Innovation, Sciences et Développement économique Canada
Office de la Propriété Intellectuelle du Canada

Innovation, Science and Economic Development Canada
Canadian Intellectual Property Office

CA 3126835 A1 2020/08/06

(21) 3 126 835

(12) DEMANDE DE BREVET CANADIEN
CANADIAN PATENT APPLICATION

(13) A1

(86) Date de dépôt PCT/PCT Filing Date: 2020/01/29
(87) Date publication PCT/PCT Publication Date: 2020/08/06
(85) Entrée phase nationale/National Entry: 2021/07/14
(86) N° demande PCT/PCT Application No.: US 2020/015599
(87) N° publication PCT/PCT Publication No.: 2020/160098
(30) Priorités/Priorities: 2019/01/29 (US62/798,017); 2020/01/28 (US16/774,933)

(51) Cl.Int./Int.Cl. *G08B 23/00* (2006.01)

(71) Demandeur/Applicant:
POOL KNIGHT, LLC, US

(72) Inventeurs/Inventors:
GALI, RAMY R., US;
MATAR, PHILLIP E., US;
MAY, DAVID C, US

(74) Agent: RIDOUT & MAYBEE LLP

(54) Titre : SYSTEME DE SURVEILLANCE INTELLIGENT POUR PISCINES
(54) Title: SMART SURVEILLANCE SYSTEM FOR SWIMMING POOLS

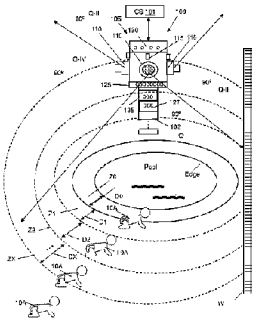


FIG. 1A

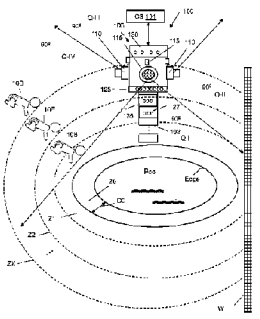


FIG. 1B

(57) Abrégé/Abstract:
A swimming pool monitoring system using a plurality of sensor systems to detect the presence of objects within a defined perimeter of the swimming pool prior to the objects reaching the edge of the pool. The objects may be people or animals. The sensor systems may include a ranging sensor, an audio sensor, an olfactory sensor and a video imaging sensor. The sensors are monitored by a computer system that has stored data for objects authorized to be within the pool perimeter. The system provides an alert or alarm upon detection of an unauthorized or unknown object in the monitored perimeter by comparing detected objects to the stored data. The system can determine the distance of the object from the pool edge and provide an adjustable alarm as the objects nears the pool edge. The system uses facial identification and voice identification to detect authorized objects and distinguish between unauthorized and unknown objects in order to establish a level of alert or alarm that can be communicated via loudspeaker, text message or email. The system can accept updated data from any sensor for adding additional authorized or unauthorized object identification data to a system database.

(12) INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
06 August 2020 (06.08.2020)

WIPO | PCT

(10) International Publication Number
WO 2020/160098 A1

(51) International Patent Classification:
G08B 23/00 (2006.01)

(21) International Application Number:
PCT/US2020/015599

(22) International Filing Date:
29 January 2020 (29.01.2020)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:

62/798,017	29 January 2019 (29.01.2019)	US
16/774,933	28 January 2020 (28.01.2020)	US

(71) Applicant: **POOL KNIGHT, LLC** [US/US]; 11517 Whispering Hollow Drive, Tampa, FL 33635 (US).

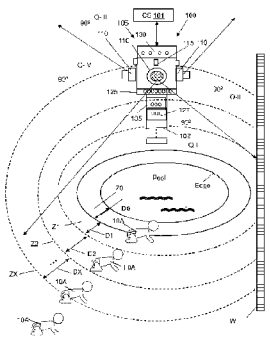
(72) Inventors: **GALI, Ramy, R.**; 9481 Campi Drive, Lake North, FL 33467 (US). **MATAR, Phillip, E.**; 11517 Whispering Hollow Drive, Tampa, FL 33635 (US). **MAY, David, C**; 3093 Cordgrass Court, The Villages, FL 32163 (US).

(74) Agent: **SANKS, Terry M.**; Beusse Wolter Sanks & Maire, PLLC, 390 N. Orange Avenue, Suite 2500, Orlando, FL 32801 (US).

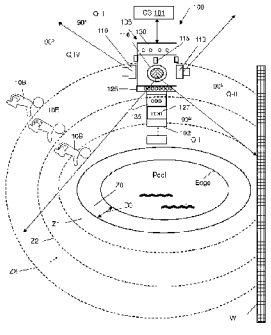
(81) Designated States *(unless otherwise indicated, for every kind of national protection available)*: AE, AG, AL, AM, AO, AT, AU, AZ, BA, BB, BG, BH, BN, BR, BW, BY, BZ, CA, CH, CL, CN, CO, CR, CU, CZ, DE, DJ, DK, DM, DO, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, GT, HN, HR, HU, ID, IL, IN, IR, IS, 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, OM, PA, PE, PG, PH, PL, PT, QA, RO, RS, RU, RW, SA, SC, SD, SE, SG, SK, SL, ST, SV, SY, TH, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, WS, 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).

(54) Title: SMART SURVEILLANCE SYSTEM FOR SWIMMING POOLS



HG. 1A



HG. 1B

(57) Abstract: A swimming pool monitoring system using a plurality of sensor systems to detect the presence of objects within a defined perimeter of the swimming pool prior to the objects reaching the edge of the pool. The objects may be people or animals. The sensor systems may include a ranging sensor, an audio sensor, an olfactory sensor and a video imaging sensor. The sensors are monitored by a computer system that has stored data for objects authorized to be within the pool perimeter. The system provides an alert or alarm upon detection of an unauthorized or unknown object in the monitored perimeter by comparing detected objects to the stored data. The system can determine the distance of the object from the pool edge and provide an adjustable alarm as the objects nears the pool edge. The system uses facial identification and voice identification to detect authorized objects and distinguish between unauthorized and unknown objects in order to establish a level of alert or alarm that can be communicated via loudspeaker, text message or email. The system can accept updated data from any sensor for adding additional authorized or unauthorized object identification data to a system database.

WO 2020/160098 A1

[Continued on next page]

WO 2020/160098 A1

Declarations under Rule 4.17:

— *as to the identity of the inventor (Rule 4.17(i))*
— *as to applicant's entitlement to apply for and be granted a patent (Rule 4.17(ii))*
— *as to the applicant's entitlement to claim the priority of the earlier application (Rule 4.17(iii))*

Published:

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

SMART SURVEILLANCE SYSTEM FOR SWIMMING POOLS

[0001]

BACKGROUND

[0002] Embodiments relate to a smart unauthorized object pool-perimeter breach alert system, method and computer readable medium to detect unauthorized and unknown objects breaching a perimeter of a pool.

[0003] Every day, about ten people die from unintentional drowning. Of these, it is estimated that two (2) are children aged 14 or younger. Drowning ranks fifth among the leading causes of unintentional injury death in the United States. From 2005-2014, there were an average of 3,536 fatal unintentional drownings (non-boating related) annually in the United States — about ten deaths per day. About one in five people who die from drowning are children 14 and younger. For every child who dies from drowning, another five receive emergency department care for non-fatal submersion injuries.

[0004] More than 50% of drowning victims treated in emergency departments (EDs) require hospitalization or transfer for further care (compared with a hospitalization rate of about 6% for all unintentional injuries). These non-fatal drowning injuries can cause severe brain damage that may result in long-term disabilities such as memory problems, learning disabilities, and permanent loss of basic functioning (e.g., permanent vegetative state). If a child falls into a pool, it takes less than 2 minutes for unconsciousness to set in and 3 to 5 minutes for brain damage to begin.

[0005] Some pool security safety devices employ sensors that are located right at the pool entry point to detect a drowning where emergency life-saving actions need to be taken without delay. Additionally, most pool security safety devices employ only one sensor type which in many cases is not optimal for the tracked object (baby, child, elderly, etc.) and end up

Date Reçue/Date Received 2021-07-14

users have low confidence and continually diminishing confidence in these systems. These systems respond to "a potential drowning is underway." Thus, emotion is high, and mistakes are prevalent.

SUMMARY

[0007] Embodiments relate to smart unauthorized object pool-perimeter breach surveillance and alert system, method and computer system to detect and provide an alarm when an unauthorized object breaches a perimeter of a pool. In one embodiment the system incorporates a plurality of sensor devices, sometimes referred to simply as sensors, for monitoring a perimeter around a swimming pool. Perimeter as used herein means a defined area or plurality of area zones surrounding a pool and is extended away from the pool a sufficient distance to allow a warning or alert to be generated before an approaching object, such as a small child, reaches an edge of the pool and may enter into the water in the pool. The sensors may comprise infrared detectors or cameras, video sensors or cameras, auditory sensors, olfactory sensors, and ultrasonic sensors. The sensors may be incorporated into the system in a form to create a geo-position sensor or detector. Each of the sensors is coupled, either by direct wiring or through a Blue Tooth broadcast and reception system or other suitable communication system to the computer system. The computer system operates to utilize signals from the sensors to detect and identify authorized and unauthorized objects entering into the monitored perimeter of the pool. The computer system includes conventional computer elements such as a processor for executing computer programs stored in RAM and ROM modules and in a writable mass storage media. The computer system may also be adapted for Cloud storage. To this end, the computer system includes an accessible and re-writable database for storage of biometric data related to objects likely to entering into the perimeter. The term "objects" will be understood to mean animate and inanimate objects, but in most instances is used to refer to persons or animals, it being understood that an alarm may be necessary when a small child, or a disabled person, or a dementia victim may be entering the pool area or perimeter without proper protection or permission. The database may store facial images of authorized objects that are allowed to be in the pool perimeter. The facial images can be compared to facial images stored in the database for identifying authorized persons. The computer system has conventional input apparatus to allow the database to be updated by entering new facial images or other biometric data into the database. The biometric data may include auditory data for voice recognition so that the

computer system functions can be controlled by authorized persons, the term persons being broadly encompassed by the term "objects".

[0008] The ability to update the computer system database may be limited to certain authorized persons, sometimes identified as administrators. In addition to voice recognition, the computer system may receive input from olfactory sensors and maintain a database of known smells or odors to further help in identifying authorized or unauthorized objects entering into the pool perimeter. Olfactory biometrics may assist in identifying a crawling baby in comparison to a small dog or cat. The ultrasonic and video sensors may also determine the orientation of an object entering into the pool perimeter, such as a standing versus crawling baby or a person who may have fallen within the perimeter. Briefly, the disclosed invention utilizes a plurality of different sensors to detect and identify objects, i.e., persons and animals, entering into a perimeter of a pool and provides an alert or alarm to responsible persons to minimize the likelihood of person or animal falling into the water within the pool and possibly drowning. The identification protocol uses different sensors to minimize false alarms so that it reduces the likelihood that the system will be disabled when the pool is being used by authorized objects, such as people or pets. As used herein, the term "object" generally refers to a living person but may also include pets, such as cats or dogs. The term "unauthorized objects" generally includes "unknown objects." However, an unauthorized object may include an identified baby or elderly person living in a household having a pool that is being monitored. An unknown object is used to refer to an object intruding into the pool perimeter where the object is not identified in the computer database. The system may be programmed to provide a different type of warning that distinguishes between an unauthorized object and an unknown object. The computer database has conventional input means for allowing biometric data to be entered into the database by an authorized person. For example, the database may be updated by entering new facial images, olfactory scents, or auditory sound data. Each of these biometric data are associated with a corresponding authorized or unauthorized object to allow the computer system to more accurately identify objects entering the monitored perimeter of the pool so that an alarm may be inhibited when the detected object is an authorized object. Similarly, the computer system can respond to detection of an unauthorized object by identifying the object and program an appropriate alert of alarm. It may be appropriated to provide a more urgent alarm if the unauthorized object is a baby or small child than might be desirable if the unauthorized object is an elderly person approaching a shallow end of the pool. Thus, the system can adapt to different

types and identities of objects and determined the level of alert that is appropriate for detected object.

