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

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
15 February 2018 (15.02.2018)

WIPO | PCT

(10) International Publication Number
WO 2018/031401 A1

(51) International Patent Classification:
H04N 7/18 (2006.01) *H04N 5/77* (2006.01)

(21) International Application Number:
PCT/US2017/045477

(22) International Filing Date:
04 August 2017 (04.08.2017)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
62/374,505 12 August 2016 (12.08.2016) US
62/479,060 30 March 2017 (30.03.2017) US

(71) Applicant: **BOT HOME AUTOMATION, INC.** [US/US]; 1523 26th Street, Santa Monica, CA 90404 (US).

(72) Inventors: **SIMINOFF, James**; 16543 Akron Street, Pacific Palisades, CA 90272 (US). **ROTH, Joshua**; 1250 Villa Woods Drive, Pacific Palisades, CA 90272 (US).

(74) Agent: **CHONG, Eugene, K.**; Chong IP Law, 261 E. Colorado Blvd., Suite 203, Pasadena, CA 91101 (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, SM, ST, SV, SY, TH, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, ZA, ZM, ZW.

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

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

(54) Title: PARCEL THEFT DETERRENCE FOR AUDIO/VIDEO RECORDING AND COMMUNICATION DEVICES

(57) Abstract: Methods for audio/video (A/V) recording and communication devices including a camera, are provided. One such method comprises determining that a parcel has been left within an area about the A/V recording and communication device, determining that the parcel has been removed from the area about the A/V recording and communication device, determining whether removal of the parcel from the area about the A/V recording and communication device was authorized, and when the removal of the parcel from the area about the A/V recording and communication device is determined to have been unauthorized, generating an alert.

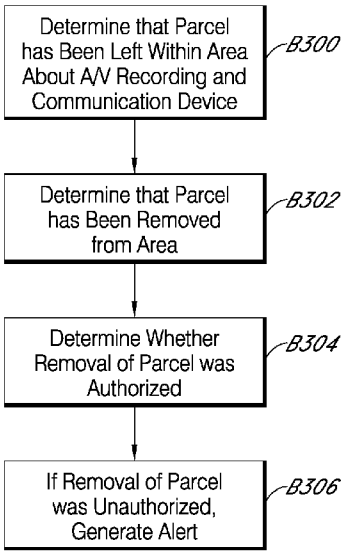

FIG. 14

WO 2018/031401 A1

PARCEL THEFT DETERRENCE FOR AUDIO/VIDEO RECORDING AND COMMUNICATION DEVICES

CROSS-REFERENCE TO RELATED APPLICATIONS

[0001] This application claims priority to provisional application Serial No. 62/479,060, filed on March 30, 2017, and provisional application Serial No. 62/374,505, filed on August 12, 2016. The entire contents of the priority applications are hereby incorporated by reference as if fully set forth.

Technical Field

[0002] The present embodiments relate to audio/video (A/V) recording and communication devices, including A/V recording and communication doorbell systems. In particular, the present embodiments relate to improvements in the functionality of A/V recording and communication devices that strengthen the ability of such devices to deter parcel theft and/or to identify and apprehend parcel thieves.

Background

[0003] Home security is a concern for many homeowners and renters. Those seeking to protect or monitor their homes often wish to have video and audio communications with visitors, for example, those visiting an external door or entryway. Audio/Video (A/V) recording and communication devices, such as doorbells, provide this functionality, and can also aid in crime detection and prevention. For example, audio and/or video captured by an A/V recording and communication device can be uploaded to the cloud and recorded on a remote server. Subsequent review of the A/V footage can aid law enforcement in capturing perpetrators of home burglaries and other crimes. Further, the presence of one or more A/V recording and communication devices on the exterior of a home, such as a doorbell unit at the entrance to the home, acts as a powerful deterrent against would-be burglars.

SUMMARY

[0004] The various embodiments of the present parcel theft deterrence for audio/video (A/V) recording and communication devices have several features, no single one of which is solely responsible for their desirable attributes. Without limiting the scope of the present embodiments as expressed by the claims that follow, their more prominent features now will be discussed briefly. After considering this discussion, and particularly after reading the section

entitled "Detailed Description," one will understand how the features of the present embodiments provide the advantages described herein.

[0005] One aspect of the present embodiments includes the realization that parcel pilferage is a pernicious and persistent problem. Parcel carriers frequently leave parcels near the front door of a home when no one answers the door at the time of delivery. These parcels are vulnerable to theft, as they are often clearly visible from the street. This problem has only gotten worse with the proliferation of online commerce, and is particularly common around major holidays when many consumers do their holiday shopping online. It would be advantageous, therefore, if the functionality of A/V recording and communication devices could be leveraged to deter parcel theft and/or to identify and apprehend parcel thieves. It would also be advantageous if the functionality of A/V recording and communication devices could be enhanced in one or more ways to deter parcel theft and/or to identify and apprehend parcel thieves. The present embodiments provide these advantages and enhancements, as described below.

[0006] In a first aspect, a method for an audio/video (A/V) recording and communication device, the device including a camera, is provided, the method comprising determining that a parcel has been left within an area about the A/V recording and communication device, determining that the parcel has been removed from the area about the A/V recording and communication device, determining whether removal of the parcel from the area about the A/V recording and communication device was authorized, and when the removal of the parcel from the area about the A/V recording and communication device is determined to have been unauthorized, generating an alert.

[0007] In an embodiment of the first aspect, determining that the parcel has been left within the area about the A/V recording and communication device comprises comparing video frames recorded by the camera of the A/V recording and communication device.

[0008] In another embodiment of the first aspect, determining that the parcel has been left in the area about the A/V recording and communication device comprises receiving information from a carrier that delivered the parcel.

[0009] In another embodiment of the first aspect, determining that the parcel has been left within the area about the A/V recording and communication device comprises automatic identification and data capture (AIDC).

[0010] In another embodiment of the first aspect, the AIDC comprises at least one of a barcode, a matrix code, a bokode, and radio frequency identification (RFID).

[0011] In another embodiment of the first aspect, determining that the parcel has been removed from the area about the A/V recording and communication device comprises comparing video frames recorded by the camera of the A/V recording and communication device.

[0012] In another embodiment of the first aspect, determining that the parcel has been removed from the area about the A/V recording and communication device comprises automatic identification and data capture (AIDC).

[0013] In another embodiment of the first aspect, the AIDC comprises radio frequency identification (RFID).

[0014] In another embodiment of the first aspect, determining whether removal of the parcel from the area about the A/V recording and communication device was authorized comprises detecting a direction of movement of the parcel.

[0015] In another embodiment of the first aspect, determining whether removal of the parcel from the area about the A/V recording and communication device was authorized comprises automatic identification and data capture (AIDC).

[0016] In another embodiment of the first aspect, the AIDC comprises at least one of a barcode, a matrix code, a bokode, radio frequency identification (RFID), a smart card, a magnetic stripe, optical character recognition (OCR), biometrics, voice recognition, facial recognition, three-dimensional facial recognition, and skin texture analysis.

[0017] Another embodiment of the first aspect further comprises comparing information received through the AIDC to information about one or more persons.

[0018] In another embodiment of the first aspect, the one or more persons comprise at least one perpetrator of one or more parcel thefts.

[0019] In another embodiment of the first aspect, the one or more parcel thefts occurred within a defined radius about the A/V recording and communication device.

[0020] In another embodiment of the first aspect, the alert comprises an alert signal sent to a client device.

[0021] In another embodiment of the first aspect, the alert comprises an audible alarm emitted from a speaker of the A/V recording and communication device.

[0022] In another embodiment of the first aspect, the alert comprises an announcement emitted from a speaker of the A/V recording and communication device, the announcement comprising a warning that the area about the A/V recording and communication device is being recorded.

[0023] Another embodiment of the first aspect further comprises identifying the parcel.

[0024] In another embodiment of the first aspect, identifying the parcel comprises the camera of the A/V recording and communication device capturing an image of an identifying mark on the parcel.

[0025] In a second aspect, a method for an audio/video (A/V) recording and communication device, the device including a camera, is provided, the method comprising determining that a parcel has been left within an area about the A/V recording and communication device, after the parcel has been left within the area about the A/V recording and communication device, detecting a person within the area about the A/V recording and communication device, recording, with the camera of the A/V recording and communication device, video images of the person within the area about the A/V recording and communication device, and emitting an alert from the speaker of the A/V recording and communication device.

[0026] In an embodiment of the second aspect, the alert comprises an audible alarm.

[0027] In another embodiment of the second aspect, the alert comprises an announcement warning the detected person that he or she is being recorded.

[0028] In a third aspect, a method for an audio/video (A/V) recording and communication device, the device including a camera, is provided, the method comprising determining that a parcel has been left within an area about the A/V recording and communication device, wherein determining that the parcel has been left within the area about the A/V recording and communication device comprises comparing video frames recorded by the camera of the A/V recording and communication device, determining that the parcel has been removed from the area about the A/V recording and communication device, wherein determining that the parcel has been removed from the area about the A/V recording and communication device comprises comparing video frames recorded by the camera of the A/V recording and communication device, determining whether removal of the parcel from the area about the A/V recording and communication device was authorized, wherein determining whether removal of the parcel from the area about the A/V recording and communication device was authorized

comprises automatic identification and data capture (AIDC), and when the removal of the parcel from the area about the A/V recording and communication device is determined to have been unauthorized, generating an alert.

[0029] In an embodiment of the third aspect, the AIDC comprises at least one of radio frequency identification (RFID) and biometrics.

[0030] In another embodiment of the third aspect, the AIDC comprises the camera of the A/V recording and communication device capturing an image of a person in the area about the A/V recording and communication device.

[0031] In another embodiment of the third aspect, the image of the person comprises an image of the person's face.

[0032] Another embodiment of the third aspect further comprises comparing the image of the person to at least one image of at least one other person.

[0033] In another embodiment of the third aspect, the removal of the parcel from the area about the A/V recording and communication device is determined to have been unauthorized when there is a match between the image of the person captured by the camera of the A/V recording and communication device and the at least one image of the at least one other person.

[0034] In a fourth aspect, a method for an audio/video (A/V) recording and communication device, the device including a processor and a camera, the device being communicatively connected to at least one network device, is provided, the method comprising determining that a parcel has been left within an area about the A/V recording and communication device, wherein determining that the parcel has been left within the area about the A/V recording and communication device comprises the processor of the A/V recording and communication device comparing video frames recorded by the camera of the A/V recording and communication device, determining that the parcel has been removed from the area about the A/V recording and communication device, wherein determining that the parcel has been removed from the area about the A/V recording and communication device comprises the processor of the A/V recording and communication device comparing video frames recorded by the camera of the A/V recording and communication device, determining whether removal of the parcel from the area about the A/V recording and communication device was authorized, wherein determining whether removal of the parcel from the area about the A/V recording and communication device was authorized comprises automatic identification and data

capture (AIDC), and when the removal of the parcel from the area about the A/V recording and communication device is determined to have been unauthorized, generating an alert.

[0035] In an embodiment of the fourth aspect, the AIDC comprises at least one of radio frequency identification (RFID) and biometrics.

[0036] In another embodiment of the fourth aspect, the AIDC comprises the camera of the A/V recording and communication device capturing an image of a person in the area about the A/V recording and communication device.

[0037] In another embodiment of the fourth aspect, the image of the person comprises an image of the person's face.

[0038] Another embodiment of the fourth aspect further comprises the at least one network device receiving the image of the person.

[0039] Another embodiment of the fourth aspect further comprises the at least one network device comparing the image of the person to at least one image of at least one other person.

[0040] In another embodiment of the fourth aspect, the removal of the parcel from the area about the A/V recording and communication device is determined to have been unauthorized when there is a match between the image of the person captured by the camera of the A/V recording and communication device and the at least one image of the at least one other person.

BRIEF DESCRIPTION OF THE DRAWINGS

[0041] The various embodiments of the present parcel theft deterrence for audio/video (A/V) recording and communication devices now will be discussed in detail with an emphasis on highlighting the advantageous features. These embodiments depict the novel and non-obvious parcel theft deterrence for A/V recording and communication devices shown in the accompanying drawings, which are for illustrative purposes only. These drawings include the following figures, in which like numerals indicate like parts:

[0042] Figure 1 is a functional block diagram illustrating a system for streaming and storing A/V content captured by an audio/video (A/V) recording and communication device according to various aspects of the present disclosure;

[0043] Figure 2 is a flowchart illustrating a process for streaming and storing A/V content from an A/V recording and communication device according to various aspects of the present disclosure;

[0044] Figure 3 is a functional block diagram illustrating an embodiment of an A/V recording and communication device according to the present disclosure;

[0045] Figure 4 is a front perspective view of an embodiment of an A/V recording and communication device according to the present disclosure;

[0046] Figure 5 is a rear perspective view of the A/V recording and communication device of Figure 4;

[0047] Figure 6 is a partially exploded front perspective view of the A/V recording and communication device of Figure 4 showing the cover removed;

[0048] Figures 7-9 are front perspective views of various internal components of the A/V recording and communication device of Figure 4;

[0049] Figure 10 is a right-side cross-sectional view of the A/V recording and communication device of Figure 4 taken through the line 10-10 in Figure 4;

[0050] Figures 11-13 are rear perspective views of various internal components of the A/V recording and communication device of Figure 4;

[0051] Figure 14 is a flowchart illustrating an embodiment of a process for deterring parcel theft with an A/V recording and communication device according to various aspects of the present disclosure;

[0052] Figure 15 is a sequence diagram illustrating an embodiment of a process for deterring parcel theft with an A/V recording and communication device according to various aspects of the present disclosure;

[0053] Figure 16 is a front elevation view of a barcode;

[0054] Figure 17 is a front elevation view of a matrix code;

[0055] Figure 18 is a front elevation view of a bokode;

[0056] Figure 19 is a front elevation view of a radio frequency identification (RFID) tag;

[0057] Figure 20 is a sequence diagram illustrating an embodiment of a process for deterring parcel theft with an A/V recording and communication device according to various aspects of the present disclosure;

[0058] Figure 21 is a front elevation view of a smart card;

[0059] Figure 22 is a rear elevation view of a magnetic stripe card;

[0060] Figure 23 is a flowchart illustrating an embodiment of a process for deterring parcel theft with an A/V recording and communication device according to various aspects of the present disclosure;

[0061] Figure 24 is a flowchart illustrating another embodiment of a process for deterring parcel theft with an A/V recording and communication device according to various aspects of the present disclosure;

[0062] Figure 25 is a functional block diagram of a client device on which the present embodiments may be implemented according to various aspects of the present disclosure; and

[0063] Figure 26 is a functional block diagram of a general-purpose computing system on which the present embodiments may be implemented according to various aspects of present disclosure.

DETAILED DESCRIPTION

[0064] The following detailed description describes the present embodiments with reference to the drawings. In the drawings, reference numbers label elements of the present embodiments. These reference numbers are reproduced below in connection with the discussion of the corresponding drawing features.

[0065] The embodiments of the present parcel theft deterrence for audio/video (A/V) recording and communication devices are described below with reference to the figures. These figures, and their written descriptions, indicate that certain components of the apparatus are formed integrally, and certain other components are formed as separate pieces. Those of ordinary skill in the art will appreciate that components shown and described herein as being formed integrally may in alternative embodiments be formed as separate pieces. Those of ordinary skill in the art will further appreciate that components shown and described herein as being formed as separate pieces may in alternative embodiments be formed integrally. Further, as used herein the term integral describes a single unitary piece.

[0066] With reference to Figure 1, the present embodiments include an audio/video (A/V) device 100 (e.g., a doorbell or a security camera). While the present disclosure provides numerous examples of methods and systems including A/V recording and communication doorbells, the present embodiments are equally applicable for A/V recording and communication

devices other than doorbells. For example, the present embodiments may include one or more A/V recording and communication security cameras instead of, or in addition to, one or more A/V recording and communication doorbells. An example A/V recording and communication security camera may include substantially all of the structure and functionality of the doorbells described herein, but without the front button and related components.

[0067] The A/V recording and communication device 100 is typically located near the entrance to a structure (not shown), such as a dwelling, a business, a storage facility, etc. The A/V recording and communication device 100 includes a camera 102, a microphone 104, and a speaker 106. The camera 102 may comprise, for example, a high definition (HD) video camera, such as one capable of capturing video images at an image display resolution of 1080p or better. While not shown, the A/V recording and communication device 100 may also include other hardware and/or components, such as a housing, one or more motion sensors (and/or other types of sensors), a button, etc. The A/V recording and communication device 100 may further include similar componentry and/or functionality as the wireless communication doorbells described in US Patent Application Publication Nos. 2015/0022620 (Application Serial No. 14/499,828) and 2015/0022618 (Application Serial No. 14/334,922), both of which are incorporated herein by reference in their entireties as if fully set forth.

