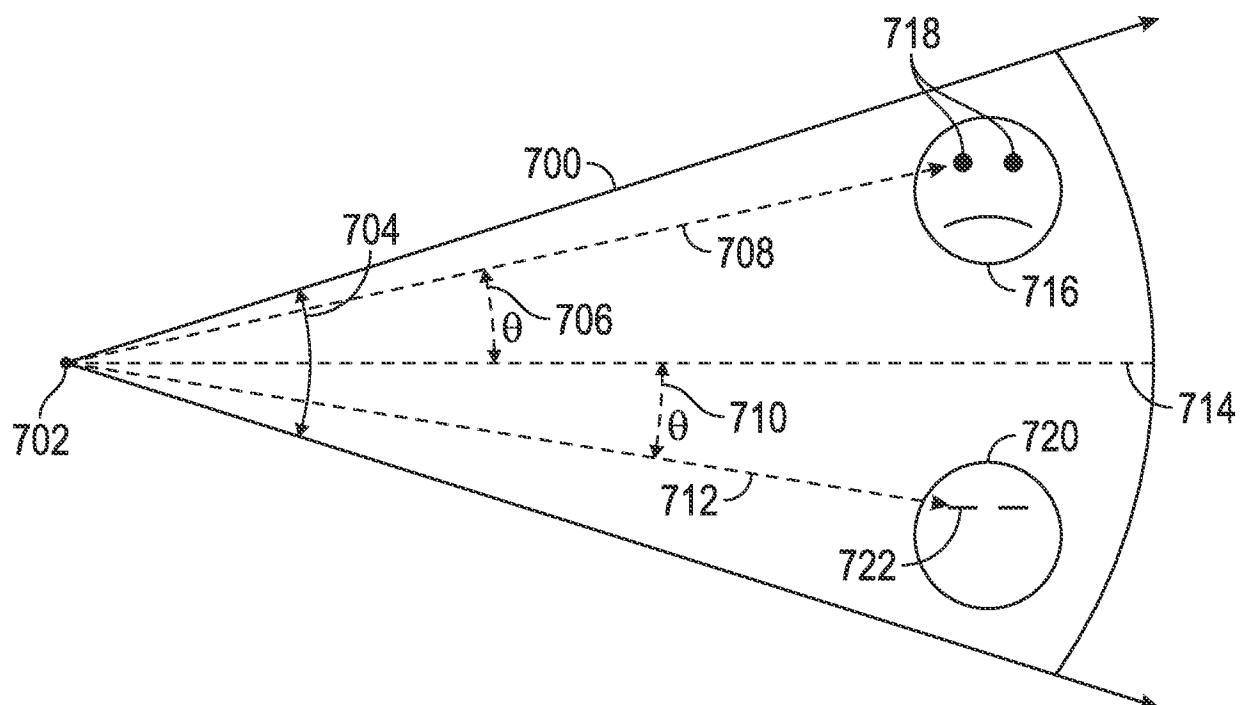


FIG. 7

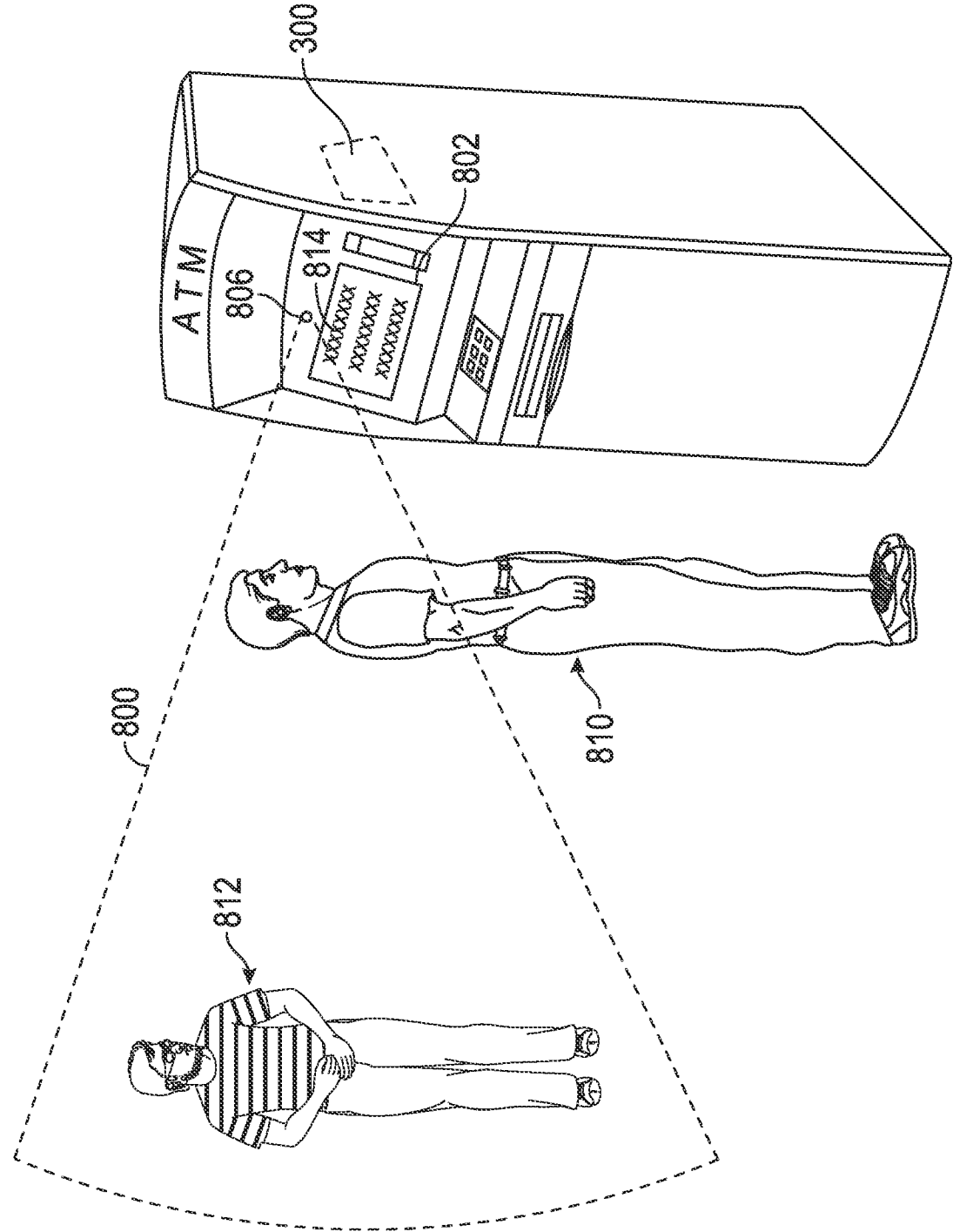


FIG. 8

6/8

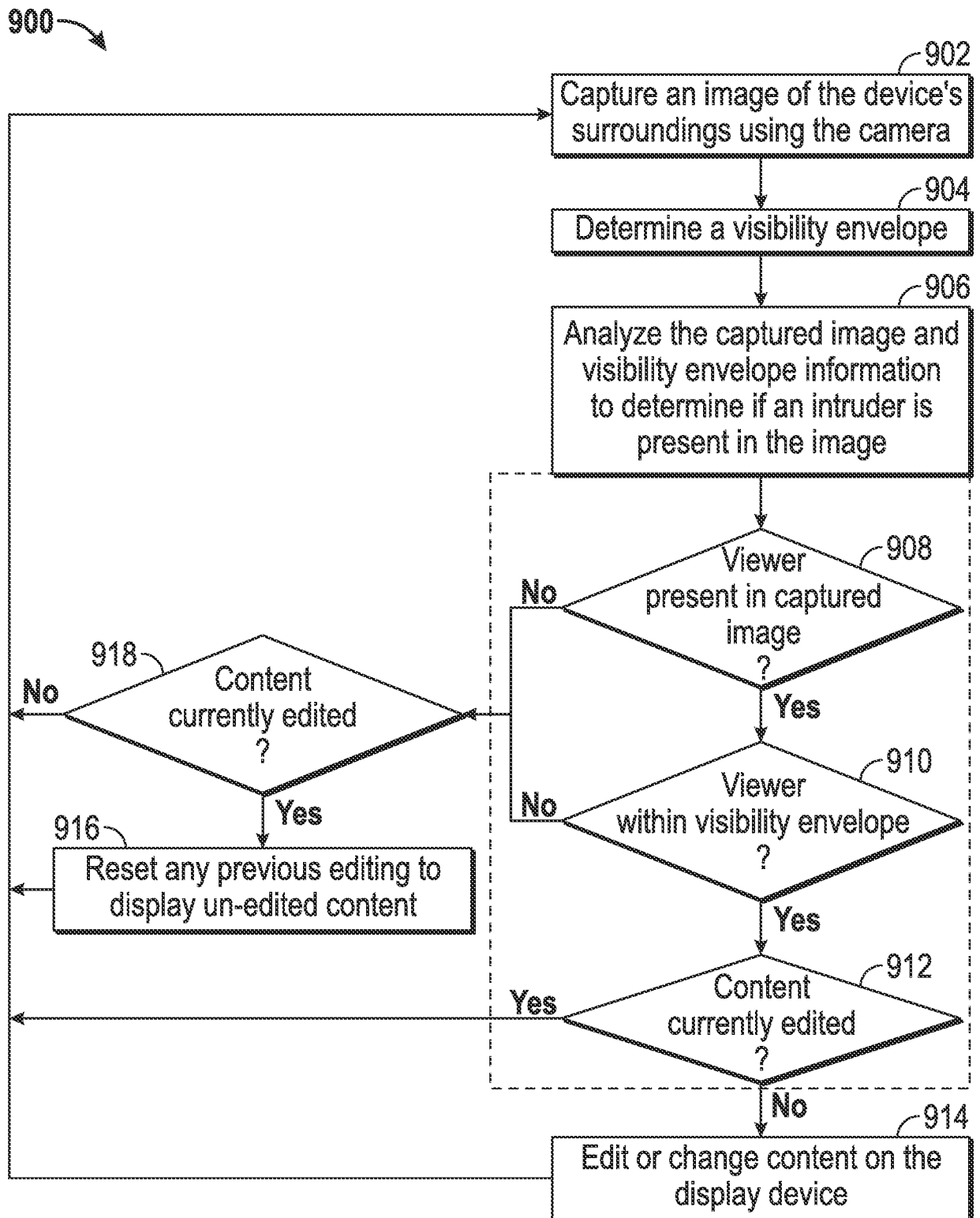


FIG. 9

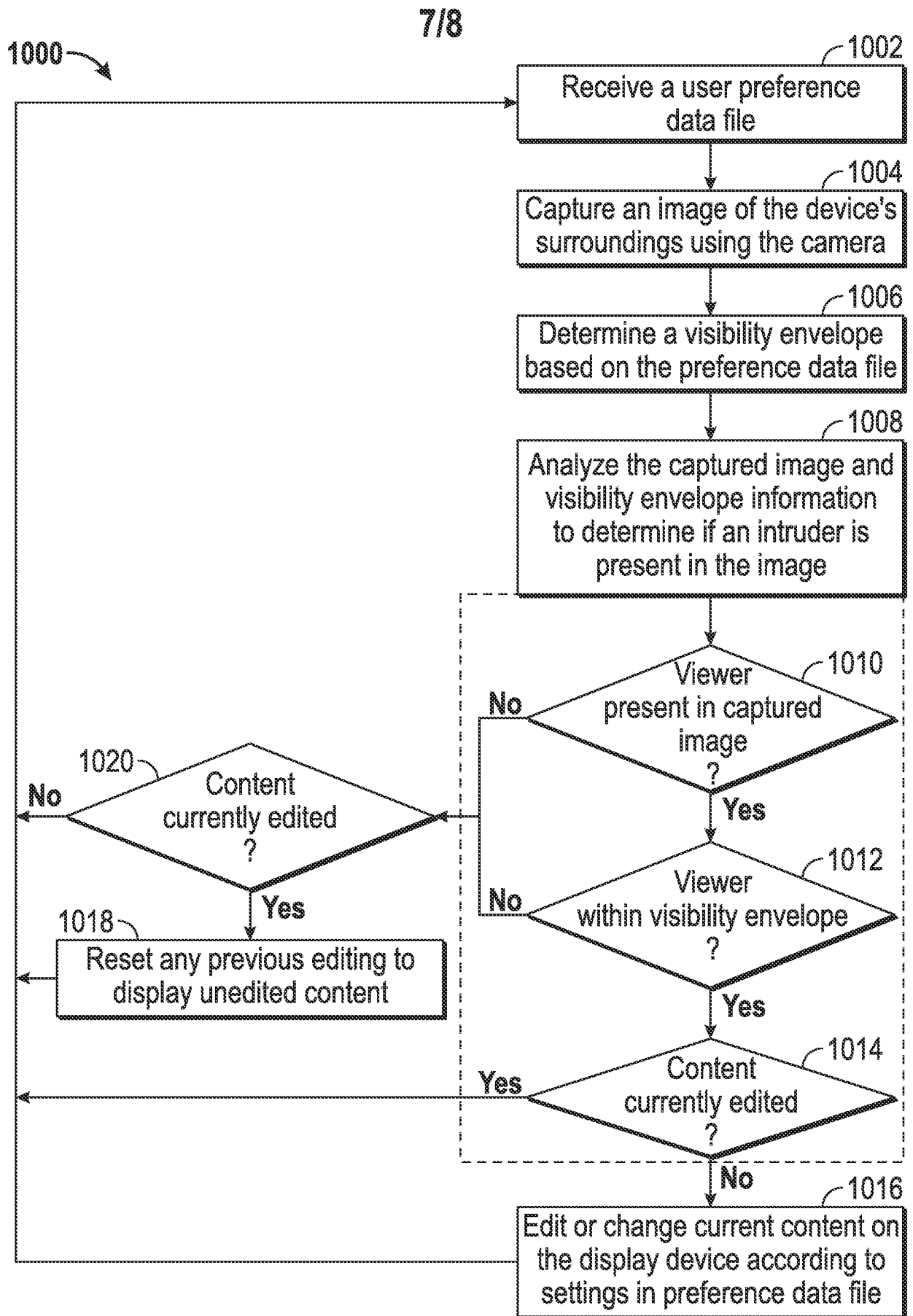


FIG. 10

8/8

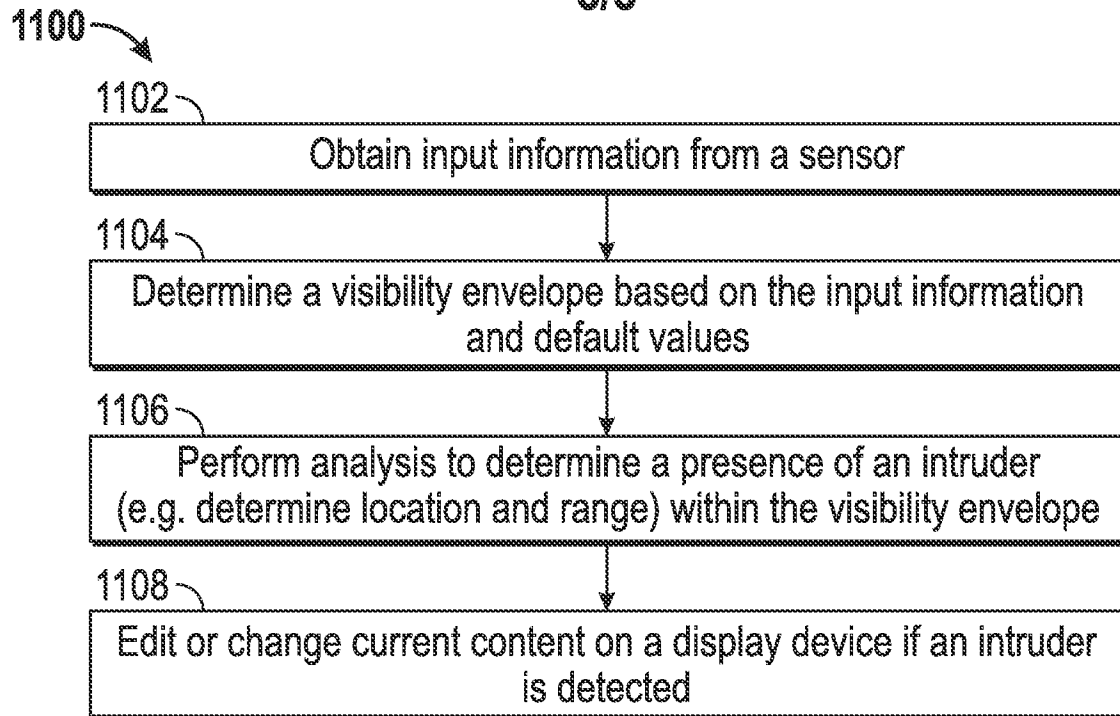


FIG. 11

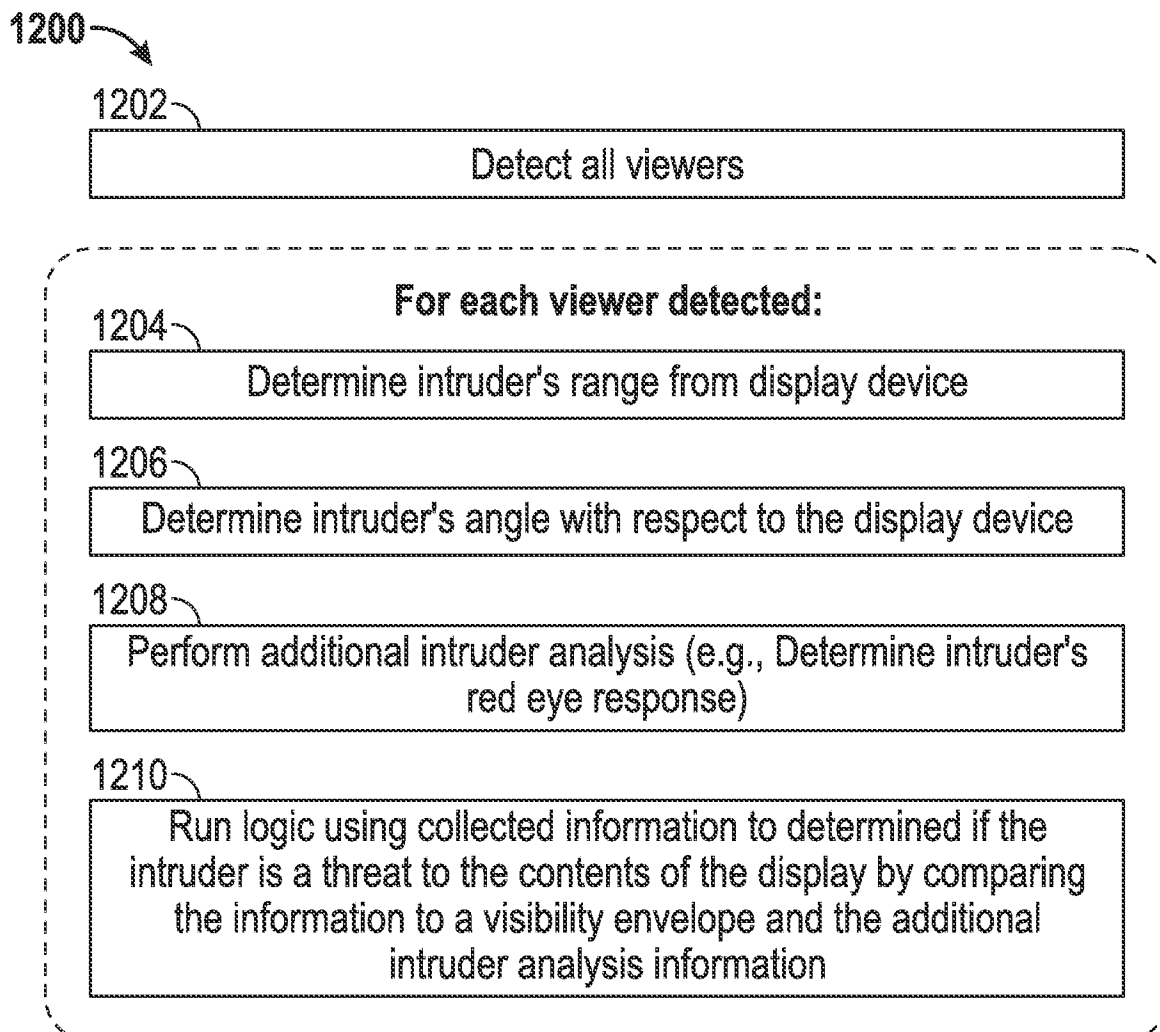


FIG. 12

INTERNATIONAL SEARCH REPORT

International application No.