BRIEF DESCRIPTION OF THE DRAWINGS

[0009] A more particular description briefly stated above will be rendered by reference to specific embodiments thereof that are illustrated in the appended drawings. Understanding that these drawings depict only typical embodiments and are not therefore to be considered to be limiting of its scope, the embodiments will be described and explained with additional specificity and detail through the use of the accompanying drawings in which:

[0010] FIG. 1A illustrates a smart unauthorized object pool-perimeter breach alert system with an unauthorized object near the perimeter of the pool in a first quadrant or sector;

[0011] FIG. 1B illustrates a smart unauthorized object pool-perimeter breach alert system with an unauthorized object near the perimeter of the pool in a fourth quadrant or sector;

[0012] FIG. 2 illustrates a block diagram of the smart object unauthorized pool-perimeter breach alert system;

[0013] FIG. 3A illustrates a block diagram of the local ambient environment condition sensors;

[0014] FIG. 3B illustrates a block diagram of geo-position sensors;

[0015] FIG. 4 illustrates a diagram of an infrared imaging sensor detecting authorized and unauthorized objects in a pool area;

[0016] FIG. 5 illustrates a graphical representation of image recognition of an unauthorized subject;

[0017] FIG. 6 illustrates a block diagram of a computer system in communication with a network; and

[0018] FIG. 7 illustrates a configurable sector sensing pattern.

DETAILED DESCRIPTION

[0019] Embodiments are described herein with reference to the attached figures wherein like reference numerals are used throughout the figures to designate similar or equivalent elements. The figures are not drawn to scale and they are provided merely to illustrate aspects disclosed herein. Several disclosed aspects are described below with reference to non-limiting example applications for illustration. It should be understood that numerous specific details, relationships, and methods are set forth to provide a full understanding of the embodiments disclosed herein. One having ordinary skill in the relevant art, however, will readily recognize

that the disclosed embodiments can be practiced without one or more of the specific details or with other methods. In other instances, well-known structures or operations are not shown in detail to avoid obscuring aspects disclosed herein. The embodiments are not limited by the illustrated ordering of acts or events, as some acts may occur in different orders and/or concurrently with other acts or events. Furthermore, not all illustrated acts or events are required to implement a methodology in accordance with the embodiments.

[0020] Notwithstanding that the numerical ranges and parameters setting forth the broad scope are approximations, the numerical values set forth in specific non-limiting examples are reported as precisely as possible. Any numerical value, however, inherently contains certain errors necessarily resulting from the standard deviation found in their respective testing measurements. Moreover, all ranges disclosed herein are to be understood to encompass any and all sub-ranges subsumed therein. For example, a range of "less than 10" can include any and all sub-ranges between (and including) the minimum value of zero and the maximum value of 10, that is, any and all sub-ranges having a minimum value of equal to or greater than zero and a maximum value of equal to or less than 10, e.g., 1 to 4.

[0021] FIG. 1A illustrates a smart unauthorized object pool-perimeter breach alert system 100 with an unauthorized object near the perimeter of the pool in a first quadrant Q-I. The quadrant may be a sector. The system 100 is configured to be installed at least in part at some location in the surrounding environment of a pool. The system 100 may be configured to detect authorized and unauthorized object near the perimeter of the pool up to 360°. In some embodiments, the installation of system 100 may only detect authorized and unauthorized object near the perimeter of the pool up to 180°, for example, because of obstructions in proximity to the pool. In other embodiments, the system 100 may be configured to detect authorized and unauthorized objects near the perimeter of the pool up to 270°.

[0022] Pools can be installed a few feet from a structure such as a home, garage, and pool house, for example, with ingress and egress. In other embodiments, a pool may be installed 50-100 feet from the home or other nearest building with ingress and egress. Thus, the installation of the system 100 may be placed within the environment to capture up to 360° so that unauthorized subjects approaching the pool from any direction up to 360° can be readily detected and especially points of ingress to the perimeter of the pool.

[0023] The system 100 may include a support structure 102 configured to have mounted thereon a sensor suite 105. The sensor suite 105 may include one or more infrared imaging

sensors 110. In the illustration, three IR imaging sensors 110 are shown capturing images in sectors or quadrants Q-I, Q-II, and Q-IV. The sensors for sector or quadrant Q-III are not shown in this illustration. In some embodiments, each IR imaging sensors 110 may have a field of view (FOV) of approximately 90°. However, for sectors smaller than 90°, the FOV may be smaller. The IR image represents a heat signature. In some embodiments, the FOV of the imaging sensors 110 may overlap with an adjacent imaging sensor 110 so that there are no blind spots in the space around the perimeter of the pool. In other embodiment, the FOV of the IR imaging sensors 110 may be 180°. Accordingly, the system 100 would require less IR imaging sensors. In other embodiments, each sector or quadrant may have more than one IR imaging sensor. The sensor suite 105 may include red, green, blue (RGB) imaging sensors 115. The RGB image captured by the imaging sensors 115 may be used to compare some of the stored signatures of the local environment from a current image to remove those pixels of the local environment to isolate the image data of a current subject. As described herein, an image may include one or both of an RGB image data and an IR image data. The image data may include RGB image data and/or IR image data. Many high-quality security cameras are available to act as both day and night imaging sensors, such as, for example, a Nest Cam Outdoor Security camera with 1080p HD night vision and 130-degree wide angle view.

[0024] In some embodiments, the IR imaging sensors 110 are used during the night hours or conditions so that a heat signature of breaching objects can be detected in the dark. In some embodiments, the RGB imaging sensors 115 are used during the daylight hours since the image quality by RGB imaging sensors 115 deteriorates during low light (night-time) conditions.

[0025] The sensor suite 105 may include one or more auditory sensors 125 to detect ambient sounds in the environment in proximity to the pool, including voice sounds or auditory sounds of objects and ambient sounds naturally occurring. In some embodiments, auditory sensors 125 may be installed in at least one quadrant to detect incoming ambient sounds in the perimeter of the pool. In some embodiments, the auditory sensors 125 may be used to identify authorized and unauthorized subjects in the perimeter of the pool using a voice signature. The auditory sounds of a subject may include audible sounds from an unauthorized animal, such as a pet, or other unauthorized persons such as a baby, child, elderly adult, disabled or dementia suffering person.

[0026] The sensor suite 105 may include one or more olfactory sensors 127 to detect specific object emanating smells in the environment. The sensor suite 105 may include local ambient environment condition (LAEC) sensors 130. The LAEC sensors 130 will be described in more detail in relation to FIG. 3A.

[0027] The sensor suite 105 may include geo-position sensors 135 to determine a range of an unauthorized object 10A relative to the edge of the pool or other boundaries. The range of the unauthorized object 10A may be used in determining the timing of alerts and/or sequence of alert communications as the estimated time-of-arrival or range from the subject 10A to zone Z0 or the edge of the pool decreases. The geo-position sensors 135 may include, without limitation, an ultrasonic range sensor 360 (FIG. 3B).

[0028] The system 100 may include a computer system (CS) 101 in communication with the sensor suite 105. The computer system 101 will be described in more detail in relation to FIG. 6. The computer system 101 may be remote from the sensor suite 105. The computer system 101 may be distributed such that parts of the computer system 101 are integrated with the sensor suite 105 while other parts of the computer system 101 are remote. One or more distributed parts of the computer system 101 may provide the user with user interfaces for setting up the system 100 and uploading voice signatures, face recognition signatures, object specific smell signatures and/or scene recognition signatures. The user interfaces may allow the computer system to receive alert recipient lists, mode of delivery of the alert, etc. The distributed parts of the computing system 101 may communicate with each other using wired or wireless communication modalities including, without limitation, WIFI.

[0029] In FIG. 1A, by way of non-limiting example, the perimeter surrounding the pool is marked by zones Z0, Z1, Z2, ..., ZX wherein X may be a non-zero integer. The zone Z0 is closest to the pool and may include the edge of the pool. The zone Z0 may have the distance D0 between the end of zone Z1 or beginning of zone Z0 and the edged of the pool or the end of zone Z0. The zone Z1 may have the distance D1 between the end of zone Z2 or beginning of zone Z1 and the end of zone Z1. The zone Z2 may have the distance D2 between the end of zone ZX or beginning of zone Z2 and the end of zone Z2. The zone ZX may have the distance DX between the beginning of zone ZX and the end of zone ZX.

[0030] In the example, the zone 1 may surround the zone Z0 up to 360°. The distance D1 may be the same around zone Z0 or may be varied. For example, some area of D1 may be narrower in places and/or wider in other places. Likewise, the distance D2 may be the same

around zone 1 or may be varied. The distance DX may be the same around zone 2 or previous zone or may be varied. The distances D0, D1, D2, ..., DX may be the same or different.

[0031] In FIG. 1A, the unauthorized object 10A is shown moving from an area outside of zone ZX through zone ZX, zone Z2, Zone Z1 and to zone Z0 wherein zone Z0 is immediately adjacent to the pool. An unauthorized object 10A in zone Z0 may indicate an imminent pool breach. By way of non-limiting example, zone ZX may be used to detect when an unauthorized object 10A initially breaches a perimeter zone of the pool. Each zone moving closer toward the pool or zone Z0 may raise the alert level as each subsequent zone is breached. For example, zone ZX may have the lowest alert level while zone Z0 has the highest alert level. Each alert level may include a different sequence of alerts, a different alert message or alert indicator, and/or a different list of alert recipients, by way of non-limiting example.

[0032] Zones ZX, Z2, and Z1 on the right side of figure are discontinued by virtue of a structure, such as wall W. The wall W is just an example of a possible structure in a pool area. Accordingly, the zones discontinued, on the side of the wall opposite the side within the pool perimeter environment, may not require ranging and/or detection of unauthorized subjects. The zones around the perimeter may include those zones which have possible ingress to the pool.

[0033] By way of another example, assume that the zone Z1 has a barrier such a fence which can be removed when the pool is in use. The fence, when deployed, may designate a No-Go-Zone where no persons should breach. The term "no persons" may include those persons without a previously stored image, sometimes referred to as unknown persons. In some embodiments, those unknown persons may still be detected, if they breach the No-Go-Zone (the area beyond the fence). Sometimes, an unauthorized object may be an unknown person not yet known to the pool owners. For example, an unknown subject may be an adult neighbor, neighborhood teens, and small children entering the perimeter of the pool without permission. The system 100 may include a list of authorized objects so that anyone detected, regardless of size, which are not on the authorized subjects list can be considered an "unauthorized object." For example, the current facial identification database may include pool owner family members including AUTHORIZED mother, father and other responsible and capable family members (teenagers). It may also include unauthorized family members that are not allowed in the pool area unattended by an authorized adult . This feature may serve to prevent drowning by persons breaching the security fence

[0034] The system 100 may include selectable modes of operation which allow unidentified persons to be detected without the cause for alarm. For example, if an unknown person is accompanied by an authorized person in the perimeter of the pool, an alert may not be required.