[0068] With further reference to Figure 1, the A/V recording and communication device 100 communicates with a user's network 110, which may be for example a wired and/or wireless network. If the user's network 110 is wireless, or includes a wireless component, the network 110 may be a Wi-Fi network compatible with the IEEE 802.11 standard and/or other wireless communication standard(s). The user's network 110 is connected to another network 112, which may comprise, for example, the Internet and/or a public switched telephone network (PSTN). As described below, the A/V recording and communication device 100 may communicate with the user's client device 114 via the network 110 and the network 112 (Internet/PSTN). The user's client device 114 may comprise, for example, a mobile telephone (may also be referred to as a cellular telephone), such as a smartphone, a personal digital assistant (PDA), or another communication device. The user's client device 114 comprises a display (not shown) and related components capable of displaying streaming and/or recorded video images. The user's client device 114 may also comprise a speaker and related components capable of broadcasting streaming and/or recorded audio, and may also comprise a microphone. The A/V recording and

communication device 100 may also communicate with one or more remote storage device(s) 116 (may be referred to interchangeably as "cloud storage device(s)"), one or more servers 118, and/or a backend API (application programming interface)120 via the network 110 and the network 112 (Internet/PSTN). While Figure 1 illustrates the storage device 116, the server 118, and the backend API 120 as components separate from the network 112, it is to be understood that the storage device 116, the server 118, and/or the backend API 120 may be considered to be components of the network 112.

[0069] The network 112 may be any wireless network or any wired network, or a combination thereof, configured to operatively couple the above-mentioned modules, devices, and systems as shown in Figure 1. For example, the network 112 may include one or more of the following: a PSTN (public switched telephone network), the Internet, a local intranet, a PAN (Personal Area Network), a LAN (Local Area Network), a WAN (Wide Area Network), a MAN (Metropolitan Area Network), a virtual private network (VPN), a storage area network (SAN), a frame relay connection, an Advanced Intelligent Network (AIN) connection, a synchronous optical network (SONET) connection, a digital T1, T3, E1 or E3 line, a Digital Data Service (DDS) connection, a DSL (Digital Subscriber Line) connection, an Ethernet connection, an ISDN (Integrated Services Digital Network) line, a dial-up port such as a V.90, V.34, or V.34bis analog modem connection, a cable modem, an ATM (Asynchronous Transfer Mode) connection, or an FDDI (Fiber Distributed Data Interface) or CDDI (Copper Distributed Data Interface) connection. Furthermore, communications may also include links to any of a variety of wireless networks, including WAP (Wireless Application Protocol), GPRS (General Packet Radio Service), GSM (Global System for Mobile Communication), LTE, VoLTE, LoRaWAN, LPWAN, RPMA, LTE Cat-"X" (e.g. LTE Cat 1, LTE Cat 0, LTE CatM1, LTE Cat NB1), CDMA (Code Division Multiple Access), TDMA (Time Division Multiple Access), FDMA (Frequency Division Multiple Access), and/or OFDMA (Orthogonal Frequency Division Multiple Access) cellular phone networks, GPS, CDPD (cellular digital packet data), RIM (Research in Motion, Limited) duplex paging network, Bluetooth radio, or an IEEE 802.11-based radio frequency network. The network can further include or interface with any one or more of the following: RS-232 serial connection, IEEE-1394 (Firewire) connection, Fibre Channel connection, IrDA (infrared) port, SCSI (Small Computer Systems Interface) connection, USB

(Universal Serial Bus) connection, or other wired or wireless, digital or analog, interface or connection, mesh or Digi® networking.

[0070] According to one or more aspects of the present embodiments, when a person (may be referred to interchangeably as "visitor") arrives at the A/V recording and communication device 100, the A/V recording and communication device 100 detects the visitor's presence and begins capturing video images within a field of view of the camera 102. The A/V communication device 100 may also capture audio through the microphone 104. The A/V recording and communication device 100 may detect the visitor's presence using a motion sensor, and/or by detecting that the visitor has depressed the button on the A/V recording and communication device 100.

[0071] In response to the detection of the visitor, the A/V recording and communication device 100 sends an alert to the user's client device 114 (Figure 1) via the user's network 110 and the network 112. The A/V recording and communication device 100 also sends streaming video, and may also send streaming audio, to the user's client device 114. If the user answers the alert, two-way audio communication may then occur between the visitor and the user through the A/V recording and communication device 100 and the user's client device 114. The user may view the visitor throughout the duration of the call, but the visitor cannot see the user (unless the A/V recording and communication device 100 includes a display, which it may in some embodiments).

[0072] The video images captured by the camera 102 of the A/V recording and communication device 100 (and the audio captured by the microphone 104) may be uploaded to the cloud and recorded on the remote storage device 116 (Figure 1). In some embodiments, the video and/or audio may be recorded on the remote storage device 116 even if the user chooses to ignore the alert sent to his or her client device 114.

[0073] With further reference to Figure 1, the system may further comprise a backend API 120 including one or more components. A backend API (application programming interface) may comprise, for example, a server (e.g. a real server, or a virtual machine, or a machine running in a cloud infrastructure as a service), or multiple servers networked together, exposing at least one API to client(s) accessing it. These servers may include components such as application servers (e.g. software servers), depending upon what other components are included, such as a caching layer, or database layers, or other components. A backend API may,

for example, comprise many such applications, each of which communicate with one another using their public APIs. In some embodiments, the API backend may hold the bulk of the user data and offer the user management capabilities, leaving the clients to have very limited state.

[0074] The backend API 120 illustrated Figure 1 may include one or more APIs. An API is a set of routines, protocols, and tools for building software and applications. An API expresses a software component in terms of its operations, inputs, outputs, and underlying types, defining functionalities that are independent of their respective implementations, which allows definitions and implementations to vary without compromising the interface. Advantageously, an API may provide a programmer with access to an application's functionality without the programmer needing to modify the application itself, or even understand how the application works. An API may be for a web-based system, an operating system, or a database system, and it provides facilities to develop applications for that system using a given programming language. In addition to accessing databases or computer hardware like hard disk drives or video cards, an API can ease the work of programming GUI components. For example, an API can facilitate integration of new features into existing applications (a so-called "plug-in API"). An API can also assist otherwise distinct applications with sharing data, which can help to integrate and enhance the functionalities of the applications.

[0075] The backend API 120 illustrated in Figure 1 may further include one or more services (also referred to as network services). A network service is an application that provides data storage, manipulation, presentation, communication, and/or other capability. Network services are often implemented using a client-server architecture based on application-layer network protocols. Each service may be provided by a server component running on one or more computers (such as a dedicated server computer offering multiple services) and accessed via a network by client components running on other devices. However, the client and server components can both be run on the same machine. Clients and servers may have a user interface, and sometimes other hardware associated with them.

[0076] Figure 2 is a flowchart illustrating a process for streaming and storing A/V content from the A/V recording and communication device 100 according to various aspects of the present disclosure. At block B260, the A/V recording and communication device 100 (e.g., an A/V recording and communication device, such as a doorbell) detects the visitor's presence and captures video images within a field of view of the camera 102. The A/V recording and

communication device 100 may also capture audio through the microphone 104. As described above, the A/V recording and communication device 100 may detect the visitor's presence by detecting motion using the camera 102 and/or a motion sensor, and/or by detecting that the visitor has pressed a front button of the A/V recording and communication device 100 (if the A/V recording and communication device 100 is a doorbell). Also, as described above, the video recording/capture may begin when the visitor is detected, or may begin earlier, as described below.

[0077] At block B262, a communication module of the A/V recording and communication device 100 sends a request, via the user's network 110 and the network 112, to a device in the network 112. For example, the network device to which the request is sent may be a server such as the server 118. The server 118 may comprise a computer program and/or a machine that waits for requests from other machines or software (clients) and responds to them. A server typically processes data. One purpose of a server is to share data and/or hardware and/or software resources among clients. This architecture is called the client-server model. The clients may run on the same computer or may connect to the server over a network. Examples of computing servers include database servers, file servers, mail servers, print servers, web servers, game servers, and application servers. The term server may be construed broadly to include any computerized process that shares a resource to one or more client processes. In another example, the network device to which the request is sent may be an API such as the backend API 120, which is described above.

[0078] In response to the request, at block B264 the network device may connect the A/V recording and communication device 100 to the user's client device 114 through the user's network 110 and the network 112. At block B266, the A/V recording and communication device 100 may record available audio and/or video data using the camera 102, the microphone 104, and/or any other device/sensor available. At block B268, the audio and/or video data is transmitted (streamed) from the A/V recording and communication device 100 to the user's client device 114 via the user's network 110 and the network 112. At block B270, the user may receive a notification on his or her client device 114 with a prompt to either accept or deny the call.

[0079] At block B272, the process determines whether the user has accepted or denied the call. If the user denies the notification, then the process advances to block B274, where the

audio and/or video data is recorded and stored at a cloud server. The session then ends at block B276 and the connection between the A/V recording and communication device 100 and the user's client device 114 is terminated. If, however, the user accepts the notification, then at block B278 the user communicates with the visitor through the user's client device 114 while audio and/or video data captured by the camera 102, the microphone 104, and/or other devices/sensors is streamed to the user's client device 114. At the end of the call, the user may terminate the connection between the user's client device 114 and the A/V recording and communication device 100 and the session ends at block B276. In some embodiments, the audio and/or video data may be recorded and stored at a cloud server (block B274) even if the user accepts the notification and communicates with the visitor through the user's client device 114.

[0080] Figures 3-13 illustrate one embodiment of a low-power-consumption A/V recording and communication device 130 according to various aspects of the present disclosure. Figure 3 is a functional block diagram illustrating various components of the A/V recording and communication device 130 and their relationships to one another. For example, the A/V recording and communication device 130 includes a pair of terminals 131, 132 configured to be connected to a source of external AC (alternating-current) power, such as a household AC power supply 134 (may also be referred to as AC mains). The AC power 134 may have a voltage in the range of 16-24 VAC, for example. The incoming AC power 134 may be converted to DC (direct-current) by an AC/DC rectifier 136. An output of the AC/DC rectifier 136 may be connected to an input of a DC/DC converter 138, which may step down the voltage from the output of the AC/DC rectifier 136 from 16-24 VDC to a lower voltage of about 5 VDC, for example. In various embodiments, the output of the DC/DC converter 138 may be in a range of from about 2.5 V to about 7.5 V, for example.

[0081] With further reference to Figure 3, the output of the DC/DC converter 138 is connected to a power manager 140, which may comprise an integrated circuit including a processor core, memory, and/or programmable input/output peripherals. In one non-limiting example, the power manager 140 may be an off-the-shelf component, such as the BQ24773 chip manufactured by Texas Instruments. As described in detail below, the power manager 140 controls, among other things, an amount of power drawn from the external power supply 134, as well as an amount of supplemental power drawn from a battery 142, to power the A/V recording and communication device 130. The power manager 140 may, for example, limit the amount of

power drawn from the external power supply 134 so that a threshold power draw is not exceeded. In one non-limiting example, the threshold power, as measured at the output of the DC/DC converter 138, may be equal to 1.4 A. The power manager 140 may also control an amount of power drawn from the external power supply 134 and directed to the battery 142 for recharging of the battery 142. An output of the power manager 140 is connected to a power sequencer 144, which controls a sequence of power delivery to other components of the A/V recording and communication device 130, including a communication module 146, a front button 148, a microphone 150, a speaker driver 151, a speaker 152, an audio CODEC (Coder-DECoder) 153, a camera 154, an infrared (IR) light source 156, an IR cut filter 158, a processor 160 (may also be referred to as a controller 160), a plurality of light indicators 162, and a controller 164 for the light indicators 162. Each of these components is described in detail below. The power sequencer 144 may comprise an integrated circuit including a processor core, memory, and/or programmable input/output peripherals. In one non-limiting example, the power sequencer 144 may be an off-the-shelf component, such as the RT5024 chip manufactured by Richtek.

[0082] With further reference to Figure 3, the A/V recording and communication device 130 further comprises an electronic switch 166 that closes when the front button 148 is depressed. When the electronic switch 166 closes, power from the AC power source 134 is diverted through a signaling device 168 that is external to the A/V recording and communication device 130 to cause the signaling device 168 to emit a sound, as further described below. In one non-limiting example, the electronic switch 166 may be a triac device. The A/V recording and communication device 130 further comprises a reset button 170 configured to initiate a hard reset of the processor 160, as further described below.

[0083] With further reference to Figure 3, the processor 160 may perform data processing and various other functions, as described below. The processor 160 may comprise an integrated circuit including a processor core, memory 172, non-volatile memory 174, and/or programmable input/output peripherals (not shown). The memory 172 may comprise, for example, DDR3 (double data rate type three synchronous dynamic random-access memory). The non-volatile memory 174 may comprise, for example, NAND flash memory. In the embodiment illustrated in Figure 3, the memory 172 and the non-volatile memory 174 are illustrated within the box representing the processor 160. It is to be understood that the embodiment illustrated in Figure 3 is merely an example, and in some embodiments the memory

172 and/or the non-volatile memory 174 are not necessarily physically incorporated with the processor 160. The memory 172 and/or the non-volatile memory 174, regardless of their physical location, may be shared by one or more other components (in addition to the processor 160) of the present A/V recording and communication device 130.

[0084] The transfer of digital audio between the user and a visitor may be compressed and decompressed using the audio CODEC 153, which is operatively coupled to the processor 160. When the visitor speaks, audio from the visitor is compressed by the audio CODEC 153, digital audio data is sent through the communication module 146 to the network 112 via the user's network 110, routed by the server 118 and delivered to the user's client device 114. When the user speaks, after being transferred through the network 112, the user's network 110, and the communication module 146, the digital audio data is decompressed by the audio CODEC 153 and emitted to the visitor through the speaker 152, which is driven by the speaker driver 151.

[0085] With further reference to Figure 3, some of the present embodiments may include a shunt 176 connected in parallel with the signaling device 168. The shunt 176 facilitates the ability of the A/V recording and communication device 130 to draw power from the AC power source 134 without inadvertently triggering the signaling device 168. The shunt 176, during normal standby operation, presents a relatively low electrical impedance, such as a few ohms, across the terminals of the signaling device 168. Most of the current drawn by the A/V recording and communication device 130, therefore, flows through the shunt 176, and not through the signaling device 168. The shunt 176, however, contains electronic circuitry (described below) that switches the shunt 176 between a state of low impedance, such as a few ohms, for example, and a state of high impedance, such as > 1K ohms, for example. When the front button 148 of the A/V recording and communication device 130 is pressed, the electronic switch 166 closes, causing the voltage from the AC power source 134 to be impressed mostly across the shunt 176 and the signaling device 168 in parallel, while a small amount of voltage, such as about 1V, is impressed across the electronic switch 166. The circuitry in the shunt 176 senses this voltage, and switches the shunt 176 to the high impedance state, so that power from the AC power source 134 is diverted through the signaling device 168. The diverted AC power 134 is above the threshold necessary to cause the signaling device 168 to emit a sound. Pressing the front button 148 of the device 130 therefore causes the signaling device 168 to "ring," alerting any person(s) within the structure to which the device 130 is mounted that there is a visitor at the front door (or

at another location corresponding to the location of the device 130). In one non-limiting example, the electronic switch 166 may be a triac device.

[0086] With reference to Figures 4-6, the A/V recording and communication device 130 further comprises a housing 178 having an enclosure 180 (Figure 6), a back plate 182 secured to the rear of the enclosure 180, and a shell 184 overlying the enclosure 180. With reference to Figure 6, the shell 184 includes a recess 186 that is sized and shaped to receive the enclosure 180 in a close fitting engagement, such that outer surfaces of the enclosure 180 abut conforming inner surfaces of the shell 184. Exterior dimensions of the enclosure 180 may be closely matched with interior dimensions of the shell 184 such that friction maintains the shell 184 about the enclosure 180. Alternatively, or in addition, the enclosure 180 and/or the shell 184 may include mating features 188, such as one or more tabs, grooves, slots, posts, etc. to assist in maintaining the shell 184 about the enclosure 180. The back plate 182 is sized and shaped such that the edges of the back plate 182 extend outward from the edges of the enclosure 180, thereby creating a lip 190 against which the shell 184 abuts when the shell 184 is mated with the enclosure 180, as shown in Figures 4 and 5. In some embodiments, multiple shells 184 in different colors may be provided so that the end user may customize the appearance of his or her A/V recording and communication device 130. For example, the A/V recording and communication device 130 may be packaged and sold with multiple shells 184 in different colors in the same package.

[0087] With reference to Figure 4, a front surface of the A/V recording and communication device 130 includes the button 148 (may also be referred to as front button 148, Figure 3), which is operatively connected to the processor 160. In a process similar to that described above with reference to Figure 2, when a visitor presses the front button 148, an alert may be sent to the user's client device to notify the user that someone is at his or her front door (or at another location corresponding to the location of the A/V recording and communication device 130). With further reference to Figure 4, the A/V recording and communication device 130 further includes the camera 154, which is operatively connected to the processor 160, and which is located behind a shield 192. As described in detail below, the camera 154 is configured to capture video images from within its field of view. Those video images can be streamed to the user's client device and/or uploaded to a remote network device for later viewing according to a process similar to that described above with reference to Figure 2.