PCT/US2013/059940**A. CLASSIFICATION OF SUBJECT MATTER****H04N 21/441(2011.01)i, H04N 21/41(2011.01)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)

H04N 21/441; G06F 3/14; G05B 19/00; G07D 9/00; G08B 21/00; G06K 9/00; G06Q 40/00; G06F 1/32; G06F 3/0489; G06F 3/041; H04N 21/41

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: viewer, detection, display, content, sensor, envelope, intruder, edit, and similar terms.

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	US 2011-0321143 A1 (SRIHARI V. ANGALURI et al.) 29 December 2011 See paragraphs 4, 14-15, 17, 20, 25-27, 30, 33-35; figures 1, 3; and claims 1-2, 16.	1, 3-33, 41-65, 67-96 , 104-128, 134-155
Y		2, 34-40, 66, 97-103 , 129-133, 156-162
Y	JP 2009-053884 A (NIPPON ATM CORP.) 12 March 2009 See paragraphs 27, 33-34, 37; figure 1; and claim 1.	2, 34-40, 66, 97-103 , 129-133, 156-162
A	US 2010-0309010 A1 (DE HUA DANG) 9 December 2010 See paragraphs 9-15; figures 1-2; and claims 1, 5-6.	1-162
A	KR 10-2010-0050823 (LG N-SYS INC.) 14 May 2010 See paragraphs 12-16; figure 1; and claim 1.	1-162
A	KR 10-2011-0118323 A (ATEC CO., LTD.) 31 October 2011 See paragraphs 95-106; figures 3a-3b; and claim 1.	1-162

☐ 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

"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

19 December 2013 (19.12.2013)

Date of mailing of the international search report

20 December 2013 (20.12.2013)

Name and mailing address of the ISA/KR


 Korean Intellectual Property Office
 189 Cheongsa-ro, Seo-gu, Daejeon Metropolitan City,
 302-701, Republic of Korea

Facsimile No. +82-42-472-7140

Authorized officer

KIM, Jin Ho

Telephone No. +82-42-481-8699



INTERNATIONAL SEARCH REPORT

Information on patent family members

International application No.

PCT/US2013/059940

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
US 2011-0321143 A1	29/12/2011	KR 10-2011-0140109 A US 8539560 B2	30/12/2011 17/09/2013
JP 2009-053884 A	12/03/2009	JP 5147333 B2	20/02/2013
US 2010-0309010 A1	09/12/2010	CN 101909174 A US 8416095 B2	08/12/2010 09/04/2013
KR 10-2010-0050823 A	14/05/2010	None	
KR 10-2011-0118323 A	31/10/2011	None	