[0035] FIG. 1B illustrates a smart unauthorized object pool-perimeter breach alert system 100 with an unauthorized object 10B near the perimeter of the pool in a fourth sector or quadrant Q-IV. As described in relation to FIG. 1A, the area represented by sector or quadrant Q-IV has egress to the pool. By way of non-limiting example, egress to the perimeter of the pool may be from a door located in a kitchen area through which the unauthorized object 10B may exit to enter sector or quadrant Q-IV. On the other hand, egress to the perimeter of the pool may be from a door located in a laundry room through which the unauthorized object 10B may exit to enter sector or quadrant Q-I.

[0036] In some embodiments, the wall may represent a portion of a screen enclosure around a pool. Screen enclosures may connect to buildings to provide egress from the building into the pool area through a doorway, for example, while the enclosure blocks access along other sides surrounding the pool. Accordingly, depending on installation of system 100, imaging and ranging functions may only require 180° of observation instead a full 360°.

[0037] FIG. 2 illustrates a block diagram of the smart unauthorized object pool-perimeter breach alert system 100 of FIGS. 1A and 1B. The sensor suite 105 may include sensor types such as infrared (IR) imaging sensors 110, RGB imaging sensors 115, auditory sensors 125, olfactory sensors 127, local ambient environment condition (LAEC) sensors 130, and geo-position sensor 135. The suite 105 may distribute multiple sensors of some or all types up to 360°. For example, the sensor suite may include one geo-position sensor 135 configured to perform ranging up to 360°, while each sector or quadrant monitored may include one IR imaging sensor 110 and at least one geo-position sensor 135. The sensor suite 105 may include only one set of LAEC sensors 130 since the environmental conditions would not change quadrant to quadrant.

[0038] Each IR imaging sensor110 may include a night vision mode 111 and a daylight vision mode 112. The system 100 may include one or more processors 220. The one or more processors 220 may be part of the computer system 101. The processor 220 may include imaging processing functions to process both IR images and RGB images. The system 100 may include alert communicator 240 to alert at least one alert recipient 245 at an address according to

an identified alert delivery mode. The alert delivery mode may include text messages, a call to a land-line phone number, a call to a mobile phone number, communications using voice over Internet protocol (VOIP), and an email to an email address(s).

[0039] The system 100 may include applications 207 for performing the functions herein. The applications 207 may include various data sets for access by the applications to be entered by various graphical user interfaces (GUI). For example, the applications 207 may include at least one GUI 250 for entering a subject list GUI 250 identifying those subjects considered unauthorized. In some embodiments, the objects may include both authorized and unauthorized. The object list GUI 250 may include a user interface to establish unauthorized subject face (recognition) signatures 252 and unauthorized object speech (recognition) signatures 254. The object list GUI 250 may include a user interface to establish authorized object face (recognition) signatures 252 and authorized object speech (recognition) signatures 254, in some embodiments.

[0040] The GUI 250 may allow a user to capture face signatures 252 using the GUI 250 or select an existing picture to upload the face signature 252. Likewise, the GUI 250 may allow the user to capture voice signatures 254 or select an existing voice signature. Thus, data representative of voice captured in the real-time ambient sounds, via the auditory sensors 125, may be used by the speech recognition module 270 to detect and pair the captured sound to the voice signature of an authorized or unauthorized object during a measurement cycle.

[0041] The range/direction estimator 275 may determine a direction of ingress of the unauthorized object using data points collected by one or more sensors of the geo-position (GP) sensors 135. Each GP sensor 135 may provide a sensed signal to the range/direction estimator 275 at the same measurement cycle. The range/direction estimator 275 may include an ultrasonic range measurement module (not shown). The ultrasonic data points are captured by directing ultrasonic frequency waves from at least one ultrasonic ranging sensor 360 (FIG. 3B) into the perimeter of the pool.

[0042] For example, each sector or quadrant may include an ultrasonic ranging sensor 360 configured to detect the return of propagated ultrasonic frequency waves. The returning ultrasonic frequency waves are measured by the range/direction estimator 275 to estimate a range of a subject within the perimeter of the pool. Other imaging data may be used in ranging.

[0043] The ranging estimations may receive data from the geo-position sensors 135 to provide an estimated time of arrival based at least on one set of data points.

[0044] The applications 207 may include a local scene information GUI 260. The local scene information GUI 260 may allow a user to identify one or more boundaries and/or zones in the perimeter of the pool. The GUI 260 may be used to capture local scene information and establish boundaries or zones to establish a hierarchy of alert levels. Nonetheless, only one alert boundary may be established.

[0045] The applications 207 may include a face recognition module 265 configured to process data representative of an image of a captured face 58 of the subject 57 (FIG. 5) in the proximity of the pool to determine whether the captured face 58 is recognized as a match to a face signature of an unauthorized subject. The operation of the face recognition module 265 may be described in more detail in relation to FIG. 5. The applications 207 may include a speech recognition module 270 configured to recognize a captured voice signal 58 of the subject 57 (FIG. 5) in the proximity of the pool. The system 100 may use the auditory sensors to detect voice of a subject and environmental sounds which may be extracted or filtered from a received auditory signal during a measurement cycle to isolate the voice of the subject from the ambient environmental sounds.

[0046] The applications 207 may include a machine learning module 285. The machine learning module 285 may track data points over time used for alerts to minimize false alarms. The tracked data points may be stored locally or remotely in a cloud server. The applications 207 may include an unauthorized subject image generator 290 based on the captured image data of a detected unauthorized subject at any measurement cycle or when an alert is to be generated. It can be used to detect moving image object behavior, changes to specific object behavior, behavior anomalies, etc. Separate application 207 instances may also be used to provide machine learning data from the auditory and olfactory sensors, as well to help improve the sensors signature recognition performances.

[0047] The applications 207 may include a user alert GUI 295. The application 207 may generate an alert communication to be transmitted to an alert recipient identifying an unauthorized subject in the perimeter of the pool. The alert communication may include an image of the detected unauthorized subject via the user alert GUI 295. The alert communicator 240 transmits, according to an alert delivery mode, a text message, user alert GUI, or email to an identified alert recipient. The alert may be sent to at least one mobile device 30A, computing device 30B, or other communication device set by the recipient. The alert communicator 240 may transmit an alert to a local first responder 30C. The user alert GUI 295 may communicate

images with colored annotations showing where the system 100 has detected one or more "signatures of concern" representative of unauthorized subjects in breach of the perimeter of the pool and, in some cases, a pool breach.

[0048] The system 100 may be configured to generate a plurality of data points for breach alert generation. By way of non-limiting example, approximately 40 decision data points may be used to attempt to, with high levels of confidence and accuracy, alert users that an unauthorized object ("baby Jane," grandpa Mike) is about to enter the pool or particular zone in a perimeter adjacent to the pool. The system 100 may leverage smart phones, call lists, HD (High Definition) images and video to give the user (alert recipient) real-time data to formulate an appropriate response once a breach is alerted. For example, a parent may rush to close and lock a pool gate before the baby gets to the pool edge or intercept the baby from its path to the pool.

[0049] The system 100 uses the sensor suite 105 and analytic software that attempts to predict if a specific user specified unauthorized subject (baby, elder, puppy, etc.) is attempting to advance towards the pool area or No-Go Zone. Instead of looking at a drowning situation in-process, system 100 may perform a look-ahead process to determine at least one of a direction, range and speed of an unauthorized subject to generate an alert to try to avoid breach of the pool or pool edge. Thus, a drowning situation can be averted, such that the unauthorized subject is detected and apprehended before reaching the water. Rather than alerting the user that a drowning in underway, the system 100 attempts to predict and guide resources to block or intercept unauthorized subjects before a drowning in underway.

[0050] The system 100 uses the decision data points (i.e., approximately 40) to achieve a higher level of detail and decision-making accuracy to predict a potential pool breach condition or imminent pool breach condition is about to happen with a specific unauthorized subject (baby, etc.) in an effort to prevent drowning by the unauthorized subject. The system 100 can also detect when a pool is breached presenting a potential drowning condition. The system 100 does more than just detect something in or around the pool. The system 100 progresses up the data gathering and decision-making process to detect, determine orientation and/or direction of, track a range of, recognize and identify an unauthorized subject. The system 100 may first determine gather data points to determine if the subject entering the designated perimeter of the pool is an unauthorized subject. If the subject is determined to be other than an unauthorized subject, the data gathering process may end for that specific subject in the perimeter of the pool.

By way of non-limiting example, the system 100 is configured to detect multiple subjects breaching a perimeter of a pool. Such subjects may be authorized or unauthorized.

[0051] The system 100 may employ image processing techniques based on a Johnson Criteria and the "DORI" acronym. The image processing techniques may provide a 25% confidence level at the "Detection level" (D) of the image processing technique. The confidence may increase to approximately 50% when the "Orientation level" (O) in an image is examined or detected using the image processing techniques. Then the confidence level may step up to approximately a 75% level when the "Recognition level" (R) of subjects in the image is examined and detected. Additionally, the confidence level may further improve to approximately 100% when the "Identification level" (I) of the subjects in the image is examined. With nearly a 100% level of confidence in a decision to provide an alert reduces false alarms to the end-user.

[0052] The system 100 uses warm body IR (Infrared) sensors 110, geo-position sensors 135 (ultrasonic range sensor, visual (RGB) detection sensors and image processing software), auditory sensors 125, and olfactory sensors (smell) 127. Internet data representative of local environment information (time-of-day, temperature, weather conditions) may allow sensors of the sensor suite 105 to adjust to real-time local environmental conditions (e.g., day versus night, snow, etc.) to optimize captured sensor data integrity of the detected real-time signatures. The real-time signatures are used for comparison with stored signatures of unauthorized subjects.

[0053] The system 100 may include a speaker 247 in the perimeter of the pool to alert those in the area. For example, while others are using the pool, an unauthorized subject may still be monitored to generate a local alert of imminent breach of the pool edge by such unauthorized subject to prevent accidental drowning.

[0054] FIG. 3A illustrates a block diagram of the local ambient environment condition (LAEC) sensors 130. The LAEC sensors 130 may include a temperature sensor 332 configured to sense the current ambient temperature of the environment associated with the scene. The LAEC sensors 130 may include a humidity sensor 334 configured to sense a quantity of humidity in the environment associated with the scene.

[0055] FIG. 3B illustrates a block diagram of geo-position sensors 135. The geo-position sensors 135 may include one or more of an ultrasonic range sensor 360 and image processing module 366. The image processing module 366 may be shared by other sensor types. The geo-position sensors 135 may use image data from one or more RGB imaging sensors 115

for determining geo-position data points. The geo-position sensors 135 may be used in detection and identification of an orientation of subject in the perimeter of the pool, for example. A height from the ground may be determined for use in locating a face of a subject, which may be a potential unauthorized subject. The orientation may include crawling signaling a potential baby or toddler. The system 100 may detect whether the subject is crawling. The orientation may be sitting, such as in a wheelchair. An unauthorized subject may include babies, toddlers, small children and disabled or elderly persons using walking assist devices. Walking assist devices may include wheelchairs, walkers, and canes. Subjects using walking assist devices may trip or fall in the perimeter of the pool. The detected change in orientation of unauthorized subjects with walking assist device may signal a fall in the area of the perimeter of the pool or if the pool was breached.

[0056] The LAEC sensors 130 may include ambient lighting sensor 336 configured to sense a quantity of ambient light in the environment associated with the scene. The quantity of light may be a function of daylight, nighttime, dusk and/or dawn. The quantity of ambient light may be a function of natural light from the sun without the addition of supplemental light such as from electrical lighting devices in the environment. During the nighttime hours, the surrounding ambient light may be detected at a higher level with the aid of supplemental lighting. The ambient lighting may control the modes of the IR imaging sensors 110. During low light conditions, the IR imaging sensors 110 may operate in a night vision mode 111. In normal or daylight conditions, the IR imaging sensors 110 may operate in a daylight vision mode 112.