[0088] With reference to Figure 5, a pair of terminal screws 194 extends through the back plate 182. The terminal screws 194 are connected at their inner ends to the terminals 131, 132 (Figure 3) within the A/V recording and communication device 130. The terminal screws 194 are configured to receive electrical wires to connect to the A/V recording and communication device 130, through the terminals 131, 132, to the household AC power supply 134 of the structure on which the A/V recording and communication device 130 is mounted. In the illustrated embodiment, the terminal screws 194 are located within a recessed portion 196 of the rear surface 198 of the back plate 182 so that the terminal screws 194 do not protrude from the outer envelope of the A/V recording and communication device 130. The A/V recording and communication device 130 can thus be mounted to a mounting surface with the rear surface 198 of the back plate 182 abutting the mounting surface. The back plate 182 includes apertures 200 adjacent its upper and lower edges to accommodate mounting hardware, such as screws (not shown), for securing the back plate 182 (and thus the A/V recording and communication device 130) to the mounting surface. With reference to Figure 6, the enclosure 180 includes corresponding apertures 202 adjacent its upper and lower edges that align with the apertures 200 in the back plate 182 to accommodate the mounting hardware. In certain embodiments, the A/V recording and communication device 130 may include a mounting plate or bracket (not shown) to facilitate securing the A/V recording and communication device 130 to the mounting surface.

[0089] With further reference to Figure 6, the shell 184 includes a central opening 204 in a front surface. The central opening 204 is sized and shaped to accommodate the shield 192. In the illustrated embodiment, the shield 192 is substantially rectangular, and includes a central opening 206 through which the front button 148 protrudes. The shield 192 defines a plane parallel to and in front of a front surface 208 of the enclosure 180. When the shell 184 is mated with the enclosure 180, as shown in Figures 4 and 10, the shield 192 resides within the central opening 204 of the shell 184 such that a front surface 210 of the shield 192 is substantially flush with a front surface 212 of the shell 184 and there is little or no gap (Figure 4) between the outer edges of the shield 192 and the inner edges of the central opening 204 in the shell 184.

[0090] With further reference to Figure 6, the shield 192 includes an upper portion 214 (located above and to the sides of the front button 148) and a lower portion 216 (located below and to the sides of the front button 148). The upper and lower portions 214, 216 of the shield 192 may be separate pieces, and may comprise different materials. The upper portion 214 of the

shield 192 may be transparent or translucent so that it does not interfere with the field of view of the camera 154. For example, in certain embodiments the upper portion 214 of the shield 192 may comprise glass or plastic. As described in detail below, the microphone 150, which is operatively connected to the processor 160, is located behind the upper portion 214 of the shield 192. The upper portion 214, therefore, may include an opening 218 that facilitates the passage of sound through the shield 192 so that the microphone 150 is better able to pick up sounds from the area around the A/V recording and communication device 130.

[0091] The lower portion 216 of the shield 192 may comprise a material that is substantially transparent to infrared (IR) light, but partially or mostly opaque with respect to light in the visible spectrum. For example, in certain embodiments the lower portion 216 of the shield 192 may comprise a plastic, such as polycarbonate. The lower portion 216 of the shield 192, therefore, does not interfere with transmission of IR light from the IR light source 156, which is located behind the lower portion 216. As described in detail below, the IR light source 156 and the IR cut filter 158, which are both operatively connected to the processor 160, facilitate "night vision" functionality of the camera 154.

[0092] The upper portion 214 and/or the lower portion 216 of the shield 192 may abut an underlying cover 220 (Figure 10), which may be integral with the enclosure 180 or may be a separate piece. The cover 220, which may be opaque, may include a first opening 222 corresponding to the location of the camera 154, a second opening (not shown) corresponding to the location of the microphone 150 and the opening 218 in the upper portion 214 of the shield 192, and a third opening (not shown) corresponding to the location of the IR light source 156.

[0093] Figures 7-10 illustrate various internal components of the A/V recording and communication device 130. Figures 7-9 are front perspective views of the device 130 with the shell 184 and the enclosure 180 removed, while Figure 10 is a right-side cross-sectional view of the device 130 taken through the line 10-10 in Figure 4. With reference to Figures 7 and 8, the A/V recording and communication device 130 further comprises a main printed circuit board (PCB) 224 and a front PCB 226. With reference to Figure 8, the front PCB 226 comprises a button actuator 228. With reference to Figures 7, 8, and 10, the front button 148 is located in front of the button actuator 228. The front button 148 includes a stem 230 (Figure 10) that extends into the housing 178 to contact the button actuator 228. When the front button 148 is

pressed, the stem 230 depresses the button actuator 228, thereby closing the electronic switch 166 (Figure 8), as described below.

[0094] With reference to Figure 8, the front PCB 226 further comprises the light indicators 162, which may illuminate when the front button 148 of the device 130 is pressed. In the illustrated embodiment, the light indicators 162 comprise light-emitting diodes (LEDs 162) that are surface mounted to the front surface of the front PCB 226 and are arranged in a circle around the button actuator 228. The present embodiments are not limited to the light indicators 162 being LEDs, and in alternative embodiments the light indicators 162 may comprise any other type of light-emitting device. The present embodiments are also not limited by the number of light indicators 162 shown in Figure 8, nor by the pattern in which they are arranged.

[0095] With reference to Figure 7, the device 130 further comprises a light pipe 232. The light pipe 232 is a transparent or translucent ring that encircles the front button 148. With reference to Figure 4, the light pipe 232 resides in an annular space between the front button 148 and the central opening 206 in the shield 192, with a front surface 234 of the light pipe 232 being substantially flush with the front surface 210 of the shield 192. With reference to Figures 7 and 10, a rear portion of light pipe 232 includes a plurality of posts 236 whose positions correspond to the positions of the LEDs 162. When the LEDs 162 are illuminated, light is transmitted through the posts 236 and the body of the light pipe 232 so that the light is visible at the front surface 234 of the light pipe 232. The LEDs 162 and the light pipe 232 thus provide a ring of illumination around the front button 148. The light pipe 232 may comprise a plastic, for example, or any other suitable material capable of transmitting light.

[0096] The LEDs 162 and the light pipe 232 may function as visual indicators for a visitor and/or a user. For example, the LEDs 162 may illuminate upon activation or stay illuminated continuously. In one aspect, the LEDs 162 may change color to indicate that the front button 148 has been pressed. The LEDs 162 may also indicate that the battery 142 needs recharging, or that the battery 142 is currently being charged, or that charging of the battery 142 has been completed. The LEDs 162 may indicate that a connection to the user's wireless (and/or wired) network is good, limited, poor, or not connected. The LEDs 162 may be used to guide the user through setup or installation steps using visual cues, potentially coupled with audio cues emitted from the speaker 152.

[0097] With further reference to Figure 7, the A/V recording and communication device 130 further comprises a rechargeable battery 142. As described in further detail below, the A/V recording and communication device 130 is connected to an external power source 134 (Figure 3), such as AC mains. The A/V recording and communication device 130 is primarily powered by the external power source 134, but may also draw power from the rechargeable battery 142 so as not to exceed a threshold amount of power from the external power source 134, to thereby avoid inadvertently sounding the signaling device 168. With reference to Figure 3, the battery 142 is operatively connected to the power manager 140. As described below, the power manager 140 controls an amount of power drawn from the battery 142 to supplement the power drawn from the external AC power source 134 to power the A/V recording and communication device 130 when supplemental power is needed. The power manager 140 also controls recharging of the battery 142 using power drawn from the external power source 134. The battery 142 may comprise, for example, a lithium-ion battery, or any other type of rechargeable battery.

[0098] With further reference to Figure 7, the A/V recording and communication device 130 further comprises the camera 154. The camera 154 is coupled to a front surface of the front PCB 226, and includes a lens 238 and an imaging processor 240 (Figure 9). The camera lens 238 may be a lens capable of focusing light into the camera 154 so that clear images may be captured. The camera 154 may comprise, for example, a high definition (HD) video camera, such as one capable of capturing video images at an image display resolution of 720p or better. In certain of the present embodiments, the camera 154 may be used to detect motion within its field of view, as described below.

[0099] With further reference to Figure 7, the A/V recording and communication device 130 further comprises an infrared (IR) light source 242. In the illustrated embodiment, the IR light source 242 comprises an IR light-emitting diode (LED) 242 coupled to an IR LED printed circuit board (PCB) 244. In alternative embodiments, the IR LED 242 may not comprise a separate PCB 244, and may, for example, be coupled to the front PCB 226.

[00100] With reference to Figures 7 and 10, the IR LED PCB 244 is located below the front button 148 (Figure 7) and behind the lower portion 216 of the shield 192 (Figure 10). As described above, the lower portion 216 of the shield 192 is transparent to IR light, but may be opaque with respect to light in the visible spectrum. In alternative embodiments of the IR LED PCB 244, the IR LED PCB 244 may include more than one IR LED 242. For example, the IR

LED PCB 244 may include three IR LEDs 242, or any other number of IR LEDs 242. In embodiments including more than one IR LED 242, the size of the third opening in the cover may be increased to accommodate the larger size of the IR LED PCB 244.

[00101] The IR LED 242 may be triggered to activate when a low level of ambient light is detected. When activated, IR light emitted from the IR LED 242 illuminates the camera 154's field of view. The camera 154, which may be configured to detect IR light, may then capture the IR light emitted by the IR LED 242 as it reflects off objects within the camera 154's field of view, so that the A/V recording and communication device 130 can clearly capture images at night (may be referred to as "night vision").

[00102] With reference to Figure 9, the A/V recording and communication device 130 further comprises an IR cut filter 158. The IR cut filter 158 is a mechanical shutter that can be selectively positioned between the lens 238 and the image sensor of the camera 154. During daylight hours, or whenever there is a sufficient amount of ambient light, the IR cut filter 158 is positioned between the lens 238 and the image sensor to filter out IR light so that it does not distort the colors of images as the human eye sees them. During nighttime hours, or whenever there is little to no ambient light, the IR cut filter 158 is withdrawn from the space between the lens 238 and the image sensor, so that the camera 154 is sensitive to IR light ("night vision"). In some embodiments, the camera 154 acts as a light detector for use in controlling the current state of the IR cut filter 158 and turning the IR LED 242 on and off. Using the camera 154 as a light detector is facilitated in some embodiments by the fact that the A/V recording and communication device 130 is powered by a connection to AC mains, and the camera 154, therefore, is always powered on. In other embodiments, however, the A/V recording and communication device 130 may include a light sensor separate from the camera 154 for use in controlling the IR cut filter 158 and the IR LED 242.

[00103] With reference back to Figure 6, the A/V recording and communication device 130 further comprises a reset button 170. The reset button 170 contacts a reset button actuator 246 (Figure 8) coupled to the front PCB 226. When the reset button 170 is pressed, it may contact the reset button actuator 246, which may trigger the erasing of any data stored at the non-volatile memory 174 and/or at the memory 172 (Figure 3), and/or may trigger a reboot of the processor 160. In some embodiments, the reset button 170 may also be used in a process to activate the A/V recording and communication device 130, as described below.

[00104] Figures 11-13 further illustrate internal components of the A/V recording and communication device 130. Figures 11-13 are rear perspective views of the device 130 with the back plate 182 and additional components removed. For example, in Figure 11 the back plate 182 is removed, while in Figure 12 the back plate 182 and the main PCB 224 are removed, and in Figure 13 the back plate 182, the main PCB 224, and the front PCB 226 are removed. With reference to Figure 11, several components are coupled to the rear surface of the main PCB 224, including the communication module 146, the processor 160, memory 172, and non-volatile memory 174. The functions of each of these components are described below. With reference to Figure 12, several components are coupled to the rear surface of the front PCB 226, including the power manager 140, the power sequencer 144, the AC/DC rectifier 136, the DC/DC converter 138, and the controller 164 for the light indicators 162. The functions of each of these components are also described below. With reference to Figure 13, several components are visible within the enclosure 180, including the microphone 150, a speaker chamber 248 (in which the speaker 152 is located), and an antenna 250 for the communication module 146. The functions of each of these components are also described below.

[00105] With reference to Figure 7, the antenna 250 is coupled to the front surface of the main PCB 224 and operatively connected to the communication module 146, which is coupled to the rear surface of the main PCB 224 (Figure 11). The microphone 150, which may also be coupled to the front surface of the main PCB 224, is located near the opening 218 (Figure 4) in the upper portion 214 of the shield 192 so that sounds emanating from the area around the A/V recording and communication device 130 can pass through the opening 218 and be detected by the microphone 150. With reference to Figure 13, the speaker chamber 248 is located near the bottom of the enclosure 180. The speaker chamber 248 comprises a hollow enclosure in which the speaker 152 is located. The hollow speaker chamber 248 amplifies the sounds made by the speaker 152 so that they can be better heard by a visitor in the area near the A/V recording and communication device 130. With reference to Figures 5 and 13, the lower surface 252 of the shell 184 and the lower surface (not shown) of the enclosure 180 may include an acoustical opening 254 through which the sounds made by the speaker 152 can pass so that they can be better heard by a visitor in the area near the A/V recording and communication device 130. In the illustrated embodiment, the acoustical opening 254 is shaped generally as a rectangle having a length extending substantially across the lower surface 252 of the shell 184 (and also the

enclosure 180). The illustrated shape is, however, just one example. With reference to Figure 5, the lower surface 252 of the shell 184 may further include an opening 256 for receiving a security screw (not shown). The security screw may extend through the opening 256 and into a similarly located opening in the enclosure 180 to secure the shell 184 to the enclosure 180. If the device 130 is mounted to a mounting bracket (not shown), the security screw may also maintain the device 130 on the mounting bracket.

[00106] With reference to Figure 13, the A/V recording and communication device 130 may further include a battery heater 258. The present A/V recording and communication device 130 is configured for outdoor use, including in cold climates. Cold temperatures, however, can cause negative performance issues for rechargeable batteries, such as reduced energy capacity, increased internal resistance, reduced ability to charge without damage, and reduced ability to supply load current. The battery heater 258 helps to keep the rechargeable battery 142 warm in order to reduce or eliminate the foregoing negative performance issues. In the illustrated embodiment, the battery heater 258 comprises a substantially flat, thin sheet abutting a side surface of the rechargeable battery 142. The battery heater 258 may comprise, for example, an electrically resistive heating element that produces heat when electrical current is passed through it. The battery heater 258 may thus be operatively coupled to the power manager 140 and/or the power sequencer 144 (Figure 12). In some embodiments, the rechargeable battery 142 may include a thermally sensitive resistor ("thermistor," not shown) operatively connected to the processor 160 so that the battery 142's temperature can be monitored and the amount of power supplied to the battery heater 258 can be adaptively controlled to keep the rechargeable battery 142 within a desired temperature range.

[00107] As discussed above, the present disclosure provides numerous examples of methods and systems including A/V recording and communication doorbells, but the present embodiments are equally applicable for A/V recording and communication devices other than doorbells. For example, the present embodiments may include one or more A/V recording and communication security cameras instead of, or in addition to, one or more A/V recording and communication doorbells. An example A/V recording and communication security camera may include substantially all of the structure and functionality of the device 130, but without the front button 148, the button actuator 228, and/or the light pipe 232.

[00108] The present disclosure also provides numerous examples of methods and systems including A/V recording and communication devices that are powered by a connection to AC mains, but the present embodiments are equally applicable for A/V recording and communication devices that are battery powered. For example, the present embodiments may include an A/V recording and communication device such as those described in US Patent Application Publication Nos. 2015/0022620 (Application Serial No. 14/499,828) and 2015/0022618 (Application Serial No. 14/334,922), both of which are incorporated herein by reference in their entireties as if fully set forth.

[00109] As discussed above, parcel theft is an increasingly common problem. Parcel carriers frequently leave parcels near the front door of a home when no one answers the door at the time of delivery. These parcels are vulnerable to theft, as they are often clearly visible from the street. This problem has only gotten worse with the proliferation of online commerce, and is particularly common around major holidays when many consumers do their holiday shopping online. It would be advantageous, therefore, if the functionality of A/V recording and communication devices could be leveraged to deter parcel theft and/or to identify and apprehend parcel thieves. It would also be advantageous if the functionality of A/V recording and communication devices could be enhanced in one or more ways to deter parcel theft and/or to identify and apprehend parcel thieves. The present embodiments provide these advantages and enhancements, as described below.

[00110] For example, some of the present embodiments deter parcel theft and/or facilitate the identification and apprehension of parcel thieves by determining that a parcel has been delivered, determining that the parcel has been removed from the delivery area, determining whether removal of the parcel was authorized, and, when the removal of the parcel is determined to have been unauthorized, generating an alert. Further, because the present embodiments include A/V recording and communication devices, acts of parcel theft are recorded by the camera of the A/V recording and communication device. These images are useful in identifying and apprehending parcel thieves.

[00111] Some of the present embodiments comprise computer vision for one or more aspects, such as object recognition. Computer vision includes methods for acquiring, processing, analyzing, and understanding images and, in general, high-dimensional data from the real world in order to produce numerical or symbolic information, e.g. in the form of decisions. Computer

vision seeks to duplicate the abilities of human vision by electronically perceiving and understanding an image. Understanding in this context means the transformation of visual images (the input of the retina) into descriptions of the world that can interface with other thought processes and elicit appropriate action. This image understanding can be seen as the disentangling of symbolic information from image data using models constructed with the aid of geometry, physics, statistics, and learning theory. Computer vision has also been described as the enterprise of automating and integrating a wide range of processes and representations for vision perception. As a scientific discipline, computer vision is concerned with the theory behind artificial systems that extract information from images. The image data can take many forms, such as video sequences, views from multiple cameras, or multi-dimensional data from a scanner. As a technological discipline, computer vision seeks to apply its theories and models for the construction of computer vision systems.

[00112] One aspect of computer vision comprises determining whether or not the image data contains some specific object, feature, or activity. Different varieties of computer vision recognition include: Object Recognition (also called object classification) – One or several pre-specified or learned objects or object classes can be recognized, usually together with their 2D positions in the image or 3D poses in the scene. Identification – An individual instance of an object is recognized. Examples include identification of a specific person's face or fingerprint, identification of handwritten digits, or identification of a specific vehicle. Detection – The image data are scanned for a specific condition. Examples include detection of possible abnormal cells or tissues in medical images or detection of a vehicle in an automatic road toll system. Detection based on relatively simple and fast computations is sometimes used for finding smaller regions of interesting image data that can be further analyzed by more computationally demanding techniques to produce a correct interpretation.

[00113] Several specialized tasks based on computer vision recognition exist, such as: Optical Character Recognition (OCR) – Identifying characters in images of printed or handwritten text, usually with a view to encoding the text in a format more amenable to editing or indexing (e.g. ASCII). 2D Code Reading – Reading of 2D codes such as data matrix and QR codes. Facial Recognition. Shape Recognition Technology (SRT) – Differentiating human beings (e.g. head and shoulder patterns) from objects.

[00114] Typical functions and components (e.g. hardware) found in many computer vision systems are described in the following paragraphs. The present embodiments may include at least some of these aspects. For example, with reference to Figure 3, embodiments of the present A/V recording and communication device 130 may include a computer vision module 163. The computer vision module 163 may include any of the components (e.g. hardware) and/or functionality described herein with respect to computer vision, including, without limitation, one or more cameras, sensors, and/or processors. In some embodiments, the microphone 150, the camera 154, and/or the imaging processor 240 may be components of the computer vision module 163.

[00115] Image acquisition – A digital image is produced by one or several image sensors, which, besides various types of light-sensitive cameras, may include range sensors, tomography devices, radar, ultra-sonic cameras, etc. Depending on the type of sensor, the resulting image data may be a 2D image, a 3D volume, or an image sequence. The pixel values may correspond to light intensity in one or several spectral bands (gray images or color images), but can also be related to various physical measures, such as depth, absorption or reflectance of sonic or electromagnetic waves, or nuclear magnetic resonance.

[00116] Pre-processing – Before a computer vision method can be applied to image data in order to extract some specific piece of information, it is usually beneficial to process the data in order to assure that it satisfies certain assumptions implied by the method. Examples of pre-processing include, but are not limited to re-sampling in order to assure that the image coordinate system is correct, noise reduction in order to assure that sensor noise does not introduce false information, contrast enhancement to assure that relevant information can be detected, and scale space representation to enhance image structures at locally appropriate scales.

[00117] Feature extraction – Image features at various levels of complexity are extracted from the image data. Typical examples of such features are: Lines, edges, and ridges; Localized interest points such as corners, blobs, or points; More complex features may be related to texture, shape, or motion.

[00118] Detection/segmentation – At some point in the processing a decision may be made about which image points or regions of the image are relevant for further processing. Examples are: Selection of a specific set of interest points; Segmentation of one or multiple image regions that contain a specific object of interest; Segmentation of the image into

nested scene architecture comprising foreground, object groups, single objects, or salient object parts (also referred to as spatial-taxon scene hierarchy).

[00119] High-level processing – At this step, the input may be a small set of data, for example a set of points or an image region that is assumed to contain a specific object. The remaining processing may comprise, for example: Verification that the data satisfy model-based and application-specific assumptions; Estimation of application-specific parameters, such as object pose or object size; Image recognition – classifying a detected object into different categories; Image registration – comparing and combining two different views of the same object.

[00120] Decision making – Making the final decision required for the application, for example match/no-match in recognition applications.

[00121] One or more of the present embodiments may include a vision processing unit (not shown separately, but may be a component of the computer vision module 163). A vision processing unit is an emerging class of microprocessor; it is a specific type of AI (artificial intelligence) accelerator designed to accelerate machine vision tasks. Vision processing units are distinct from video processing units (which are specialized for video encoding and decoding) in their suitability for running machine vision algorithms such as convolutional neural networks, SIFT, etc. Vision processing units may include direct interfaces to take data from cameras (bypassing any off-chip buffers), and may have a greater emphasis on on-chip dataflow between many parallel execution units with scratchpad memory, like a manycore DSP (digital signal processor). But, like video processing units, vision processing units may have a focus on low precision fixed point arithmetic for image processing.

[00122] As described above, one aspect of the present embodiments includes the realization that parcel pilferage is a pernicious and persistent problem. Parcel carriers frequently leave parcels near the front door of a home when no one answers the door at the time of delivery. These parcels are vulnerable to theft, as they are often clearly visible from the street. This problem has only gotten worse with the proliferation of online commerce, and is particularly common around major holidays when many consumers do their holiday shopping online. It would be advantageous, therefore, if the functionality of A/V recording and communication devices could be leveraged to deter parcel theft and/or to identify and apprehend parcel thieves. It would also be advantageous if the functionality of A/V recording and communication devices

could be enhanced in one or more ways to deter parcel theft and/or to identify and apprehend parcel thieves. The present embodiments provide these advantages and enhancements, as described below.

[00123] Figure 14 illustrates an example embodiment of a process for deterring parcel theft with an A/V recording and communication device according to various aspects of the present disclosure. At block B300, the process determines that a parcel has been left within an area about an A/V recording and communication device, such as the A/V recording and communication device 130 described above. The present embodiments encompass any method of determining that a parcel has been left within an area about an A/V recording and communication device, and several examples are provided below. The present embodiments are not, however, limited to these examples, which are provided for illustration only. Any of the examples described below, as well as any of the present embodiments, may include one or more aspects of computer vision.

[00124] In one example embodiment, determining that the parcel has been left within the area about the A/V recording and communication device 130 may comprise comparing video frames recorded by the camera 154 of the A/V recording and communication device 130, e.g. using computer vision. For example, before a parcel is left within the area about the A/V recording and communication device 130, the field of view of the camera 154 may remain largely static. Different objects may occasionally (or frequently) pass through the camera's field of view, such as people, animals, cars, etc., but these objects generally do not remain within the camera's field of view for very long (on the order of seconds) and, if they stop within the camera's field of view, they typically begin moving again soon after stopping. By contrast, when a parcel is left within the camera's field of view, it typically remains within the camera's field of view for a significant amount of time (on the order of minutes or hours), and the parcel typically remains motionless throughout the time that it remains within the camera's field of view (at least until someone picks it up and carries it away). Thus, comparing video frames from a time before a parcel is left within the camera's field of view with video frames from a time after the parcel is left within the camera's field of view may enable a reliable determination to be made as to whether an object that is present within the camera's field of view is a parcel or not.

[00125] The present embodiments contemplate numerous methodologies for determining whether an object that is present within the camera's field of view is a parcel or not. Any or all

of these methodologies may include one or more aspects of computer vision. For example, in some embodiments an object within the camera's field of view may be determined to be a parcel if the object is not present within the camera's field of view at a first time (in a first video frame), the object is present within the camera's field of view at a second time after the first time (in a second video frame), and the object remains within the camera's field of view for at least a threshold amount of time. Determining whether the object remains within the camera's field of view for at least the threshold amount of time may comprise review of one or more video frames that are recorded after the second video frame. In other embodiments, an object within the camera's field of view may be determined to be a parcel if the object is not present within the camera's field of view at a first time (in a first video frame), the object is present within the camera's field of view at a second time after the first time (in a second video frame), and the object remains motionless within the camera's field of view for at least a threshold amount of time. Determining whether the object remains motionless within the camera's field of view for at least the threshold amount of time may comprise review of one or more video frames that are recorded after the second video frame.

[00126] In other embodiments, an object within the camera's field of view may be determined to be a parcel if the object is not present within the camera's field of view at a first time (in a first video frame), a person is detected approaching the A/V recording and communication device 130 at a second time after the first time (in a second video frame), the person is detected moving away from the A/V recording and communication device 130 at a third time after the second time (in a third video frame), and the object is present within the camera's field of view at a fourth time after the third time (in a fourth video frame).

[00127] In other embodiments, an object within the camera's field of view may be determined to be a parcel if the object is not present within the camera's field of view at a first time (in a first video frame), a stationary vehicle (which may be a delivery vehicle, for example) is detected within the camera's field of view at a second time after the first time (in a second video frame), the object is present within the camera's field of view at a third time after the second time (in a third video frame), and the vehicle is no longer present within the camera's field of view at a fourth time after the third time (in a fourth video frame).

[00128] In other embodiments, an object within the camera's field of view may be determined to be a parcel if the object is not present within the camera's field of view at a first

time (in a first video frame), the object is present within the camera's field of view at a second time after the first time (in a second video frame), and the object meets one or more criteria, such as having one or more physical characteristics. Examples of physical characteristics that may be examined to determine whether the object is a parcel include, without limitation, size, shape, color, and material (or materials). For example, if the object is made of cardboard and is brown or white (common colors for cardboard shipping boxes), it may be determined to be a parcel.

[00129] The present embodiments contemplate many processes for examining physical characteristics of the object and making a determination as to whether the object is a parcel. For example, some embodiments may comprise gathering information about the object using computer vision, and then comparing the gathered information about the object to stored information about parcels to determine whether there is a match. For example, the present embodiments may include a database of parcels and/or physical characteristics of parcels. The database may include pictures of known parcels, and comparing the gathered information about the object to the stored information about parcels may comprise comparing a picture of the object to the pictures of known parcels. Gathering information about the object using computer vision may comprise using one or more cameras, scanners, imagers, etc. and/or one or more sensors, such as sonar.

[00130] With reference to Figure 15, information received by the computer vision module 163 of the A/V recording and communication device 130 may be sent to one or more network devices, such as the server 118 and/or the backend API 120, in a computer vision query signal 310. The one or more network devices may then analyze the sent information and/or compare the sent information with other information in one or more databases to determine whether there is a match, for example in order to identify the parcel. In one example embodiment, comparing the sent information about the parcel with other information in one or more databases to determine whether there is a match may comprise comparing the sent information, such as one or more photos or images, about the parcel with photos and/or images of known parcels. If there is a match, then one or more actions may occur, such as the A/V recording and communication device 130 transitioning to a different operational mode. For example, the network device, such as the server 118 and/or the backend API 120, may send a computer vision response signal 312 to the A/V recording and communication device 130. The computer vision response signal 312 may include a command to the A/V recording and communication device 130 to change the

operational mode of the A/V recording and communication device 130. For example, the command to the A/V recording and communication device 130 may cause the A/V recording and communication device 130 to transition to an "armed" mode in which the A/V recording and communication device 130 is configured to take one or more actions when the parcel is removed from the area about the A/V recording and communication device 130, as described below.

[00131] In another example embodiment, determining that the parcel has been left within the area about the A/V recording and communication device 130 may comprise receiving information from a carrier (e.g. the postal service, FedEx, UPS, etc.) that delivered the parcel. For example, when the parcel carrier delivers the parcel, or at some time after the parcel carrier has delivered the parcel, the carrier may update a delivery status of the parcel in the carrier's parcel tracking system to indicate that the parcel has been delivered. The carrier's parcel tracking system may then forward that information to one or more network devices, such as the server 118 and/or the backend API 120, which may then forward the information to the A/V recording and communication device 130.

[00132] In another example embodiment, determining that the parcel has been left within the area about the A/V recording and communication device 130 may comprise automatic identification and data capture (AIDC). For example, the parcel may include at least one of a barcode 320 (Figure 16), a matrix code 322 (Figure 17), a bokode 324 (Figure 18), and a radio frequency identification (RFID) tag 326 (Figure 19). AIDC refers to methods of automatically identifying objects, collecting data about them, and entering that data directly into computer systems (e.g. without human involvement). Technologies typically considered part of AIDC include barcodes, matrix codes, bokodes, RFID, biometrics (e.g. iris recognition, facial recognition, voice recognition, etc.), magnetic stripes, Optical Character Recognition (OCR), and smart cards. AIDC is also commonly referred to as "Automatic Identification," "Auto-ID," and "Automatic Data Capture."

[00133] AIDC encompasses obtaining external data, particularly through analysis of images and/or sounds. To capture data, a transducer may convert an image or a sound into a digital file. The file is then typically stored and analyzed by a computer, and/or compared with other files in a database, to verify identity and/or to provide authorization to enter a secured system. AIDC also refers to methods of recognizing objects, getting information about them, and entering that data or feeding it directly into computer systems without any human

involvement. In biometric security systems, capture may refer to the acquisition of and/or the process of acquiring and identifying characteristics, such as finger images, palm images, facial images, or iris prints, which all may involve video data, or voice prints, which may involve audio data.

[00134] A barcode, such as the example barcode 320 shown in Figure 16, is an optical machine-readable representation of data relating to the object to which it is attached. Barcodes systematically represent data by varying the widths and spacings of parallel lines, and may be referred to as linear or one-dimensional (1D) barcodes.

[00135] A matrix code, such as the example matrix code 322 shown in Figure 17, is a two-dimensional matrix barcode consisting of black and white "cells" or modules arranged in either a square or rectangular pattern. The information encoded can be text and/or numeric data. Quick response (QR) codes and Data Matrix codes are specific types of matrix codes.

[00136] A bokode, such as the example bokode 324 shown in Figure 18, is a type of data tag that holds much more information than a barcode over the same area. The bokode pattern is a tiled series of matrix codes. Bokodes may be circular, and may include an LED covered with a mask and a lens.

[00137] Radio-frequency identification (RFID) uses electromagnetic fields to automatically identify and track tags attached to objects. The tags, such as the example RFID tag 326 shown in Figure 19, contain electronically stored information, and may be passive or active. Passive tags collect energy from a nearby RFID reader's interrogating radio waves. Active tags have a local power source, such as a battery, and may operate at hundreds of meters from the RFID reader. Unlike a barcode, the tag need not be within the line of sight of the reader, so it may be embedded in the tracked object.

[00138] The A/V recording and communication device 130 may capture information embedded in one of these types (or any other type) of AIDC technologies. For example, with reference to Figure 3, the A/V recording and communication device 130 may include an AIDC module 165 operatively connected to the processor 160. The AIDC module 165 may include hardware and/or software configured for one or more types of AIDC, including, but not limited to, any of the types of AIDC described herein. For example, the AIDC module 165 may include an RFID reader (not shown), and the camera 154 of the A/V recording and communication device 130 may in some embodiments be considered to be part of the AIDC module 165. For

example, with respect to barcodes, matrix codes, and bokodes (or any other type code), the camera 154 of the A/V recording and communication device 130 may scan the code, and any information embedded therein. To facilitate scanning the code, the parcel carrier may hold the parcel up to the camera 154. With respect to RFID, the RFID reader of the AIDC module 165 may interrogate an RFID tag 326 on, or embedded in, the parcel. In some embodiments, the processor 160 of the A/V recording and communication device 130 may be considered to be part of the AIDC module 165 and/or the processor 160 may operate in conjunction with the AIDC module 165 in various AIDC processes.

[00139] AIDC and computer vision have significant overlap, and use of either one of these terms herein should be construed as also encompassing the subject matter of the other one of these terms. For example, the computer vision module 163 and the AIDC module 165 may comprise overlapping hardware components and/or functionality. In some embodiments, the computer vision module 163 and the AIDC module 165 may be combined into a single module.