[0057] The LAEC sensors 130 may include weather data 338 such as sensed or detected at a remote local weather station. The LAEC sensors 130 may communicate, such as via the Internet, with the weather station to obtain current weather conditions sensed or detected by the weather station. The LAEC sensors 130 may be configured to communicate with the remote weather station to object current weather conditions. The weather conditions may be updated with the reading of the local sensors of system 100. The weather conditions or local ambient environmental conditions may cause the performance of system 100 to be controlled such as in the presence of snow, the presence of fog, high wind conditions, extreme weather conditions, etc. For example, the presence of snow may change the image of the scene. Accordingly, the local scene recognition module 280 may vary a scene signature used in a current breach

detection cycle. For example, local scene signatures may include scene signatures for snow conditions, fog conditions, and rain conditions, for example.

[0058] FIG. 4 illustrates a diagram of an infrared (IR) imaging sensor 110 detecting authorized and unauthorized subjects in a pool area. The IR imaging sensor 110 may be coupled to a lens 412. The lens 412 may be dome shaped in some embodiments. The lens 412 may include a plurality of Fresnel lens 413 arranged in a dome shape. The light passing through the lens 412 or each Fresnel lens 413 is passed to the IR image sensor 110 to capture the propagated light of the scene. Additionally, the lens 412 or each Fresnel lens 413 may be responsive to infrared (IR) wavelengths to detect a heat pattern within the scene.

[0059] By way of non-limiting example, an authorized subject may include an adult 40B. Non-authorized subjects may include, without limitation, disabled persons 40A, children 40C, and animals 40D. Non-authorized subjects may be those subjects which are not capable of swimming in a pool. Some adults may not be able to swim and would also be an unauthorized subject. In some instances, animals 40D which are known to have the capacity to swim may be an authorized subject.

[0060] FIG. 5 illustrates a very simplified graphical representation of image recognition of an unauthorized subject 57. The unauthorized subject 57 is a child. Most facial recognition algorithms use over 100 facial data measurement points and use multiple facial images of each authorized and unauthorized object. The Facial Recognition application uses Machine Learning to create an AI dataset that allows the calculation and comparison of facial signatures to provide Facial Recognition of a generic face in a video frame which then leads to Facial Identification of unique faces as members of a pool-owners family. .The system 100 may be configured to compare a face (recognition) signature 252 which is associated with unauthorized subject 57. By way of non-limiting example, the face recognition module 265 may be configured to compare stored face signature data with the captured face 58 of the subject 57 in the proximity of the pool. The system 100 may use computer vision to locate the face 58 of the subject 57 for comparing the stored face signature 252 to the instant captured face 58. The face recognition module 265 may locate the eyes 541 and 542 on the face 58 of the subject 57 to compare the eyes of the face signature 252 with the captured image data representative of the eyes 541 and 542 of the subject 57.

[0061] The face recognition module 265 may locate the nose 544 on the face 58 of the subject 57 to compare the nose of the face signature 252 with the captured image data representative of the nose 544 of the subject 57. The face recognition module 265 may locate the mouth 546 on the face 58 of the subject 57 to compare the mouth of the face signature 252 with the captured image data representative of the mouth 546 of the subject 57.

[0062] The face recognition module 265 may locate the cheeks and/or cheekbones 543 and 545 on the face 58 of the subject 57 to compare the cheeks and/or cheekbones of the face signature 252 with the captured image data representative of the cheeks and/or cheekbones 543 and 545 of the subject 57. Other facial features may also be determined, such as the forehead and chin to name a few.

Computational Hardware Overview

[0063] FIG. 6 illustrates a block diagram of a computer system 601 (i.e., computer system 101) in communication with a network. The block diagram of FIG. 6 illustrates a computer system 601 (i.e., computer system 101) upon which an embodiment of the invention may be implemented or employed. Computer system 601 includes a communication mechanism such as a bus 610 for passing information between other internal and external components of the computer system 601. Information is represented as physical signals of a measurable phenomenon, typically electric voltages, but including, in other embodiments, such phenomena as magnetic, electromagnetic, pressure, chemical, molecular atomic and quantum interactions. For example, north and south magnetic fields, or a zero and non-zero electric voltage, represent two states (0, 1) of a binary digit (bit). Other phenomena can represent digits of a higher base. A superposition of multiple simultaneous quantum states before measurement represents a quantum bit (qubit). A sequence of one or more digits constitutes digital data that is used to represent a number or code for a character. In some embodiments, information called analog data is represented by a near continuum of measurable values within a particular range. Computer system 601, or a portion thereof, constitutes a means for performing one or more steps of one or more methods described herein.

[0064] A sequence of binary digits constitutes digital data that is used to represent a number or code for a character. A bus 610 includes many parallel conductors of information so that information is transferred quickly among devices coupled to the bus 610. One or more processors 603 for processing information are coupled with the bus 610. A processor 603

performs a set of operations on information. The set of operations include bringing information in from the bus 610 and placing information on the bus 610. The set of operations also typically include comparing two or more units of information, shifting positions of units of information, and combining two or more units of information, such as by addition or multiplication. A sequence of operations to be executed by the processor 603 constitutes computer instructions.

[0065] Computer system 601 also includes a memory 604 coupled to bus 610. The memory 604, such as a random access memory (RAM) or other dynamic storage device, stores information including computer instructions. The memory 604 may also include dynamic memory which allows information stored therein to be changed by the computer system 601. RAM allows a unit of information stored at a location called a memory address to be stored and retrieved independently of information at neighboring addresses. The memory 604 is also used by the processor 603 to store temporary values during execution of computer instructions. The computer system 601 also include a read only memory (ROM) 606, non-volatile persistent storage device or static storage device coupled to the bus 610 for storing static information, including instructions, that is not changed by the computer system 601. The ROM 606 may be a secure byte-addressable memory (storage) device or a direct-access for files (DAX) memory device. The bus 610 may also have coupled thereto other storage devices including a non-volatile (persistent) storage device, such as a magnetic disk or optical disk, for storing information, including instructions, that persists even when the computer system 601 is turned off or otherwise loses power.

[0066] Information, including instructions, is provided to the bus 610 for use by the processor from an external input device 612, such as a keyboard containing alphanumeric keys operated by a human user, or a sensor. A sensor detects conditions in its vicinity and transforms those detections into signals compatible with the signals used to represent information in computer system 601. Other external devices coupled to bus 610, used primarily for interacting with humans, include a display device 614, such as a cathode ray tube (CRT) or a liquid crystal display (LCD), light emitting diode (LED) displays, for presenting images, and a pointing device 616, such as a mouse or a trackball or cursor direction keys, for controlling a position of a small cursor image presented on the display device 614 (i.e., display device 114) and issuing commands associated with graphical elements presented on the display 614.

[0067] In the illustrated embodiment, special purpose hardware, such as an application specific integrated circuit (IC) 620, may be coupled to bus 610. The special purpose hardware

may be configured to perform operations not performed by processor 603 quickly enough for special purposes. Examples of application specific ICs include Graphics Processing Units (GPU) for generating images for display device 614, cryptographic boards for encrypting and decrypting messages sent over a network, speech recognition, and interfaces to special external devices, such as robotic arms and medical scanning equipment that repeatedly perform some complex sequence of operations that are more efficiently implemented in hardware.

[0068] Computer system 601 also includes one or more instances of a communications interface 670 coupled to bus 610. Communication interface 670 provides a two-way communication coupling to a variety of external devices that operate with their own processors, such as printers, scanners and external disks. For example, the communication interface 670 may interface with the sensor suite 205 (FIG. 2) wherein applications 207 (FIG. 2) are configured to be stored in memory 604, 606 and/or storage device 608 and executed by processor 603 to perform the functions described herein.

[0069] In general, the computer system 601 through the communication interface 670 may be coupled with a network link 678 that is connected to a local network 680 to which a variety of external devices with their own processors are connected. In some embodiments, the local network 680 may be a private network and may include wired and/or wireless communications. For example, communication interface 670 may be a parallel port or a serial port or a universal serial bus (USB) port on a personal computer. In some embodiments, communications interface 670 is an integrated services digital network (ISDN) card or a digital subscriber line (DSL) card or a telephone modem that provides an information communication connection to a corresponding type of telephone line. In some embodiments, a communication interface 670 may be a cable modem that converts signals on bus 610 into signals for a communication connection over a coaxial cable or into optical signals for a communication connection over a fiber optic cable. As another example, communications interface 670 may be a local area network (LAN) card to provide a data communication connection to a compatible LAN, such as Ethernet. Wireless links may also be implemented. Carrier waves, such as acoustic waves and electromagnetic waves, including radio, optical and infrared waves travel through space without wires or cables. Signals include man-made variations in amplitude, frequency, phase, polarization or other physical properties of carrier waves. For wireless links, the communications interface 670 sends and receives electrical, acoustic or electromagnetic signals, including infrared and optical signals, that carry information streams, such as digital

data. Communication interfaces between one or more user interfaces (i.e., devices 613, 614 and 616) may communicate via communication interface 670 using BLUETOOTH, WIFI, and/or near field wireless communication modalities. Communications from computing system 601 with in-range mobile devices 30A or computing devices 30B may use BLUETOOTH, WIFI, and/or near field wireless communication modalities. Distributed components of the computing system 101 may communicate via BLUETOOTH, WIFI, and/or near field wireless communication modalities. The term computer-readable medium is used herein to refer to any medium that participates in providing information to processor 603, including instructions for execution. Such a medium may take many forms, including, but not limited to, non-volatile media, volatile media and transmission media. Non-volatile media include, for example, optical or magnetic disks, such as storage device. Volatile media include, for example, dynamic memory 604. Transmission media include, for example, coaxial cables, copper wire, fiber optic cables, and waves that travel through space without wires or cables, such as acoustic waves and electromagnetic waves, including radio, optical and infrared waves. The term computer-readable storage medium is used herein to refer to any medium that participates in providing information to processor 603, except for transmission media.

[0070] Common forms of computer-readable media include, for example, a floppy disk, a flexible disk, a hard disk, a magnetic tape, or any other magnetic medium, a compact disk ROM (CD-ROM), a digital video disk (DVD) or any other optical medium, punch cards, paper tape, or any other physical medium with patterns of holes, a RAM, a programmable ROM (PROM), an erasable PROM (EPROM), a FLASH-EPROM, or any other memory chip or cartridge, a carrier wave, or any other medium from which a computer can read. The term non-transitory computer-readable storage medium is used herein to refer to any medium that participates in providing information to processor 603, except for carrier waves and other signals.

[0071] Logic encoded in one or more tangible media includes one or both of processor instructions on a computer-readable storage media and special purpose hardware, such as ASIC 620.

[0072] Network link 678 typically provides information communication through one or more networks to other devices that use or process the information. For example, network link 678 may provide a connection through a private or local network 680 to a host computer 682, such as a secure host computer. For example, in some embodiments, the pilot may be located at

the host computer 682. Thus, the user interfaces referenced in FIG. 6, may be located with the host computer 682. In some embodiments, the computer system 601 may be positioned with the sensor suite 105 while the host computer 682 is a remote from the sensor suite. The computer system 601 may be located on support structure 102. The host computer 682 may be located within a building or residence. The host computer 682 and the computer system 601 may be configured as a distributed embodiment of computing system 101.

[0073] In some embodiments, the computer system 601 may connect to equipment 684 operated by an Internet Service Provider (ISP) or Intranet Service Provider. ISP equipment 684 in turn provides data communication services through the public, world-wide packet-switching communication network of networks now commonly referred to as the Internet 690 or alternately over an Intranet. The computing system 101 may access local environmental data over the Internet 690.

[0074] A computer called a server 692 connected to the Internet or Intranet provides a service in response to information received over the Internet or Intranet. For example, server 692 provides information representing video data for presentation at display 614 or the server may receive information representing video data for display at a location remote from the system 100 (FIGS. 1A and 1B).

[0075] The invention is related to the use of computer system 601 for implementing the techniques described herein. According to one embodiment of the invention, those techniques are performed by computer system 601 in response to at least one processor 603 executing one or more sequences of one or more instructions contained in memory 604 to form a computer program product. Such instructions, also called software and program code, may be read into memory 604 from another computer-readable medium such as storage device 608. Execution of the sequences of instructions contained in memory 604 causes processor 603 to perform the method and functions described herein. In alternative embodiments, hardware, such as application specific integrated circuit 620, may be used in place of or in combination with software to implement the invention. Thus, embodiments of the invention are not limited to any specific combination of hardware and software.

[0076] Computer program code for carrying out operations described above may be written in a variety of programming languages, including but not limited to a high-level programming language, such as without limitation, Python, C or C++, for development convenience. In addition, computer program code for carrying out operations of embodiments

described herein may also be written in other programming languages, such as, but not limited to, interpreted languages. The program code may include hardware description language (HDL) or very high speed integrated circuit (VHSIC) hardware description language, such as for firmware programming. Some modules or routines may be written in assembly language or even micro-code to enhance performance and/or memory usage. It will be further appreciated that the functionality of any or all of the program modules may also be implemented using discrete hardware components, one or more application specific integrated circuits (ASICs), or a programmed Digital Signal Processor (DSP) or microcontroller. A code in which a program of the embodiments is described can be included as a firmware in a RAM, a ROM and a flash memory. Otherwise, the code can be stored in a non-transitory, tangible computer-readable storage medium such as a magnetic tape, a flexible disc, a hard disc, a compact disc, a photo-magnetic disc, a digital versatile disc (DVD) or the like.

[0077] The signals transmitted over network link 678 and other networks through communications interface 670, carry information to and from computer system 601. Computer system 601 can send and receive information, including program code, through the networks 680, 690 among others, through network link 678 and communications interface 670. In an example using the Internet 690, a server 692 transmits program code for a particular application, requested by a message sent from computer system 601, through Internet 690, ISP equipment 684, local network 680 and communications interface 670. The received code may be executed by processor 603 as it is received or may be stored in storage device 608 or other non-volatile storage for later execution, or both. In this manner, computer system 601 may obtain application program code in the form of a signal on a carrier wave. The host computer 682 may control the computing system 601 in some instances.

[0078] Various forms of computer readable media may be involved in carrying one or more sequence of instructions or data or both to processor 603 for execution. For example, instructions and data may initially be carried on a magnetic disk of a remote computer such as host computer 682. The remote computer loads the instructions and data into its dynamic memory and sends the instructions and data over a telephone line using a modem. A modem local to the computer system 601 receives the instructions and data on a telephone line and uses an infra-red transmitter to convert the instructions and data to a signal on an infra-red a carrier wave serving as the network link 678. An infrared detector serving as communications interface 670 receives the instructions and data carried in the infrared signal and places information

representing the instructions and data onto bus 610. Bus 610 carries the information to memory 604 from which processor 603 retrieves and executes the instructions using some of the data sent with the instructions. The instructions and data received in memory 604 may optionally be stored on storage device 608, either before or after execution by the processor 603.

[0079] The memory 604 may have stored thereon applications 207 (FIG. 2) implemented as software or computer instructions. The applications when executed by the processor 603 may perform one or more functions as described herein. In FIG. 2, a dedicated processor 220 may be provided for processing the captured images by the IR image sensors 110.

[0080] FIG. 7 illustrates a configurable sector sensing pattern 700. A sector may be a quadrant in some examples. However, for systems 100 which monitor areas less than 360°, the monitored may be sectorized into adjacent sectors. In the pattern 700, area 705 may be the FOV of a passive IR imaging sensor 110. In the pattern 700, area 710 may be the FOV of a Pixy RGB imaging sensor or camera. In the pattern 700, area 720 may be the FOV of a NoIR imaging sensor or camera. In the pattern 700, area 730 may be the FOV of the ultrasonic ranging sensor 360. In some embodiments, the system 100 may use different FOVs than those shown in FIG. 7.

[0081] The system 100 may include lighting such as flood lighting or IR LEDs for imaging at night.

[0082] The terminology used herein is for the purpose of describing particular embodiments only and is not intended to be limiting. As used herein, the singular forms "a," "an," and "the" are intended to include the plural forms as well, unless the context clearly indicates otherwise. Furthermore, to the extent that the terms "including," "includes," "having," "has," "with," or variants thereof are used in either the detailed description and/or the claims, such terms are intended to be inclusive in a manner similar to the term "comprising." Moreover, unless specifically stated, any use of the terms first, second, etc., does not denote any order or importance, but rather the terms first, second, etc., are used to distinguish one element from another.

[0083] Unless otherwise defined, all terms (including technical and scientific terms) used herein have the same meaning as commonly understood by one of ordinary skill in the art to which embodiments of the invention belongs. It will be further understood that terms, such as those defined in commonly used dictionaries, should be interpreted as having a meaning that is

consistent with their meaning in the context of the relevant art and will not be interpreted in an idealized or overly formal sense unless expressly so defined herein.

[0084] While various disclosed embodiments have been described above, it should be understood that they have been presented by way of example only, and not limitation. Numerous changes, omissions and/or additions to the subject matter disclosed herein can be made in accordance with the embodiments disclosed herein without departing from the spirit or scope of the embodiments. Also, equivalents may be substituted for elements thereof without departing from the spirit and scope of the embodiments. In addition, while a particular feature may have been disclosed with respect to only one of several implementations, such feature may be combined with one or more other features of the other implementations as may be desired and advantageous for any given or particular application. Furthermore, many modifications may be made to adapt a particular situation or material to the teachings of the embodiments without departing from the scope thereof.

[0085] Further, the purpose of the foregoing Abstract is to enable the public generally and especially the scientists, engineers and practitioners in the relevant art(s) who are not familiar with patent or legal terms or phraseology, to determine quickly from a cursory inspection the nature and essence of this technical disclosure. The Abstract is not intended to be limiting as to the scope of the present disclosure in any way.

[0086] Therefore, the breadth and scope of the subject matter provided herein should not be limited by any of the above explicitly described embodiments. Rather, the scope of the embodiments should be defined in accordance with the following claims and their equivalents.

The invention claimed is:

1. A swimming pool monitoring system comprising:

a plurality of sensor systems for detecting the presence of objects within a defined perimeter of the swimming pool, the sensor systems including a ranging sensor and a video imaging sensor; and

a computer system operatively coupled to the sensor systems and including data storage for storing a plurality of predetermined images of objects and for processing ranging signals and video images from the sensor systems, the computer system comparing images of detected images of objects within the perimeter of the swimming pool to the stored predetermined images to identify unauthorized objects entering into the perimeter of the swimming pool, the computer system further using the ranging signals to determine a distance from the unauthorized object to an edge of the swimming pool and motion of the object toward the pool for providing an alarm when the unauthorized object approaches to within a predetermined distance of the pool edge; and

an infrared sensor, a geo-position sensor comprising an ultrasonic range sensor and video detection sensors with a non-transitory computer readable medium storing a program causing the computer system to execute image processing, an auditory sensor and an olfactory sensor, each providing data to the computer system for enabling identification of objects entering into the pool perimeter area.

2. The swimming pool monitoring system of claim 1, wherein the computer system analyzes the video images to determine orientation and size of the unauthorized object within the perimeter of the pool.

3. The swimming pool monitoring system of claim 1, wherein the computer system computes an approach velocity of the unauthorized object toward the pool and provides alarms commensurate with the approach velocity and nearness to the pool edge.

4. The swimming pool monitoring system of claim 1, wherein the sensor systems include an auditory sensor for detecting sounds within the perimeter of the pool and the computer system includes voice identification system for identifying authorized voices within the pool perimeter and responding to commands from the authorized voices.

5. The swimming pool monitoring system of claim 1, and including an olfactory sensor coupled to the computer system, the data storage including a database of olfactory signatures associated with authorized objects for comparison to olfactory signatures detected by the olfactory sensor, the computer system providing an alarm in response to unauthorized signatures.

6. The swimming pool monitoring sensor of claim 1, and including a passive infrared sensor system for identifying live objects within the perimeter of the pool.

7. The swimming pool monitoring sensor of claim 6, wherein the ranging sensor comprises an ultrasonic sensor for determining range of a live object from an edge of the pool.

8. The swimming pool monitoring sensor of claim 1, wherein the ranging sensor comprises a geo-position sensor including an ultrasonic range sensor and an image processing module, the image processing module using images of objects from the video camera and distance to the object for creating data points for detecting and identifying live objects within the perimeter of the pool.

9. The swimming pool monitoring sensor of claim 8, wherein the computer system uses the data points to identify orientation and size of live objects within the pool perimeter and compares the identified objects to the stored images of objects to determine the orientation and size of the identified live objects.

10. The swimming pool monitoring sensor of claim 9, wherein the computer system determines the presence of an authorized object in the perimeter of the pool and inhibits the alarm.

11. The swimming pool monitoring system of claim 10, wherein the computer system inhibits the alarm if an authorized live object is in juxtaposition with an unauthorized live object.

12. The swimming pool monitoring system of claim 1, wherein the computer system includes a data input function coupled to the video camera for enabling selected captured images to be stored in the data storage whereby the plurality of predetermined images of

objects may be updated for additional authorized and unauthorized objects.

13. The swimming pool monitoring system of claim 12, wherein the authorized objects comprise living persons and the selected captured images include facial images for enabling facial recognition of authorized and unauthorized persons in the pool perimeter.

14. The swimming pool monitoring system of claim 13, wherein the sensor systems include an auditory sensor for detecting sounds within the perimeter of the pool and the computer system includes voice identification system for identifying authorized and unauthorized voices within the pool perimeter and responding to commands from the authorized voices, the computer system associating the authorized and unauthorized voices with the authorized and unauthorized persons for confirming identity of the authorized person.

15. The swimming pool monitoring system of claim 1, and including local ambient environment condition sensors coupled to the computer system for adjusting system response as a function of ambient conditions.

16. A swimming pool monitoring system having an ultrasonic sensor and a computer system, the sensor providing position and motion detection signals to the computer system, and an alarm system coupled to be activated by the computer system, the computer system activating the alarm upon receiving signals from the sensor indicating an object entering into a predetermined perimeter area around the swimming pool; and

an infrared sensor, a geo-position sensor comprising an ultrasonic range sensor and video detection sensors with a non-transitory computer readable medium storing a program causing the computer system to execute image processing, an auditory sensor and an olfactory sensor, each providing data to the computer system for enabling identification of objects entering into the pool perimeter area.

17. The swimming pool monitoring system of claim 16, wherein the alarm system provides an alarm via at least one of a loud speaker, a text message to a predetermined receiver and an email to a predetermined receiver.

18. The swimming pool monitoring system of claim 17, and including a video sensor coupled to the computer system for providing video images of the object detected by the

ultrasonic sensor, the computer system including a database of authorized and unauthorized objects in the pool perimeter area and being programmed to compare the authorized images to the video images and inhibiting the alarm when the video image is an authorized image.