[00140] With reference to Figure 20, information received by the AIDC module 165 of the A/V recording and communication device 130 from one or more codes or tags may be sent to one or more network devices, such as the server 118 and/or the backend API 120, in an AIDC query signal 330. The one or more network devices may then analyze the sent information and/or compare the sent information with other information in one or more codes databases to determine whether there is a match, for example in order to identify the parcel. If there is a match, then one or more actions may occur, such as the A/V recording and communication device 130 transitioning to a different operational mode. For example, the network device, such as the server 118 and/or the backend API 120, may send an AIDC response signal 332 to the A/V recording and communication device 130. The AIDC response signal 332 may include a command to the A/V recording and communication device 130 to change the operational mode of the A/V recording and communication device 130. For example, the command to the A/V recording and communication device 130 may cause the A/V recording and communication device 130 to transition to an "armed" mode in which the A/V recording and communication device 130 is configured to take one or more actions when the parcel is removed from the area about the A/V recording and communication device 130, as described below.

[00141] With further reference to Figure 14, at block B302 the process determines that the parcel has been removed from the area about the A/V recording and communication device 130.

The present embodiments encompass any method of determining that a parcel has been removed from the area about an A/V recording and communication device, and several examples are provided below. The present embodiments are not, however, limited to these examples, which are provided for illustration only. Any of the examples described below, as well as any of the present embodiments, may include one or more aspects of computer vision.

[00142] In one example embodiment, determining that the parcel has been removed from the area about the A/V recording and communication device 130 may comprise comparing video frames recorded by the camera 154 of the A/V recording and communication device 130. For example, after a parcel has been determined to have been left within the area about the A/V recording and communication device 130, the parcel is likely to remain motionless in the position where it was left. Thus, if the parcel is present within the camera's field of view at a first time (in a first video frame), and is no longer present within the camera's field of view at a second time after the first time (in a second video frame), then the parcel may be determined to have been removed from the area about the A/V recording and communication device 130.

[00143] In another example embodiment, determining that the parcel has been removed from the area about the A/V recording and communication device 130 may comprise AIDC. For example, if the parcel includes an RFID tag, then an RFID reader of the AIDC module 165 may detect that the RFID tag no longer responds to interrogation signals. In some embodiments, if the RFID reader sends a threshold number of interrogation signals and receives no response from the RFID tag of the parcel, the process may determine that the parcel has been removed from the area about the A/V recording and communication device 130. In some embodiments, the threshold number of interrogation signals with no response may be one interrogation signal, or two interrogation signals, or three interrogation signals, or any other number of interrogation signals.

[00144] With further reference to Figure 14, at block B304 the process determines whether removal of the parcel from the area about the A/V recording and communication device 130 was authorized. The present embodiments encompass any method of determining whether removal of the parcel from the area about the A/V recording and communication device 130 was authorized, and several examples are provided below. The present embodiments are not, however, limited to these examples, which are provided for illustration only. Any of the

examples described below, as well as any of the present embodiments, may include one or more aspects of computer vision.

[00145] In one example embodiment, determining whether removal of the parcel from the area about the A/V recording and communication device 130 was authorized may comprise detecting (or tracking) a direction of movement of the parcel. For example, when a parcel is left outside the front entrance of a home, the homeowner (or other occupant) will typically pick up the parcel and bring it inside the home. A parcel thief, by contrast, will typically pick up the parcel and carry it away from the home. Thus, if the A/V recording and communication device 130 detects that the parcel is moving toward a structure to which the A/V recording and communication device 130 is secured (or with which the A/V recording and communication device 130 is associated), then the process may determine that the removal of the parcel from the area about the A/V recording and communication device 130 is authorized. But, if the A/V recording and communication device 130 detects that the parcel is moving away from the structure to which the A/V recording and communication device 130 is secured (or with which the A/V recording and communication device 130 is associated), then the process may determine that the removal of the parcel from the area about the A/V recording and communication device 130 is unauthorized.

[00146] In another example embodiment, determining whether removal of the parcel from the area about the A/V recording and communication device 130 was authorized may comprise AIDC and/or computer vision. For example, if an authorized person (e.g. the addressee of the parcel) removes the parcel from the area about the A/V recording and communication device 130, the A/V recording and communication device 130 may receive information from the authorized person. For example, the authorized person may present identification or credentials to the A/V recording and communication device 130. The camera 154 and/or the AIDC module 165 and/or the processor 160 of the A/V recording and communication device 130 may receive information from the identification or credentials for use in determining that the person removing the parcel from the area about the A/V recording and communication device 130 is an authorized person. If no identification or credentials are presented when the parcel is removed from the area about the A/V recording and communication device 130, or if identification or credentials are presented but they do not match an expected identification or credentials, then the process may determine that the person removing the parcel from the area about the A/V recording and

communication device 130 is not an authorized person. In some embodiments, the A/V recording and communication device 130 may provide a prompt, such as a voice prompt emitted through the speaker, requesting identification or credentials when a person is detected within the area about the A/V recording and communication device 130 and/or when the A/V recording and communication device 130 detects that the parcel has been moved or picked up.

[00147] Examples of identification or credentials that could be used in the foregoing processes include, without limitation, a card (or other carrier or substrate) bearing a barcode 320, or a matrix code 322, or a bokode 324, or an RFID tag 326, or an embedded integrated circuit (such as in a smart card, a chip card, or an integrated circuit card (ICC)), or a magnetic stripe. Figure 21 illustrates an example of a smart card 340 including an embedded integrated circuit 342, and Figure 22 illustrates an example of a card 344 including a magnetic stripe 346.

[00148] A smart card, chip card, or integrated circuit card (ICC), such as the example smart card 340 shown in Figure 21, is any pocket-sized card that has one or more embedded integrated circuits. Smart cards may be either contact or contactless. Contact smart cards include a contact area comprising contact pads. These pads provide electrical connectivity when inserted into a reader, which serves as a communication medium between the smart card and a host (e.g., a computer, or a point of sale terminal). Contact smart cards do not contain batteries. Instead, power is supplied by the card reader. With contactless smart cards, the card communicates with and is powered by the reader through RF induction technology. These cards require only proximity to an antenna to communicate. Like contact smart cards with, contactless cards do not have an internal power source. Instead, they use an inductor to capture some of the incident radio-frequency interrogation signal, rectify it, and use it to power the card's electronics.

[00149] A magnetic stripe card, such as the example card 344 shown in Figure 22, is a type of card capable of storing data by modifying the magnetism of tiny iron-based magnetic particles on a band of magnetic material on the card. The magnetic stripe, sometimes called a magstripe, is read by swiping past a magnetic reading head.

[00150] Further examples of identification or credentials that could be used in the foregoing processes include, without limitation, a card (or other carrier or substrate) bearing text that can be received as input by the AIDC module 165 and/or the camera 154 and/or the

processor 160 through optical character recognition (OCR). OCR is the mechanical or electronic conversion of images of typed, handwritten, or printed text into machine-encoded text.

[00151] Further examples of AIDC and/or computer vision that can be used in the present embodiments to verify the identity and/or authorization of a person include, without limitation, biometrics. Biometrics refers to metrics related to human characteristics. Biometrics authentication (or realistic authentication) is used in various forms of identification and access control. Biometric identifiers are the distinctive, measurable characteristics used to label and describe individuals. Biometric identifiers can be physiological characteristics and/or behavioral characteristics. Physiological characteristics may be related to the shape of the body. Examples include, but are not limited to, fingerprints, palm veins, facial recognition, three-dimensional facial recognition, skin texture analysis, DNA, palm prints, hand geometry, iris recognition, retina recognition, and odor/scent recognition. Behavioral characteristics may be related to the pattern of behavior of a person, including, but not limited to, typing rhythm, gait, and voice recognition.

[00152] The present embodiments may use any one, or any combination of more than one, of the foregoing biometrics to identify and/or authenticate a person who removes the parcel from the area about the A/V recording and communication device 130. For example, the computer vision module 163, the AIDC module 165, and/or the camera 154 and/or the processor 160 may receive information about the person using any one, or any combination of more than one, of the foregoing biometrics.

[00153] Another aspect of determining whether removal of the parcel from the area about the A/V recording and communication device 130 was authorized may comprise comparing information received through the AIDC (and/or computer vision) to information about one or more persons. With reference to Figure 20, information received by the AIDC module 165 (and/or the computer vision module 163) and/or the camera 154 and/or the processor 160 of the A/V recording and communication device 130 may be sent to one or more network devices, such as the server 118 and/or the backend API 120, in an AIDC query signal 330. The one or more network devices may then compare information in the AIDC query signal 330 about the person detected in the area about the A/V recording and communication device 130 with information from one or more sources. These information sources may include one or more databases and/or services. For example, a database and/or service may include a smart list of authorized persons.

If a person who removed the parcel is on the smart list of authorized persons, then the removal of the parcel from the area about the A/V recording and communication device 130 may be determined to be authorized.

[00154] In some embodiments, the information in the AIDC query signal 330 may be compared with information about one or more persons who are authorized to remove parcels from the area about the A/V recording and communication device 130. For example, biometric information (or other AIDC/computer vision information) about one or more authorized persons may be uploaded and stored at one or more databases and/or services accessible to the one or more network devices, such as the server 118 and/or the backend API 120. Comparison(s) between this information and the information in the AIDC query signal 330 may determine whether a person detected in the area about the A/V recording and communication device 130 is an authorized person or not. The comparison(s) may be performed by one or more network devices, such as the server 118 and/or the backend API 120, for example.

[00155] In other embodiments, the information in the AIDC query signal 330 may be compared with information about one or more persons who have been reported in connection with one or more crimes and/or suspicious events. In some embodiments, the crime(s) and/or suspicious event(s) may have occurred within a defined radius of the A/V recording and communication device 130. For example, a first user of an A/V recording and communication device may view video footage that was recorded by his or her device and determine that the person or persons in the video footage are, or may be, engaged in suspicious activity and/or criminal activity. The first user may then share that video footage with one or more other people, such as other users of A/V recording and communication devices, and/or one or more organizations, including one or more law enforcement agencies. The present embodiments may leverage this shared video footage for use in comparing with the information in the AIDC query signal 330 to determine whether a person detected in the area about the A/V recording and communication device 130 is the same person that was the subject of (and/or depicted in) the shared video footage. If a person detected in the area about the A/V recording and communication device 130 is the same person that was reported in connection with one or more crimes and/or suspicious events, then that person is probably not a person who is authorized to remove parcels from the area about the A/V recording and communication device 130. In some embodiments, the person (or persons) depicted in the shared video footage may be a

perpetrator(s) of one or more parcel thefts. Further, those parcel thefts may have occurred within a defined radius about the A/V recording and communication device 130. Further description of sharing video footage from A/V recording and communication devices is provided in US patent application Serial Nos. 15/387,471 (filed on December 12, 2016 and entitled "SHARING VIDEO FOOTAGE FROM AUDIO/VIDEO RECORDING AND COMMUNICATION DEVICES") and 15/387,444 (filed on December 12, 2016 and entitled "SHARING VIDEO FOOTAGE FROM AUDIO/VIDEO RECORDING AND COMMUNICATION DEVICES"), both of which are incorporated herein by reference in their entireties as if fully set forth.

[00156] In another example embodiment, AIDC and/or computer vision may comprise the camera 154 of the A/V recording and communication device 130 capturing an image of a person in the area about the A/V recording and communication device 130. The image of the person may comprise an image of the person's face. The image of the person's face may be compared with image(s) of the face(s) of at least one other person. In some embodiments, the at least one other person may be a person or persons who were reported in connection with suspicious activity and/or criminal activity, such as parcel theft. The comparison(s) may be performed by one or more network devices, such as the server 118 and/or the backend API 120. If a match is found between the image of the person's face captured by the camera 154 of the A/V recording and communication device 130 and the at least one image of the face(s) of at least one other person, then the process may determine that removal of the parcel from the area about the A/V recording and communication device 130 was unauthorized. The process may then generate an alert, which may comprise any or all of the alert types described herein.

[00157] With further reference to Figure 20, the network device, such as the server 118 and/or the backend API 120, may send an AIDC response signal 332 to the A/V recording and communication device 130. In some embodiments, the AIDC response signal 332 may be sent after a comparison has been made between the information in the AIDC query signal 330 and the information about one or more persons who are authorized to remove parcels from the area about A/V recording and communication device 130 and/or the information about one or more persons who have been reported in connection with one or more crimes and/or suspicious events. The AIDC response signal 332 may comprise an indicator (and/or information) about whether a person detected in the area about the A/V recording and communication device 130 is authorized to remove parcels from that area or not.

[00158] With further reference to Figure 14, at block B306, when the removal of the parcel from the area about the A/V recording and communication device 130 is determined to have been unauthorized, the process may generate an alert. In some embodiments, the alert may comprise an alert signal sent to a client device. For example, the alert may be similar to, or the same as, the process described above with respect to block B268 of Figure 2, in which audio and/or video data is transmitted (streamed) from the A/V recording and communication device 130 to the user's client device 114 via the user's network 110 and the network 112. The streaming video may include images of the person(s) who was/were determined to have been unauthorized. The user can then determine whether to take further action, such as alerting law enforcement and/or sharing the video footage with other people, such as via social media.

[00159] In some embodiments, the alert may comprise an audible alarm emitted from the speaker 152 of the A/V recording and communication device 130. The audible alarm may be any loud noise likely to attract attention and/or startle the unauthorized person, making it more likely that he or she will flee without absconding with the parcel(s). In some embodiments, the alert may comprise an announcement emitted from the speaker 152 of the A/V recording and communication device 130. The announcement may comprise a verbal warning that the area about the A/V recording and communication device 130 is being recorded. The unauthorized person, upon being informed that the area about the A/V recording and communication device 130 is being recorded, may decide to flee the scene without absconding with the parcel(s). In some embodiments, the alert may comprise both an audible alarm and an announcement in combination. Also in some embodiments, the alert may comprise any combination of an alert signal sent to a client device, an audible alarm emitted from the speaker 152 of the A/V recording and communication device 130, and an announcement emitted from the speaker 152 of the A/V recording and communication device 130.

[00160] Some of the present embodiments may comprise identifying a parcel within the area about the A/V recording and communication device 130. In some embodiments, identifying the parcel may comprise the camera 154 of the A/V recording and communication device 130 capturing an image of an identifying mark on the parcel. In various embodiments, the identifying mark may be, for example, a company logo or other identifying symbol. The identifying mark on the parcel may be compared with a plurality of identifying marks in a database. If a match is found, the parcel may be identified as originating with the sender

associated with the matching identifying mark. In other embodiments, the identifying mark may be, for example, a barcode, a matrix code, a bokode, etc. In some embodiments, RFID (or other similar technology) may be used to identify a parcel.

[00161] Figure 23 illustrates an example embodiment of a process for deterring parcel theft with an A/V recording and communication device according to various aspects of the present disclosure. At block B350, the process may determine that a parcel has been left within an area about an A/V recording and communication device, such as the A/V recording and communication device 130 described above. The present embodiments encompass any method of determining that a parcel has been left within an area about an A/V recording and communication device, including any of the examples described above. The present embodiments are not, however, limited to these examples, which are provided for illustration only.

[00162] With further reference to Figure 23, at block B352, after the parcel has been left within the area about the A/V recording and communication device 130, the process may detect a person within the area about the A/V recording and communication device 130. The detection of the person within the area about the A/V recording and communication device 130 may be according to any of the processes described herein, such as, for example, comparing video frames recorded by the camera 154 of the A/V recording and communication device 130.

[00163] With further reference to Figure 23, at block B354 the process may record, with the camera 154 of the A/V recording and communication device 130, video images of the person within the area about the A/V recording and communication device 130. At block B356, the process may emit an alert from the speaker 152 of the A/V recording and communication device 130. The alert may comprise an audible alarm and/or an announcement, similar to the example embodiments described above.

[00164] In some of the present embodiments, the processes described above, including the processes described with reference to Figures 14 and 23, may be performed automatically when a parcel is detected within the area about the A/V recording and communication device 130. In other embodiments, processes similar to those described above may only be performed in response to a user command. For example, one aspect of the present embodiments may provide an option to a user for enabling and/or disabling a parcel protection feature or mode. An option to enable/disable the parcel protection mode may be presented to the user, for example, through a

graphical user interface (GUI) of an application executing on the user's client device 114. The GUI may also provide other options (e.g., receiving motion alerts, etc.), in addition to the parcel protection mode, for the user to select or unselect (e.g., to enable or disable).

[00165] In one example embodiment, the user may manually enable parcel protection mode in response to a notification that a parcel has been delivered. For example, with reference to Figure 24, at block B360 the user may receive a notification that a parcel has been delivered (e.g., left within the field of view of the camera 154). The notification may be received in several different ways. For example, the parcel carrier may press the front button 148 of the A/V recording and communication device 130, thereby initiating a call to the user's client device 114. The user may answer the call and speak to the parcel carrier, who may inform the user that his or her parcel has been delivered and left in the area about the A/V recording and communication device 130. In another example, the call to the user's client device 114 may be initiated automatically by the A/V recording and communication device 130 in response to detecting the presence of the parcel carrier, such as by using the camera 154 for motion detection and/or a separate motion sensor. The user may then view live streaming video of the parcel delivery event (or subsequently view recorded video of the parcel delivery event) and thereby be informed of the parcel delivery without actually speaking to the parcel carrier. In yet another example, the A/V recording and communication device 130 may detect the delivery of the parcel, for example using any of the techniques described herein, and may then send a notification to the user's client device 114, for example in the form of an alert (e.g., a push notification).

[00166] Regardless of the form of notification, and with further reference to Figure 24, at block B362 the user may manually enable parcel protection mode, such as, for example, using an application executing on the user's client device 114, as described above. In some embodiments, the option to enable parcel protection mode may be presented to the user in conjunction with the notification sent to the user's client device 114, for example in the form of an alert (e.g., a push notification). If the user enables parcel protection mode, then at block B364 the process of Figure 24 advances to block B302 of Figure 14 and/or block B352 of Figure 23. In some embodiments, however, if the user declines to enable parcel protection mode, then parcel protection mode may remain inactive, and the operations shown in blocks B302-B306 of Figure 14 and blocks B362-B366 of Figure 23 would not be performed.

[00167] As described above, a user may disable the parcel protection mode manually in the same manner that the user enables this feature/mode (e.g., through a GUI of an application that is associated with the A/V recording and communication device). Some of the present embodiments may also disable the parcel protection mode automatically (e.g., without a user's intervention). Some such embodiments may disable the parcel protection mode when a parcel is removed from an area about an A/V recording and communication device by an authorized person (e.g., the homeowner, a friend or family member of the homeowner, or any other person authorized by the homeowner). Different embodiments may realize that a parcel is removed (e.g., from the field of view of a camera of an A/V recording and communication device) by an authorized person through different methods. Some aspects of the present embodiments may verify a person as an authorized person by authenticating the person's biometrics. As an example, one aspect of the present embodiments identifies the person's face (e.g., by performing a face recognition process, as described above) and compares the identification data with one or more databases that contain authorized persons' identification data.

[00168] Some of the present embodiments may disable a parcel protection mode when these embodiments determine that an authorized user is at, or within a threshold vicinity of, the location of the parcel. Some embodiments make such a determination by comparing a current location of the authorized user (e.g., by locating a client device that the user carries) and the location of the parcel. Some other embodiments may determine that a parcel is picked up by an authorized person when the parcel moves in a specific direction (e.g., toward the house instead of away from the house). Some of the present embodiments may realize that the parcel is being moved toward the house, e.g., by comparing a sequence of video images of the moving parcel captured by a camera of the A/V recording and communication device. Some other embodiments may use an AIDC module (e.g., an RFID reader) of the A/V recording and communication device to determine the direction of movement of a parcel (e.g., when the parcel includes a barcode, a matrix code, an RFID tag, etc.).

[00169] In any of the present embodiments, various aspects of methods may be performed locally, e.g. by one or more components of the A/V recording and communication device 130, and/or remotely, e.g. by one or more network devices, such as the server 118 and/or the backend API 120, for example. For example, the processor 160 of the A/V recording and communication device 130 may perform various aspects such as, but not limited to, comparing video frames

recorded by the camera 154 of the A/V recording and communication device 130 to determine whether a parcel has been left within the area about the A/V recording and communication device 130 and/or that the parcel has been removed from the area about the A/V recording and communication device 130.

[00170] Many of the present embodiments have been described with reference to persons detected by, or present in the area about, the A/V recording and communication device 130. The present embodiments are not limited, however, to scenarios involving humans. For example, the present embodiments contemplate that a parcel thief need not be a human. A parcel theft bot or drone, for example, may be encompassed by any of the present embodiments. For example, in a process similar to any process described herein, after a parcel has been left within the area about the A/V recording and communication device 130, the process may detect a parcel theft bot or drone within the area about the A/V recording and communication device 130. The process may also record, with the camera 154 of the A/V recording and communication device 130, video images of the parcel theft bot or drone within the area about the A/V recording and communication device 130.

[00171] Any of the present embodiments may comprise a designated parcel delivery area. For example, a user may designate a particular area about the A/V recording and communication device 130 as a parcel delivery area. The parcel delivery area may be demarcated in any suitable manner, such as with markings and/or text provided on the pavement and/or adjacent wall(s). Processes of determining whether a parcel has been left within the area about the A/V recording and communication device 130 and/or determining whether the parcel has been removed from the area about the A/V recording and communication device 130 may comprise determining whether an object has been left within and/or removed from the designated parcel delivery area. The user may, in some embodiments, direct or aim the camera 154 of the A/V recording and communication device 130 toward the designated parcel delivery area to facilitate determining whether an object has been left within and/or removed from the designated parcel delivery area.

[00172] As described above, the present embodiments advantageously leverage the functionality of A/V recording and communication devices to deter parcel theft and/or to identify and apprehend parcel thieves. Various embodiments may determine when one or more parcels have been left within and/or removed from the area about the A/V recording and communication device. When one or more parcels are removed from the area about the A/V recording and

communication device, various embodiments may determine whether such removal was authorized and, if desired, generate an alert. The user may then determine what, if anything, to do in response to the alert, such as notifying law enforcement and/or sharing video footage of the parcel theft, such as via social media.

[00173] Figure 25 is a functional block diagram of a client device 800 on which the present embodiments may be implemented according to various aspects of the present disclosure. The user's client device 114 described with reference to Figure 1 may include some or all of the components and/or functionality of the client device 800. The client device 800 may comprise, for example, a smartphone.

[00174] With reference to Figure 25, the client device 800 includes a processor 802, a memory 804, a user interface 806, a communication module 808, and a dataport 810. These components are communicatively coupled together by an interconnect bus 812. The processor 802 may include any processor used in smartphones and/or portable computing devices, such as an ARM processor (a processor based on the RISC (reduced instruction set computer) architecture developed by Advanced RISC Machines (ARM).). In some embodiments, the processor 802 may include one or more other processors, such as one or more conventional microprocessors, and/or one or more supplementary co-processors, such as math co-processors.

[00175] The memory 804 may include both operating memory, such as random access memory (RAM), as well as data storage, such as read-only memory (ROM), hard drives, flash memory, or any other suitable memory/storage element. The memory 804 may include removable memory elements, such as a CompactFlash card, a MultiMediaCard (MMC), and/or a Secure Digital (SD) card. In some embodiments, the memory 804 may comprise a combination of magnetic, optical, and/or semiconductor memory, and may include, for example, RAM, ROM, flash drive, and/or a hard disk or drive. The processor 802 and the memory 804 each may be, for example, located entirely within a single device, or may be connected to each other by a communication medium, such as a USB port, a serial port cable, a coaxial cable, an Ethernet-type cable, a telephone line, a radio frequency transceiver, or other similar wireless or wired medium or combination of the foregoing. For example, the processor 802 may be connected to the memory 804 via the dataport 810.

[00176] The user interface 806 may include any user interface or presentation elements suitable for a smartphone and/or a portable computing device, such as a keypad, a display screen,

a touchscreen, a microphone, and a speaker. The communication module 808 is configured to handle communication links between the client device 800 and other, external devices or receivers, and to route incoming/outgoing data appropriately. For example, inbound data from the dataport 810 may be routed through the communication module 808 before being directed to the processor 802, and outbound data from the processor 802 may be routed through the communication module 808 before being directed to the dataport 810. The communication module 808 may include one or more transceiver modules capable of transmitting and receiving data, and using, for example, one or more protocols and/or technologies, such as GSM, UMTS (3GSM), IS-95 (CDMA one), IS-2000 (CDMA 2000), LTE, FDMA, TDMA, W-CDMA, CDMA, OFDMA, Wi-Fi, WiMAX, or any other protocol and/or technology.

[00177] The dataport 810 may be any type of connector used for physically interfacing with a smartphone and/or a portable computing device, such as a mini-USB port or an IPHONE®/IPOD® 30-pin connector or LIGHTNING® connector. In other embodiments, the dataport 810 may include multiple communication channels for simultaneous communication with, for example, other processors, servers, and/or client terminals.

[00178] The memory 804 may store instructions for communicating with other systems, such as a computer. The memory 804 may store, for example, a program (e.g., computer program code) adapted to direct the processor 802 in accordance with the present embodiments. The instructions also may include program elements, such as an operating system. While execution of sequences of instructions in the program causes the processor 802 to perform the process steps described herein, hard-wired circuitry may be used in place of, or in combination with, software/firmware instructions for implementation of the processes of the present embodiments. Thus, the present embodiments are not limited to any specific combination of hardware and software.

[00179] Figure 26 is a functional block diagram of a general-purpose computing system on which the present embodiments may be implemented according to various aspects of the present disclosure. The computer system 900 may be embodied in at least one of a personal computer (also referred to as a desktop computer) 900A, a portable computer (also referred to as a laptop or notebook computer) 900B, and/or a server 900C. A server is a computer program and/or a machine that waits for requests from other machines or software (clients) and responds to them. A server typically processes data. The purpose of a server is to share data and/or

hardware and/or software resources among clients. This architecture is called the client–server model. The clients may run on the same computer or may connect to the server over a network. Examples of computing servers include database servers, file servers, mail servers, print servers, web servers, game servers, and application servers. The term server may be construed broadly to include any computerized process that shares a resource to one or more client processes.

[00180] The computer system 900 may execute at least some of the operations described above. The computer system 900 may include at least one processor 910, memory 920, at least one storage device 930, and input/output (I/O) devices 940. Some or all of the components 910, 920, 930, 940 may be interconnected via a system bus 950. The processor 910 may be single- or multi-threaded and may have one or more cores. The processor 910 may execute instructions, such as those stored in the memory 920 and/or in the storage device 930. Information may be received and output using one or more I/O devices 940.

[00181] The memory 920 may store information, and may be a computer-readable medium, such as volatile or non-volatile memory. The storage device(s) 930 may provide storage for the system 900, and may be a computer-readable medium. In various aspects, the storage device(s) 930 may be a flash memory device, a hard disk device, an optical disk device, a tape device, or any other type of storage device.

[00182] The I/O devices 940 may provide input/output operations for the system 900. The I/O devices 940 may include a keyboard, a pointing device, and/or a microphone. The I/O devices 940 may further include a display unit for displaying graphical user interfaces, a speaker, and/or a printer. External data may be stored in one or more accessible external databases 960.

[00183] The features of the present embodiments described herein may be implemented in digital electronic circuitry, and/or in computer hardware, firmware, software, and/or in combinations thereof. Features of the present embodiments may be implemented in a computer program product tangibly embodied in an information carrier, such as a machine-readable storage device, and/or in a propagated signal, for execution by a programmable processor. Embodiments of the present method steps may be performed by a programmable processor executing a program of instructions to perform functions of the described implementations by operating on input data and generating output.

[00184] The features of the present embodiments described herein may be implemented in one or more computer programs that are executable on a programmable system including at least one programmable processor coupled to receive data and/or instructions from, and to transmit data and/or instructions to, a data storage system, at least one input device, and at least one output device. A computer program may include a set of instructions that may be used, directly or indirectly, in a computer to perform a certain activity or bring about a certain result. A computer program may be written in any form of programming language, including compiled or interpreted languages, and it may be deployed in any form, including as a stand-alone program or as a module, component, subroutine, or other unit suitable for use in a computing environment.

[00185] Suitable processors for the execution of a program of instructions may include, for example, both general and special purpose processors, and/or the sole processor or one of multiple processors of any kind of computer. Generally, a processor may receive instructions and/or data from a read only memory (ROM), or a random access memory (RAM), or both. Such a computer may include a processor for executing instructions and one or more memories for storing instructions and/or data.

[00186] Generally, a computer may also include, or be operatively coupled to communicate with, one or more mass storage devices for storing data files. Such devices include magnetic disks, such as internal hard disks and/or removable disks, magneto-optical disks, and/or optical disks. Storage devices suitable for tangibly embodying computer program instructions and/or data may include all forms of non-volatile memory, including for example semiconductor memory devices, such as EPROM, EEPROM, and flash memory devices, magnetic disks such as internal hard disks and removable disks, magneto-optical disks, and CD-ROM and DVD-ROM disks. The processor and the memory may be supplemented by, or incorporated in, one or more ASICs (application-specific integrated circuits).

[00187] To provide for interaction with a user, the features of the present embodiments may be implemented on a computer having a display device, such as an LCD (liquid crystal display) monitor, for displaying information to the user. The computer may further include a keyboard, a pointing device, such as a mouse or a trackball, and/or a touchscreen by which the user may provide input to the computer.

[00188] The features of the present embodiments may be implemented in a computer system that includes a back-end component, such as a data server, and/or that includes a

middleware component, such as an application server or an Internet server, and/or that includes a front-end component, such as a client computer having a graphical user interface (GUI) and/or an Internet browser, or any combination of these. The components of the system may be connected by any form or medium of digital data communication, such as a communication network. Examples of communication networks may include, for example, a LAN (local area network), a WAN (wide area network), and/or the computers and networks forming the Internet.

[00189] The computer system may include clients and servers. A client and server may be remote from each other and interact through a network, such as those described herein. The relationship of client and server may arise by virtue of computer programs running on the respective computers and having a client-server relationship to each other.

[00190] The above description presents the best mode contemplated for carrying out the present embodiments, and of the manner and process of practicing them, in such full, clear, concise, and exact terms as to enable any person skilled in the art to which they pertain to practice these embodiments. The present embodiments are, however, susceptible to modifications and alternate constructions from those discussed above that are fully equivalent. Consequently, the present invention is not limited to the particular embodiments disclosed. On the contrary, the present invention covers all modifications and alternate constructions coming within the spirit and scope of the present disclosure. For example, the steps in the processes described herein need not be performed in the same order as they have been presented, and may be performed in any order(s). Further, steps that have been presented as being performed separately may in alternative embodiments be performed concurrently. Likewise, steps that have been presented as being performed concurrently may in alternative embodiments be performed separately.

WHAT IS CLAIMED IS:

1. A method for an audio/video (A/V) recording and communication device, the device including a camera, the method comprising:

determining that a parcel has been left within an area about the A/V recording and communication device;

determining that the parcel has been removed from the area about the A/V recording and communication device;

determining whether removal of the parcel from the area about the A/V recording and communication device was authorized; and

when the removal of the parcel from the area about the A/V recording and communication device is determined to have been unauthorized, generating an alert.

2. The method of Claim 1, wherein determining that the parcel has been left within the area about the A/V recording and communication device comprises comparing video frames recorded by the camera of the A/V recording and communication device.

3. The method of Claim 1, wherein determining that the parcel has been left in the area about the A/V recording and communication device comprises receiving information from a carrier that delivered the parcel.

4. The method of Claim 1, wherein determining that the parcel has been left within the area about the A/V recording and communication device comprises automatic identification and data capture (AIDC).

5. The method of Claim 4, wherein the AIDC comprises at least one of a barcode, a matrix code, a bokode, and radio frequency identification (RFID).

6. The method of Claim 1, wherein determining that the parcel has been removed from the area about the A/V recording and communication device comprises comparing video frames recorded by the camera of the A/V recording and communication device.

7. The method of Claim 1, wherein determining that the parcel has been removed from the area about the A/V recording and communication device comprises automatic identification and data capture (AIDC).

8. The method of Claim 7, wherein the AIDC comprises radio frequency identification (RFID).

9. The method of Claim 1, wherein determining whether removal of the parcel from the area about the A/V recording and communication device was authorized comprises detecting a direction of movement of the parcel.

10. The method of Claim 1, wherein determining whether removal of the parcel from the area about the A/V recording and communication device was authorized comprises automatic identification and data capture (AIDC).

11. The method of Claim 10, wherein the AIDC comprises at least one of a barcode, a matrix code, a bokode, radio frequency identification (RFID), a smart card, a magnetic stripe, optical character recognition (OCR), biometrics, voice recognition, facial recognition, three-dimensional facial recognition, and skin texture analysis.

12. The method of Claim 10, further comprising comparing information received through the AIDC to information about one or more persons.

13. The method of Claim 12, wherein the one or more persons comprise at least one perpetrator of one or more parcel thefts.

14. The method of Claim 13, wherein the one or more parcel thefts occurred within a defined radius about the A/V recording and communication device.

15. The method of Claim 1, wherein the alert comprises an alert signal sent to a client device.

16. The method of Claim 1, wherein the alert comprises an audible alarm emitted from a speaker of the A/V recording and communication device.

17. The method of Claim 1, wherein the alert comprises an announcement emitted from a speaker of the A/V recording and communication device, the announcement comprising a warning that the area about the A/V recording and communication device is being recorded.

18. The method of Claim 1, further comprising identifying the parcel.

19. The method of Claim 18, wherein identifying the parcel comprises the camera of the A/V recording and communication device capturing an image of an identifying mark on the parcel.