19. The swimming pool monitoring system of claim 18, wherein the computer system escalates an urgency of the alarm in response to the nearness of the object to an edge of the pool.

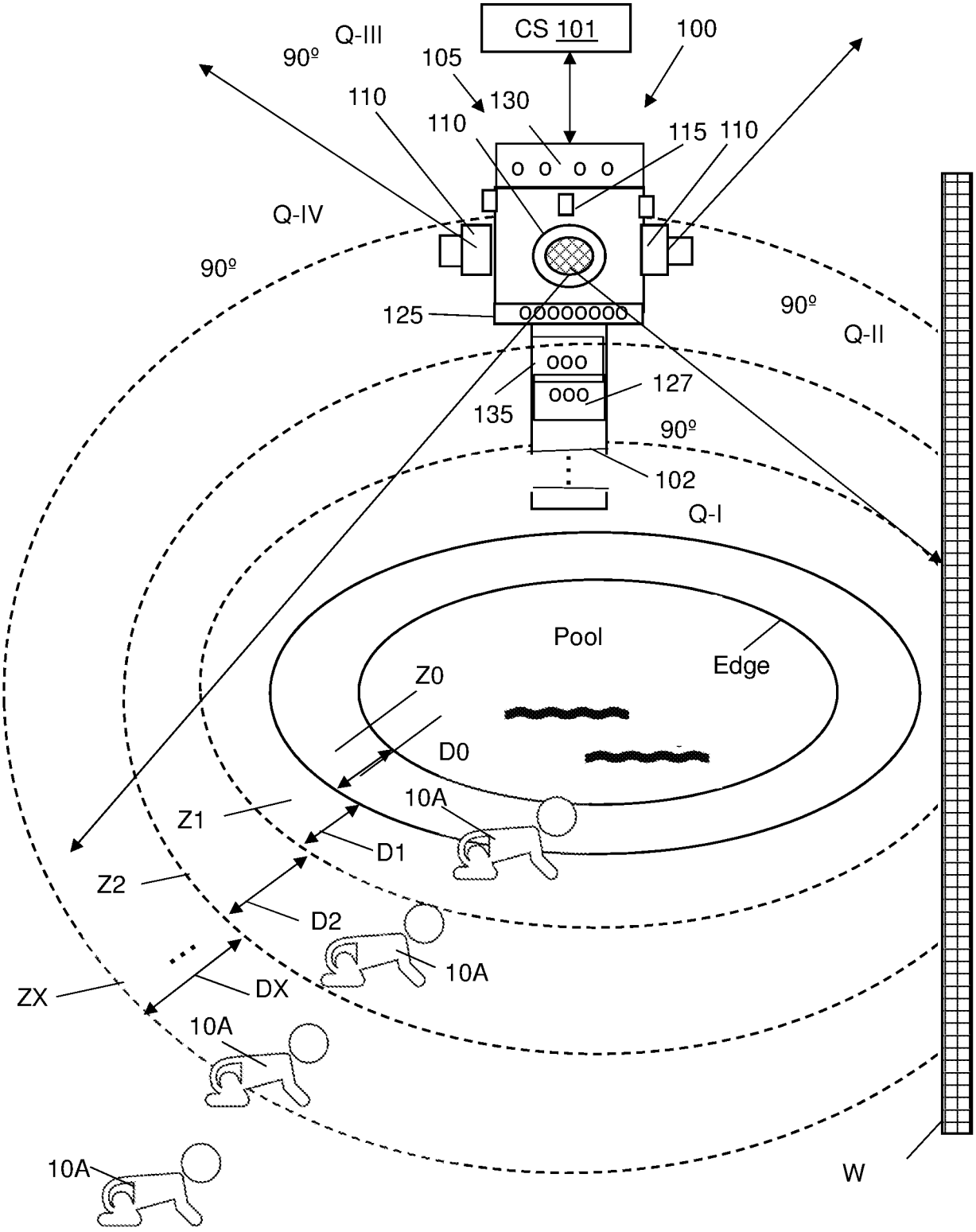

CS 101
100
Q-III
90º
105
110
130
110
115
110
Q-IV
90º
125
90º
Q-II
135
127
90º
102
Q-I
Pool
Edge
Z0
D0
10A
Z1
D1
Z2
D2
10A
ZX
DX
10A
10A
W

FIG. 1A

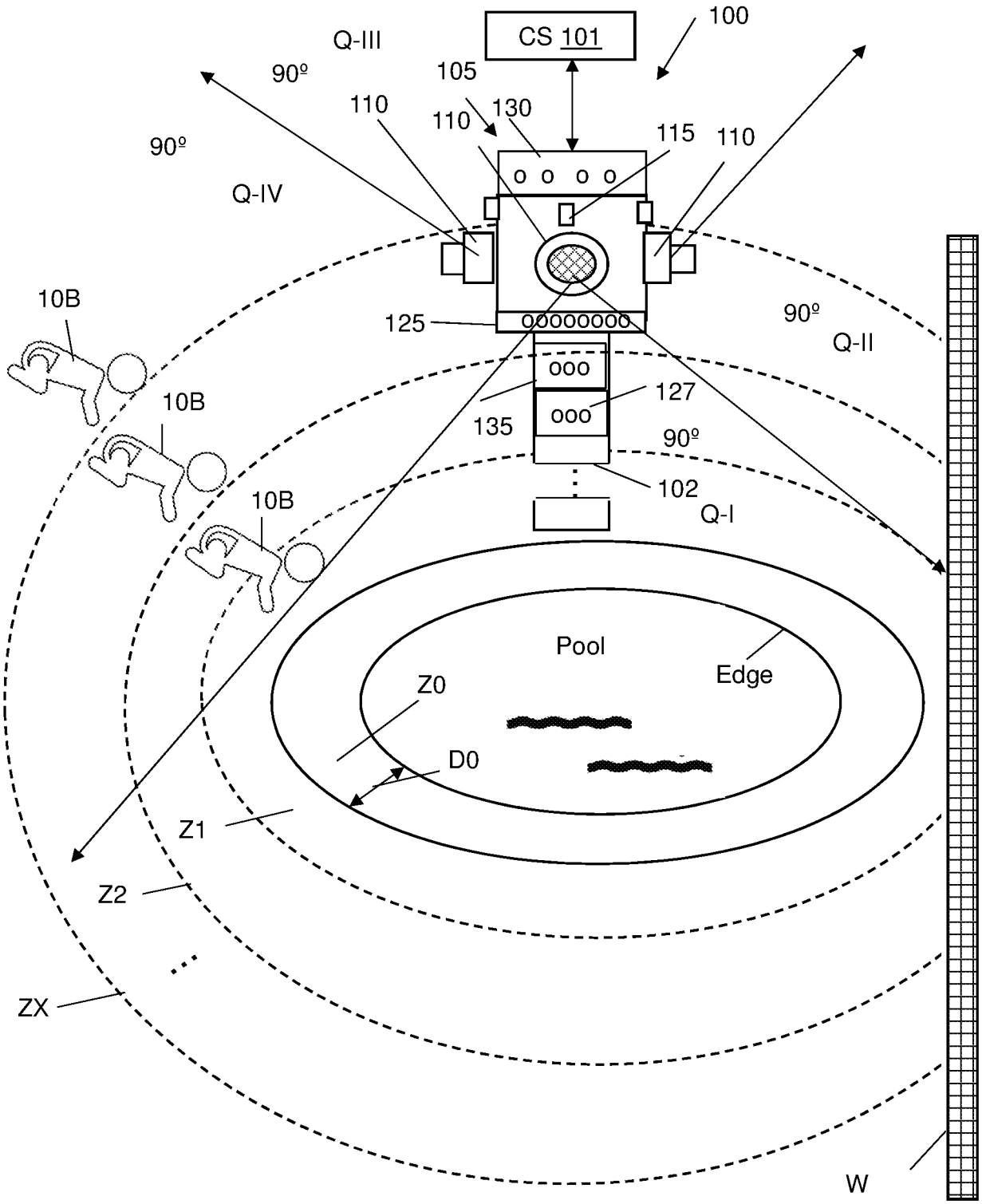

CS 101
100
Q-III
90º
105
110
110
130
115
110
90º
Q-IV
10B
125
90º
Q-II
10B
127
135
90º
10B
102
Q-I
Pool
Edge
Z0
D0
Z1
Z2
ZX
W

FIG. 1B

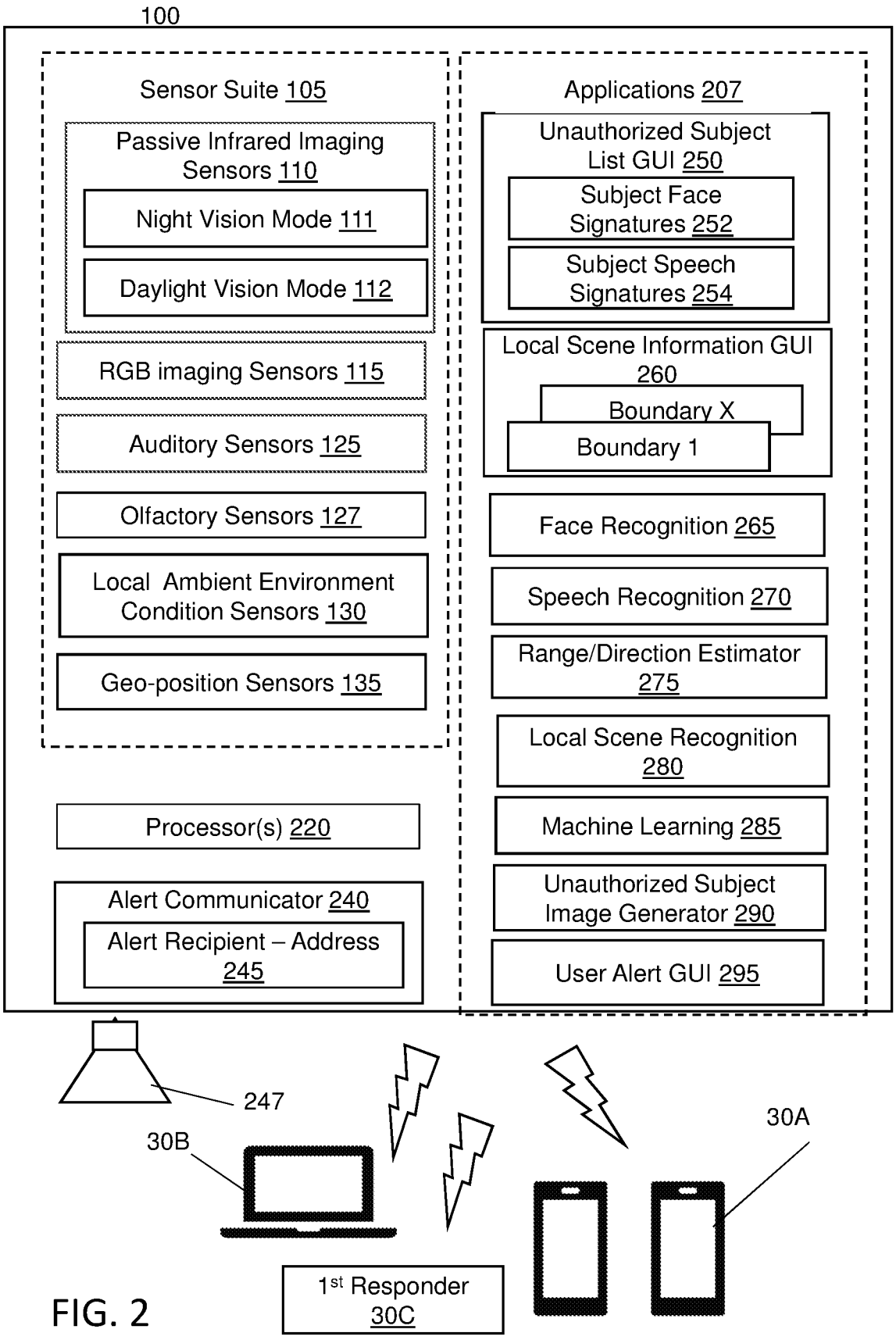

100
Sensor Suite 105
Passive Infrared Imaging Sensors 110
Night Vision Mode 111
Daylight Vision Mode 112
RGB imaging Sensors 115
Auditory Sensors 125
Olfactory Sensors 127
Local Ambient Environment Condition Sensors 130
Geo-position Sensors 135
Processor(s) 220
Alert Communicator 240
Alert Recipient – Address 245
Applications 207
Unauthorized Subject List GUI 250
Subject Face Signatures 252
Subject Speech Signatures 254
Local Scene Information GUI 260
Boundary X
Boundary 1
Face Recognition 265
Speech Recognition 270
Range/Direction Estimator 275
Local Scene Recognition 280
Machine Learning 285
Unauthorized Subject Image Generator 290
User Alert GUI 295
247
30B
30A
1st Responder 30C