20. A method for an audio/video (A/V) recording and communication device, the device including a camera, the method comprising:

determining that a parcel has been left within an area about the A/V recording and communication device;

after the parcel has been left within the area about the A/V recording and communication device, detecting a person within the area about the A/V recording and communication device;

recording, with the camera of the A/V recording and communication device, video images of the person within the area about the A/V recording and communication device; and

emitting an alert from the speaker of the A/V recording and communication device.

21. The method of Claim 20, wherein the alert comprises an audible alarm.

22. The method of Claim 20, wherein the alert comprises an announcement warning the detected person that he or she is being recorded.

23. A method for an audio/video (A/V) recording and communication device, the device including a camera, the method comprising:

determining that a parcel has been left within an area about the A/V recording and communication device, wherein determining that the parcel has been left within the area about the A/V recording and communication device comprises comparing video frames recorded by the camera of the A/V recording and communication device;

determining that the parcel has been removed from the area about the A/V recording and communication device, wherein determining that the parcel has been removed from the area about the A/V recording and communication device comprises comparing video frames recorded by the camera of the A/V recording and communication device;

determining whether removal of the parcel from the area about the A/V recording and communication device was authorized, wherein determining whether removal of the parcel from the area about the A/V recording and communication device was authorized comprises automatic identification and data capture (AIDC); and

when the removal of the parcel from the area about the A/V recording and communication device is determined to have been unauthorized, generating an alert.

24. The method of Claim 23, wherein the AIDC comprises at least one of radio frequency identification (RFID) and biometrics.

25. The method of Claim 23, wherein the AIDC comprises the camera of the A/V recording and communication device capturing an image of a person in the area about the A/V recording and communication device.

26. The method of Claim 25, wherein the image of the person comprises an image of the person's face.

27. The method of Claim 25, further comprising comparing the image of the person to at least one image of at least one other person.

28. The method of Claim 27, wherein the removal of the parcel from the area about the A/V recording and communication device is determined to have been unauthorized when there is a match between the image of the person captured by the camera of the A/V recording and communication device and the at least one image of the at least one other person.

29. A method for an audio/video (A/V) recording and communication device, the device including a processor and a camera, the device being communicatively connected to at least one network device, the method comprising:

determining that a parcel has been left within an area about the A/V recording and communication device, wherein determining that the parcel has been left within the area about the A/V recording and communication device comprises the processor of the A/V recording and communication device comparing video frames recorded by the camera of the A/V recording and communication device;

determining that the parcel has been removed from the area about the A/V recording and communication device, wherein determining that the parcel has been removed from the area about the A/V recording and communication device comprises the processor of the A/V recording and communication device comparing video frames recorded by the camera of the A/V recording and communication device;

determining whether removal of the parcel from the area about the A/V recording and communication device was authorized, wherein determining whether removal of the parcel from the area about the A/V recording and communication device was authorized comprises automatic identification and data capture (AIDC); and

when the removal of the parcel from the area about the A/V recording and communication device is determined to have been unauthorized, generating an alert.

30. The method of Claim 29, wherein the AIDC comprises at least one of radio frequency identification (RFID) and biometrics.

31. The method of Claim 29, wherein the AIDC comprises the camera of the A/V recording and communication device capturing an image of a person in the area about the A/V recording and communication device.

32. The method of Claim 31, wherein the image of the person comprises an image of the person's face.

33. The method of Claim 31, further comprising the at least one network device receiving the image of the person.

34. The method of Claim 33, further comprising the at least one network device comparing the image of the person to at least one image of at least one other person.

35. The method of Claim 34, wherein the removal of the parcel from the area about the A/V recording and communication device is determined to have been unauthorized when there is a match between the image of the person captured by the camera of the A/V recording and communication device and the at least one image of the at least one other person.

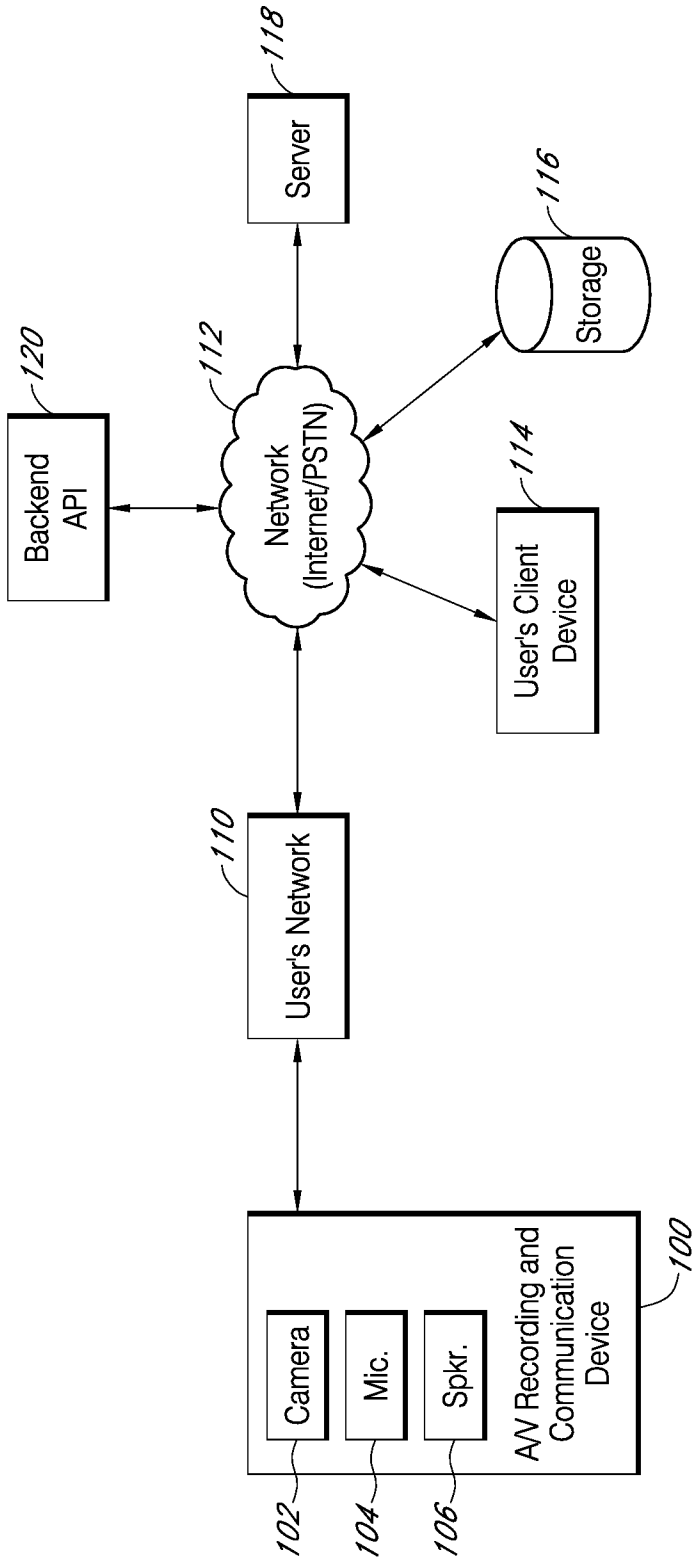
Server
118
Storage
116
Backend API
120
112
Network (Internet/PSTN)
User's Client Device
114
User's Network
110
A/V Recording and Communication Device
100
Camera
Mic.
Spkr.
102
104
106

FIG. 1

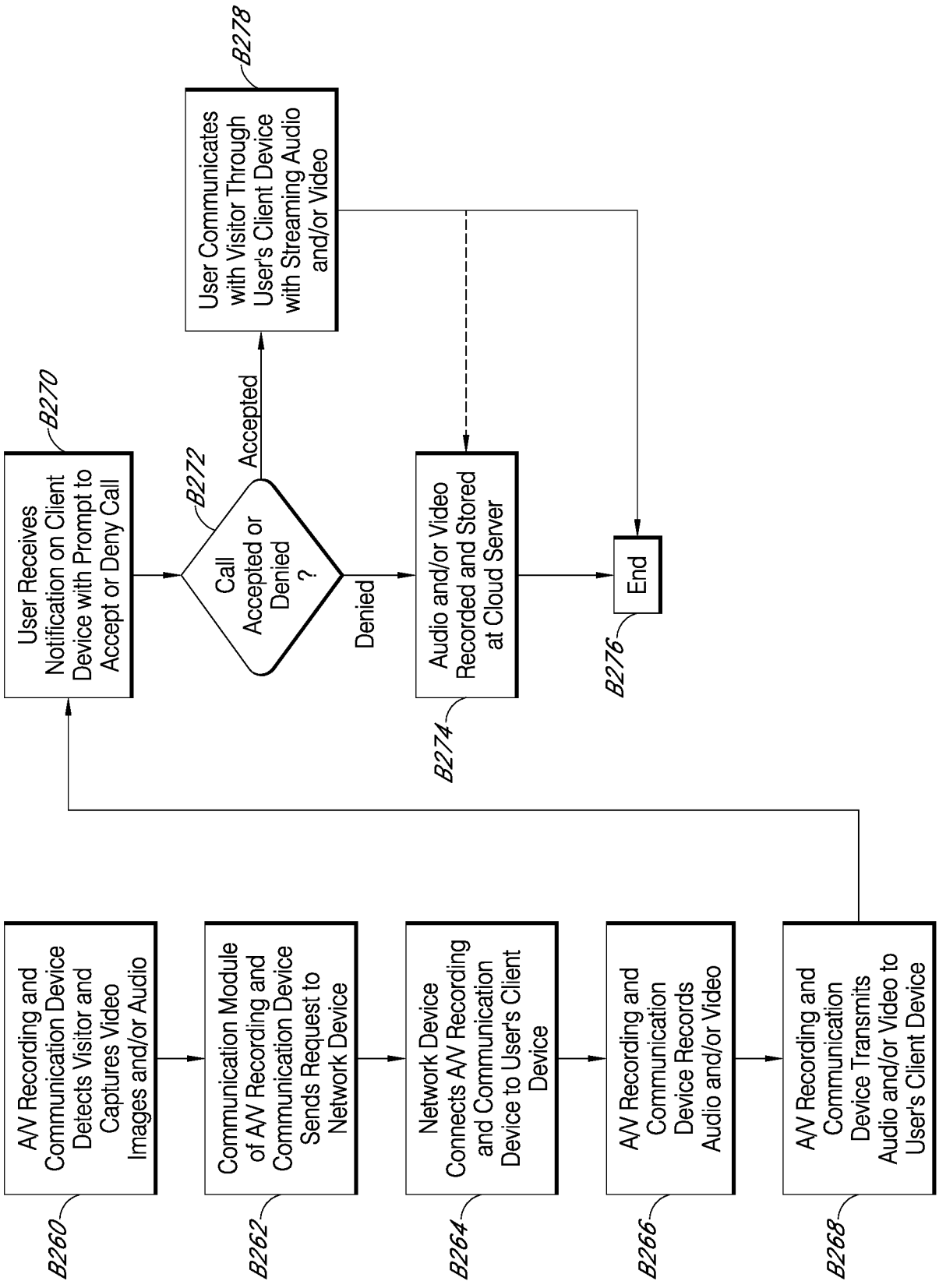
A/V Recording and Communication Device Detects Visitor and Captures Video Images and/or Audio
B260
Communication Module of A/V Recording and Communication Device Sends Request to Network Device
B262
Network Device Connects A/V Recording and Communication Device to User's Client Device
B264
A/V Recording and Communication Device Records Audio and/or Video
B266
A/V Recording and Communication Device Transmits Audio and/or Video to User's Client Device
B268
User Receives Notification on Client Device with Prompt to Accept or Deny Call
B270
Call Accepted or Denied ?
B272
Accepted
Denied
User Communicates with Visitor Through User's Client Device with Streaming Audio and/or Video
B278
Audio and/or Video Recorded and Stored at Cloud Server
B274
End
B276

FIG. 2

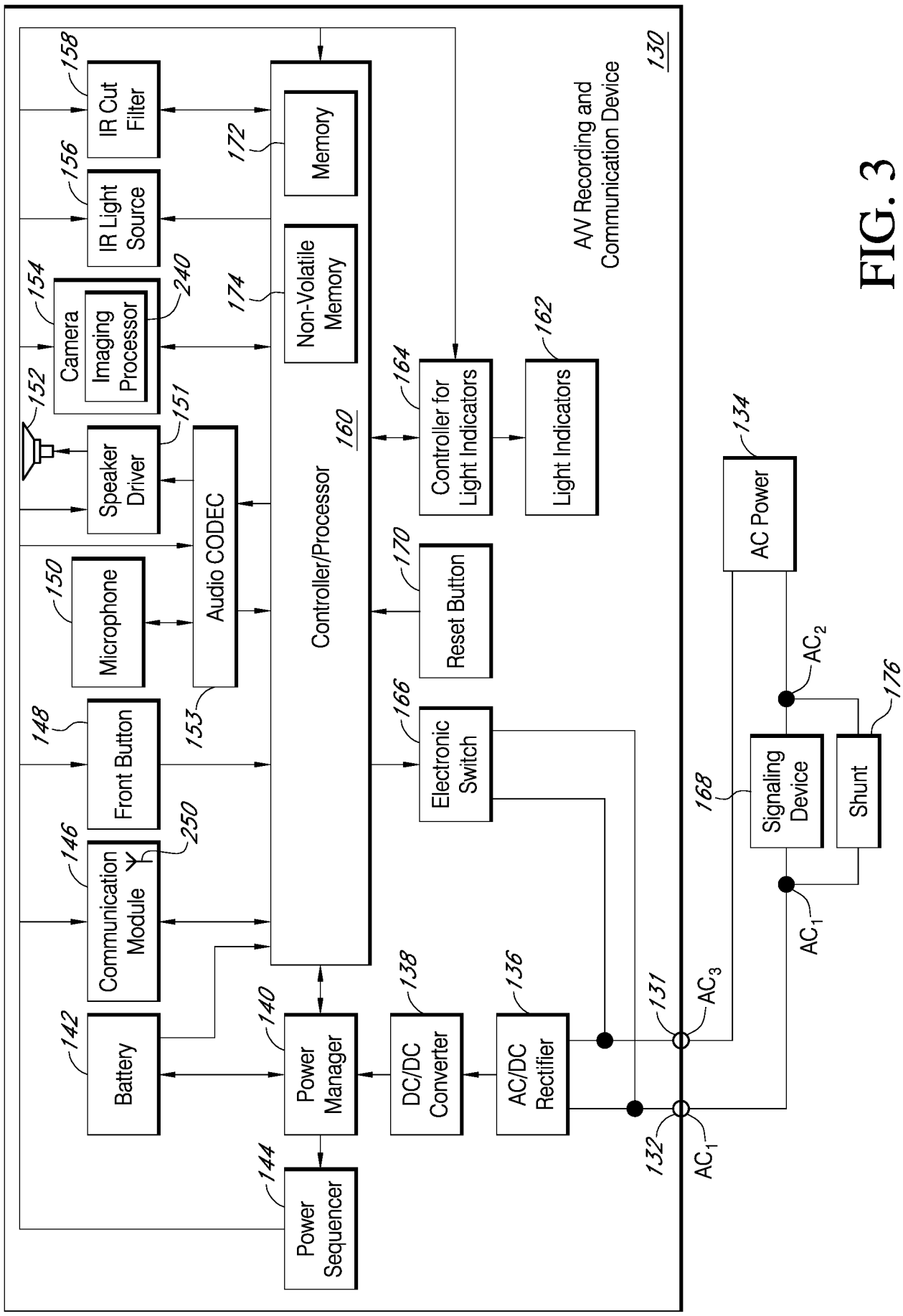
A/V Recording and Communication Device
130
Controller/Processor
160
Memory
172
Non-Volatile Memory
174
Camera
154
Imaging Processor
240
IR Cut Filter
158
IR Light Source
156
Speaker Driver
151
Audio CODEC
153
Microphone
150
Front Button
148
Communication Module
146
250
Battery
142
Power Manager
140
DC/DC Converter
138
AC/DC Rectifier
136
Power Sequencer
144
Controller for Light Indicators
164
Light Indicators
162
Reset Button
170
Electronic Switch
166
AC Power
134
Signaling Device
168
Shunt
176
131
132
AC1
AC2
AC3