FIG. 2

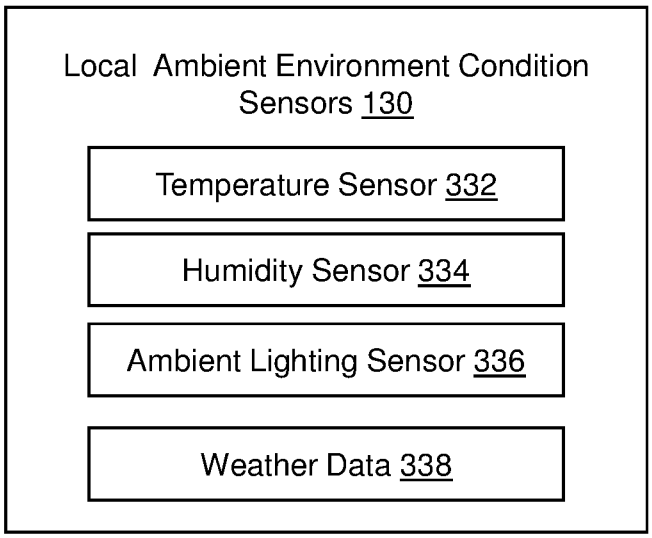

Local Ambient Environment Condition Sensors 130
Temperature Sensor 332
Humidity Sensor 334
Ambient Lighting Sensor 336
Weather Data 338

FIG. 3A

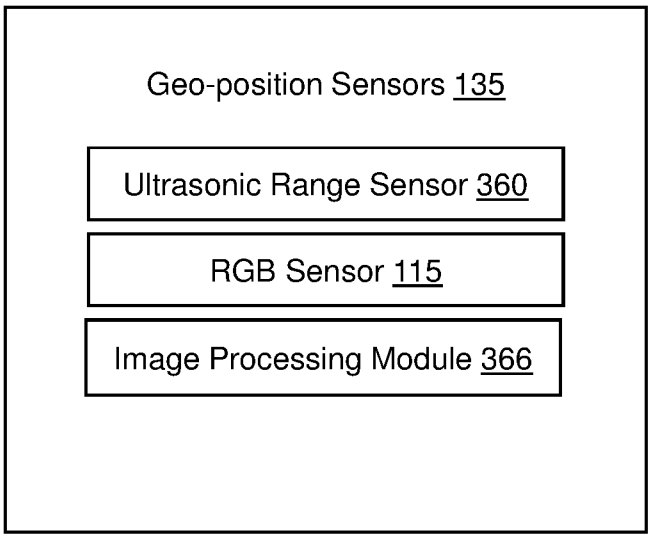

Geo-position Sensors 135
Ultrasonic Range Sensor 360
RGB Sensor 115
Image Processing Module 366

FIG. 3B

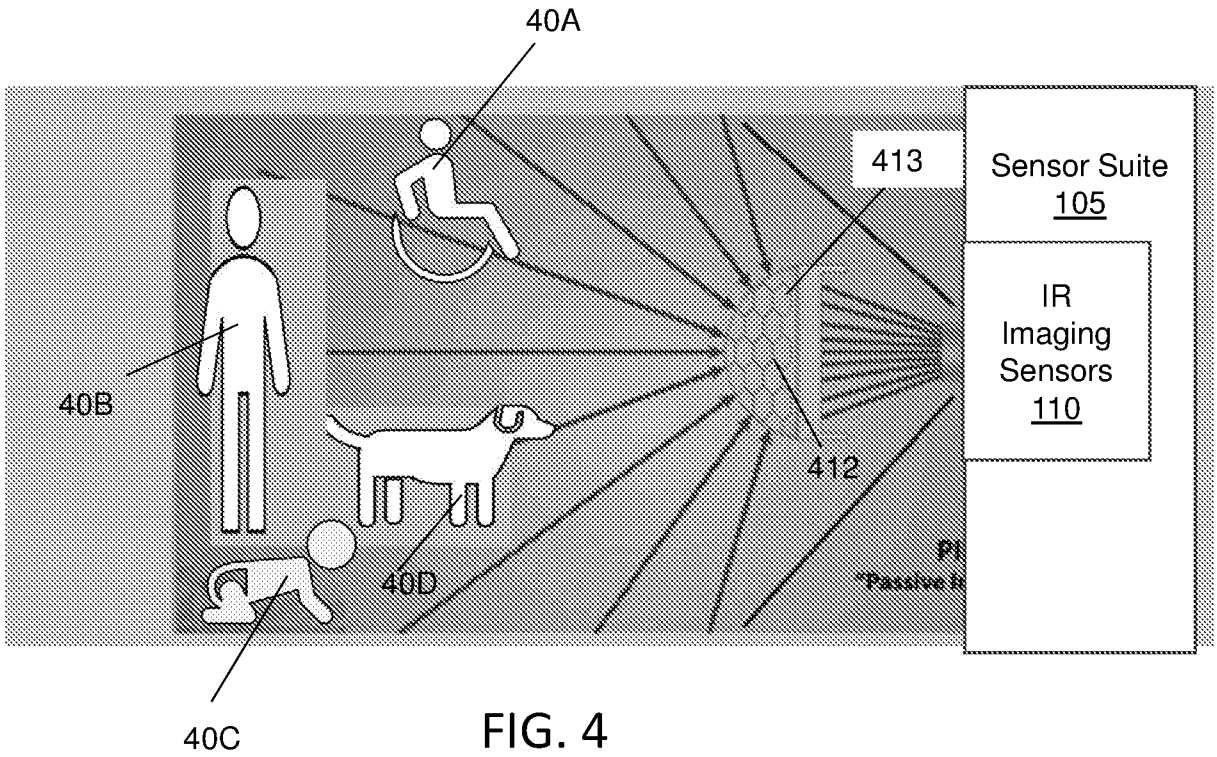

40A
413
Sensor Suite
105
IR
Imaging
Sensors
110
40B
412
40D
40C

FIG. 4

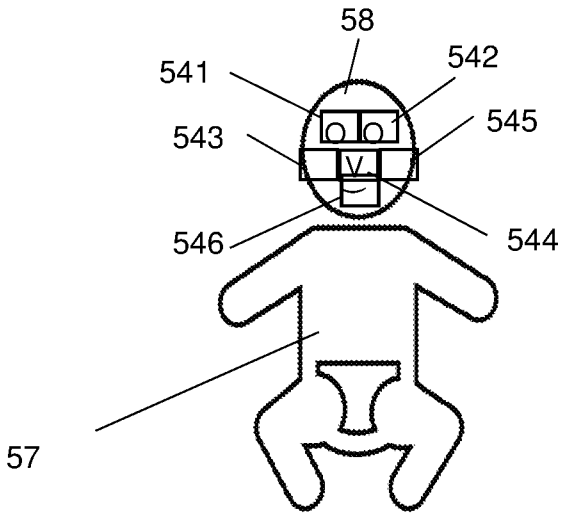
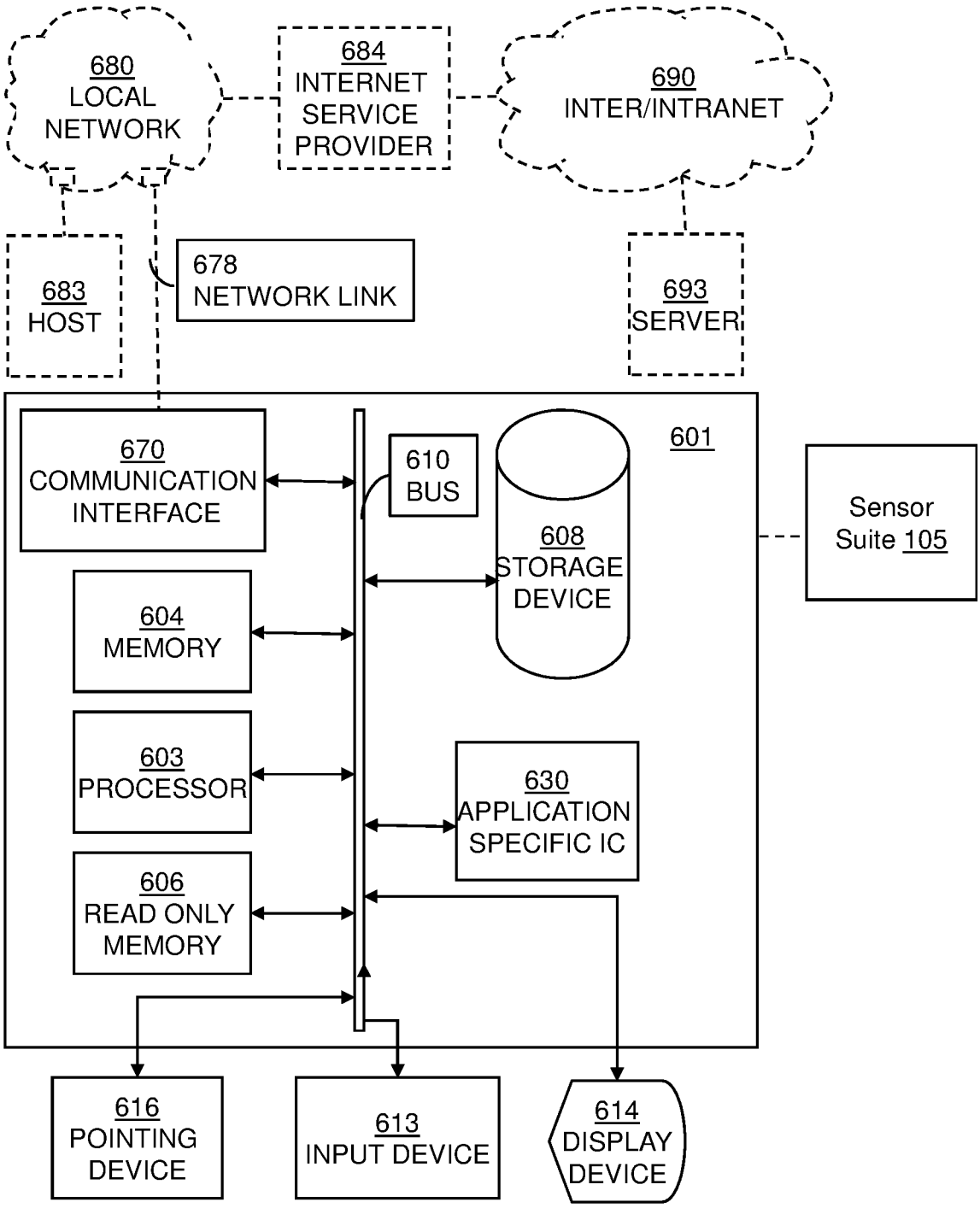

58
541
542
543
545
546
544
57

FIG. 5

FIG. 6


680
LOCAL
NETWORK
684
INTERNET
SERVICE
PROVIDER
690
INTER/INTRANET
683
HOST
678
NETWORK LINK
693
SERVER
601
670
COMMUNICATION
INTERFACE
610
BUS
608
STORAGE
DEVICE
Sensor
Suite 105
604
MEMORY
603
PROCESSOR
630
APPLICATION
SPECIFIC IC
606
READ ONLY
MEMORY
616
POINTING
DEVICE
613
INPUT DEVICE
614
DISPLAY
DEVICE

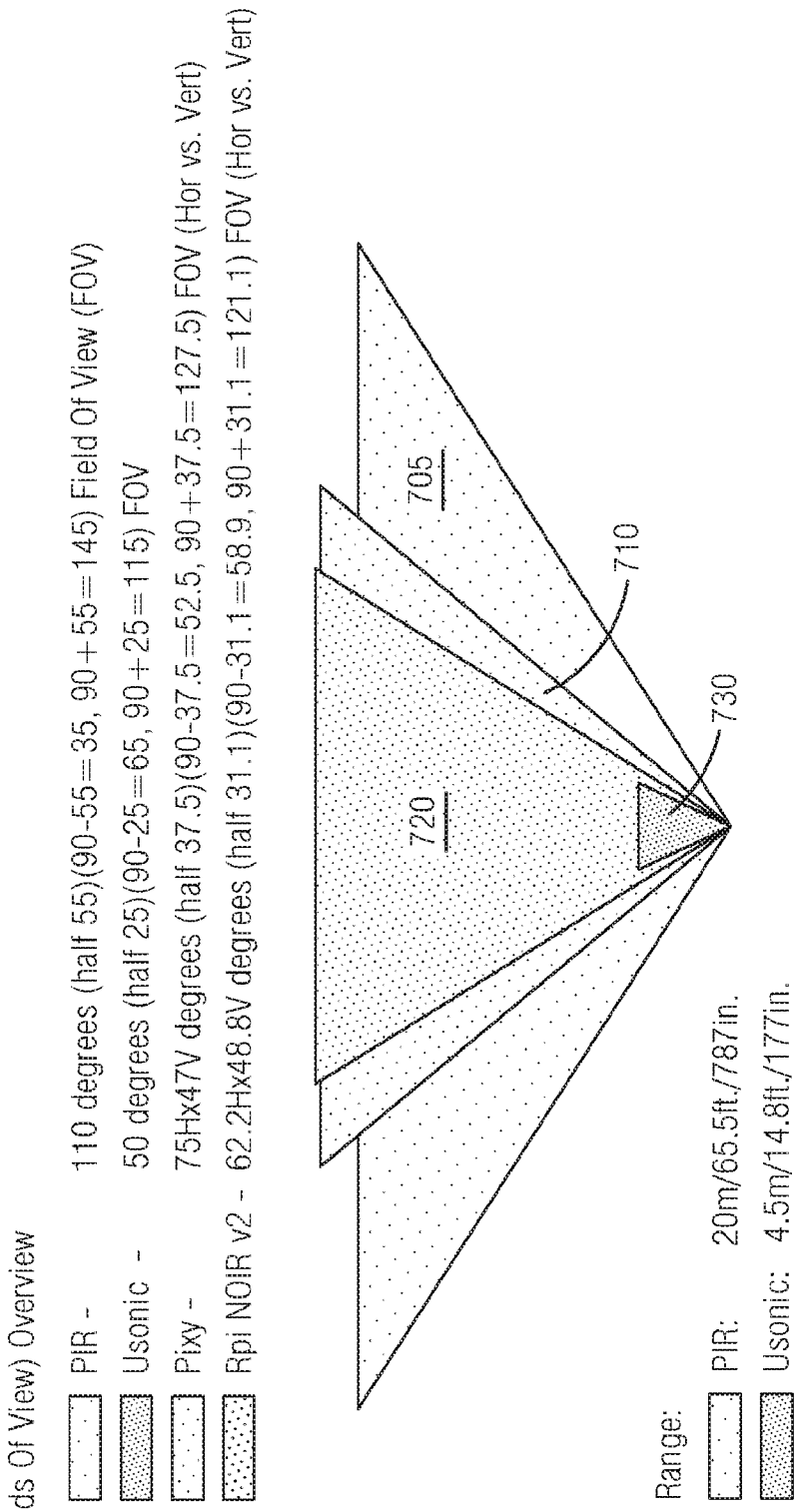

700
FOV (Fields Of View) Overview
PIR - 110 degrees (half 55)(90-55=35, 90+55=145) Field Of View (FOV)
Usonic - 50 degrees (half 25)(90-25=65, 90+25=115) FOV
Pixy - 75Hx47V degrees (half 37.5)(90-37.5=52.5, 90+37.5=127.5) FOV (Hor vs. Vert)
Rpi NOIR v2 - 62.2Hx48.8V degrees (half 31.1)(90-31.1=58.9, 90+31.1=121.1) FOV (Hor vs. Vert)
Range:
PIR: 20m/65.5ft./787in.
Usonic: 4.5m/14.8ft./177in.
705
710
720
730

FIG. 7

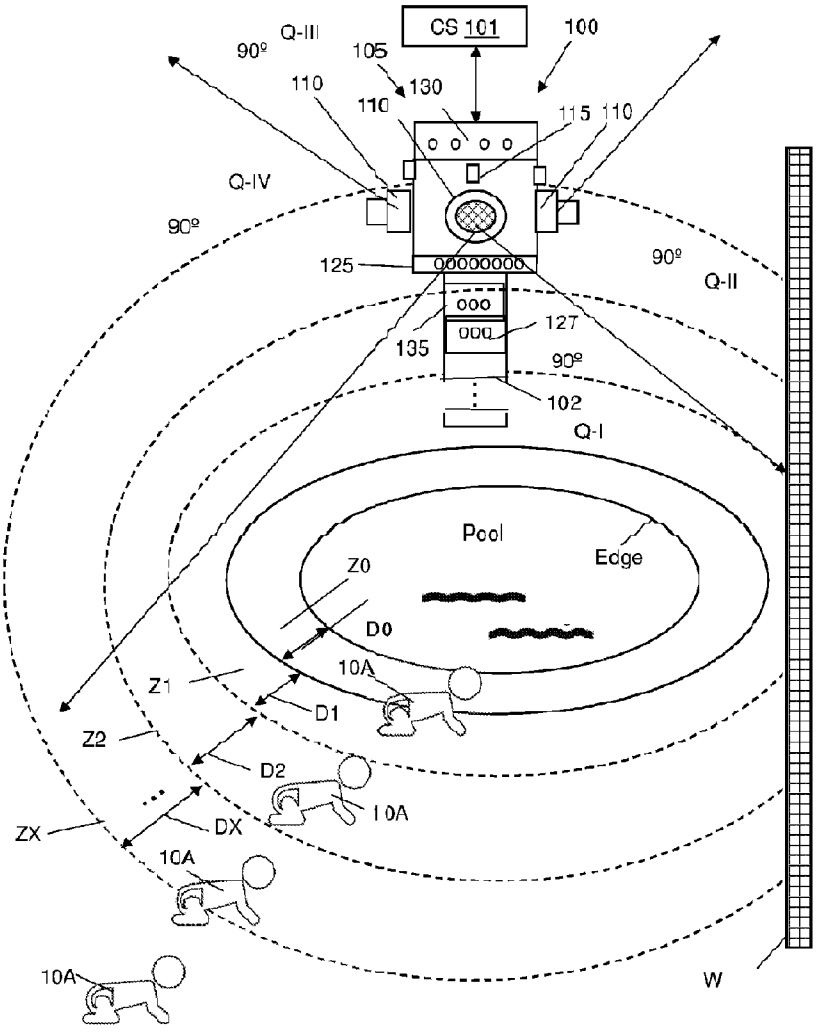

CS 101
100
Q-III
90º
105
110
130
110
115
110
Q-IV
90º
125
90º
Q-II
000
000
127
135
90º
102
Q-I
Pool
Edge
Z0
D0
10A
Z1
D1
Z2
D2
10A
ZX
DX
10A
10A
W

FIG. 1A

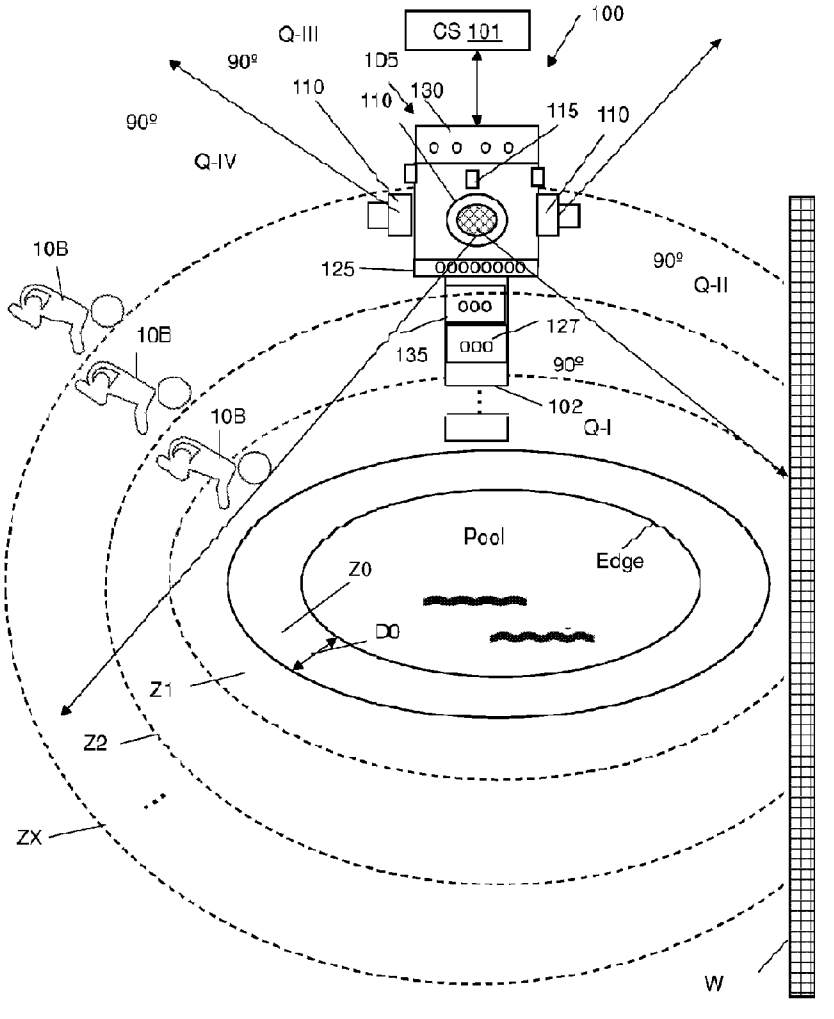

CS 101
100
Q-III
90º
105
110
130
110
115
110
90º
Q-IV
10B
125
90º
Q-II
000
10B
127
135
000
90º
102
10B
Q-I
Pool
Edge
Z0
D0
Z1
Z2
ZX
W

FIG. 1B