FIG. 3

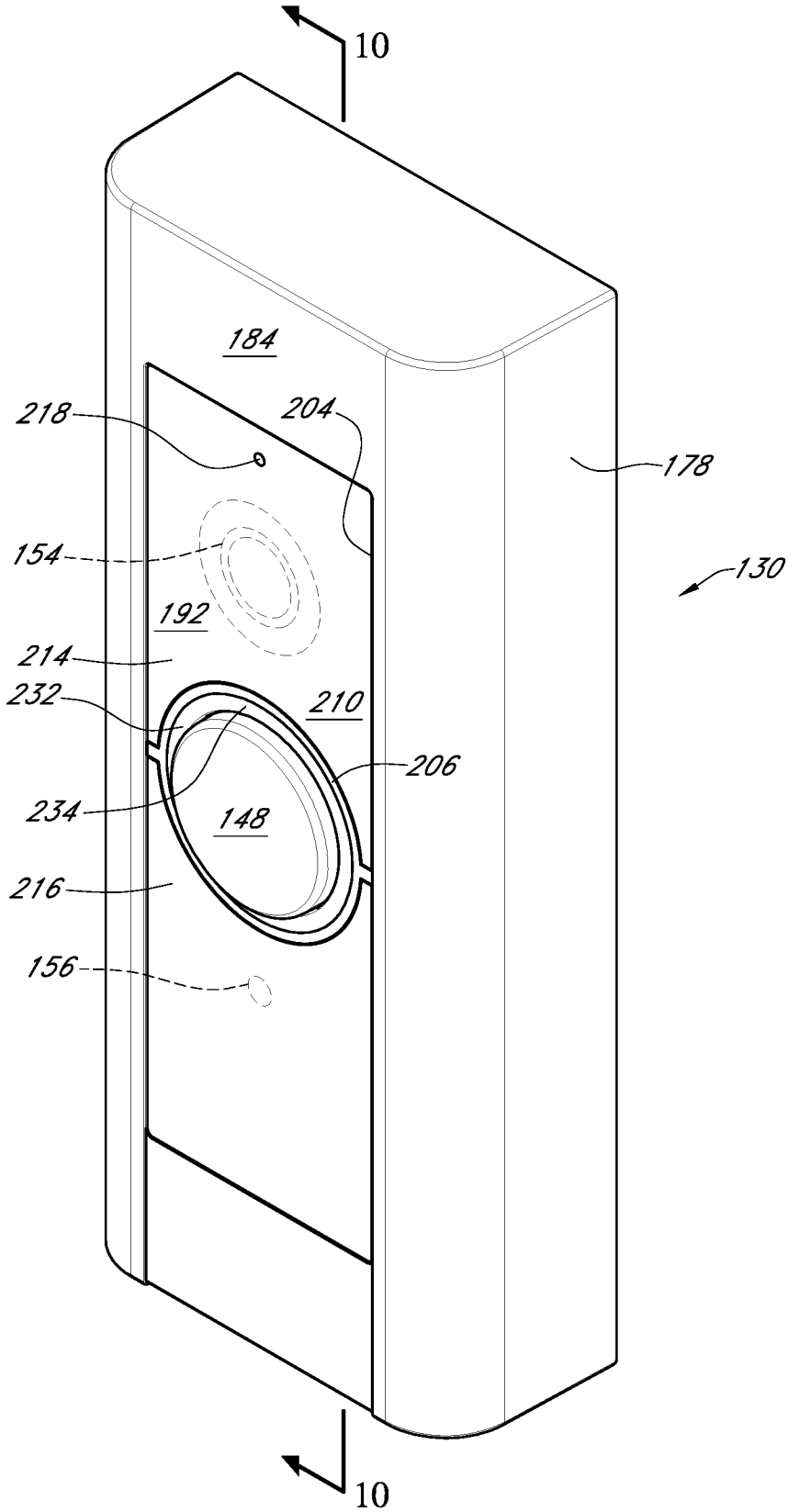

FIG. 4

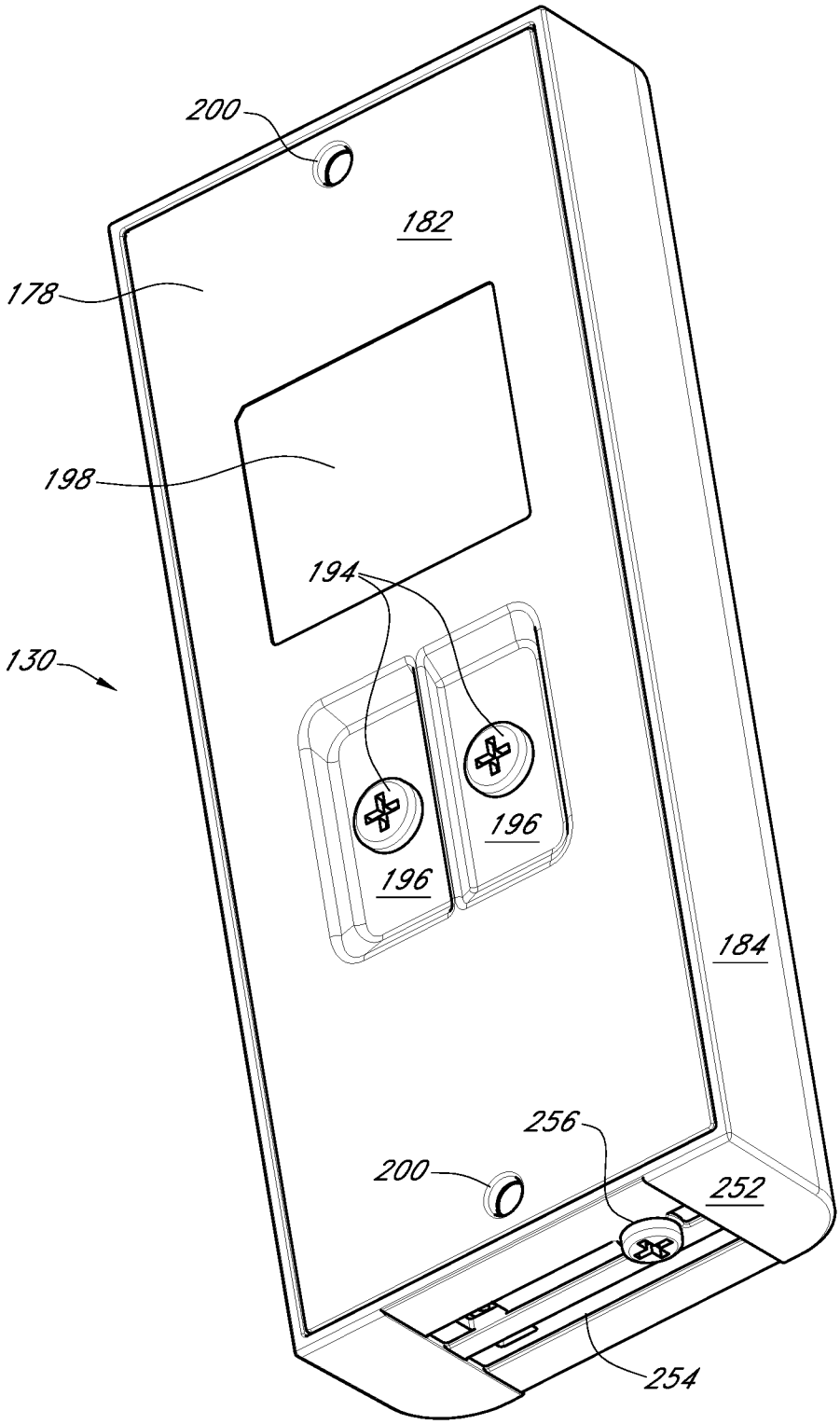

FIG. 5

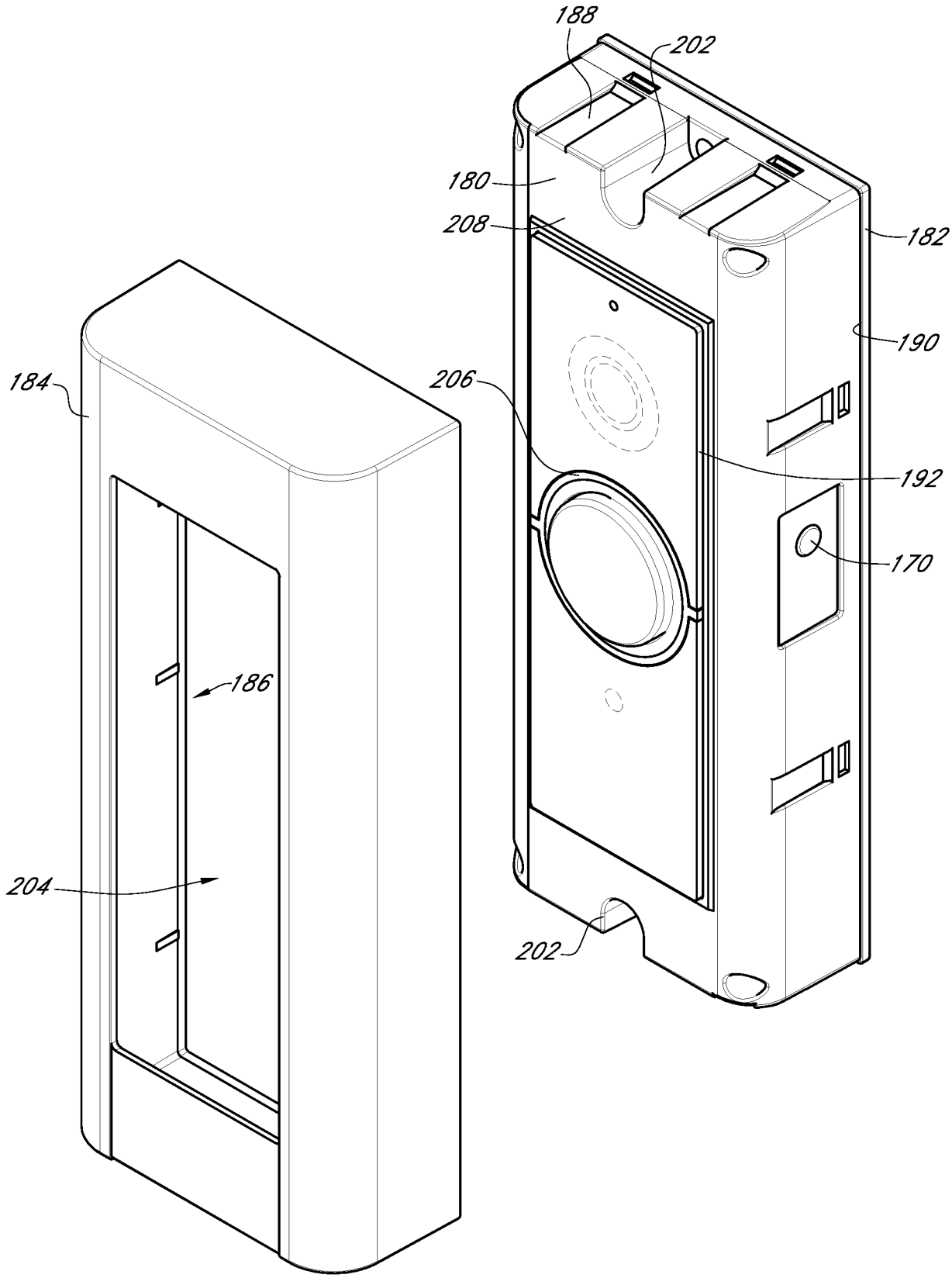

FIG. 6

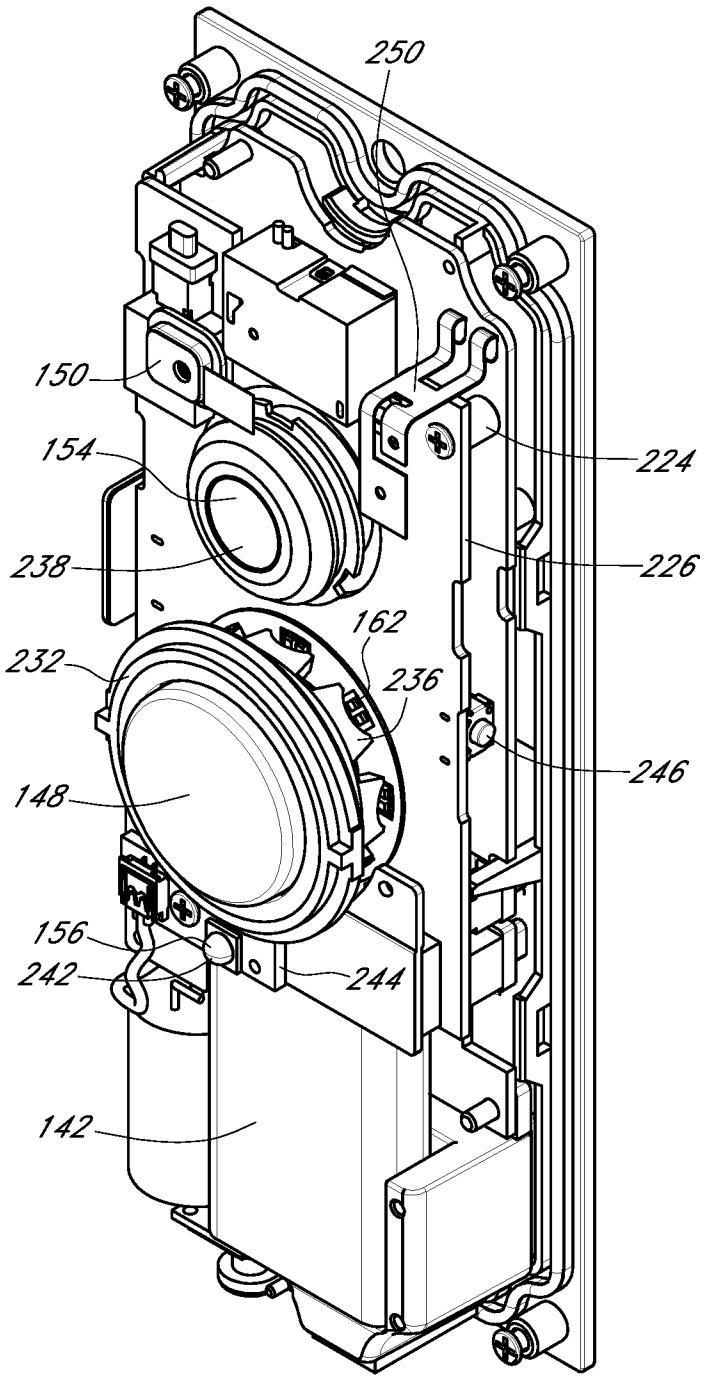

FIG. 7

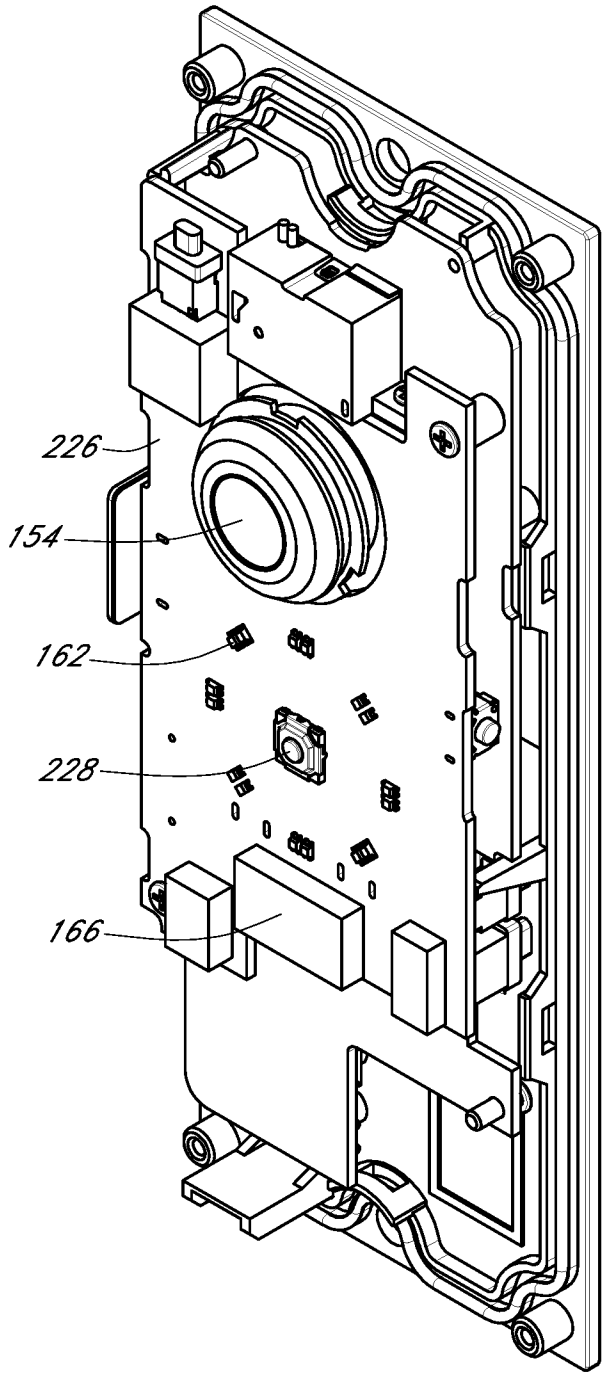

FIG. 8

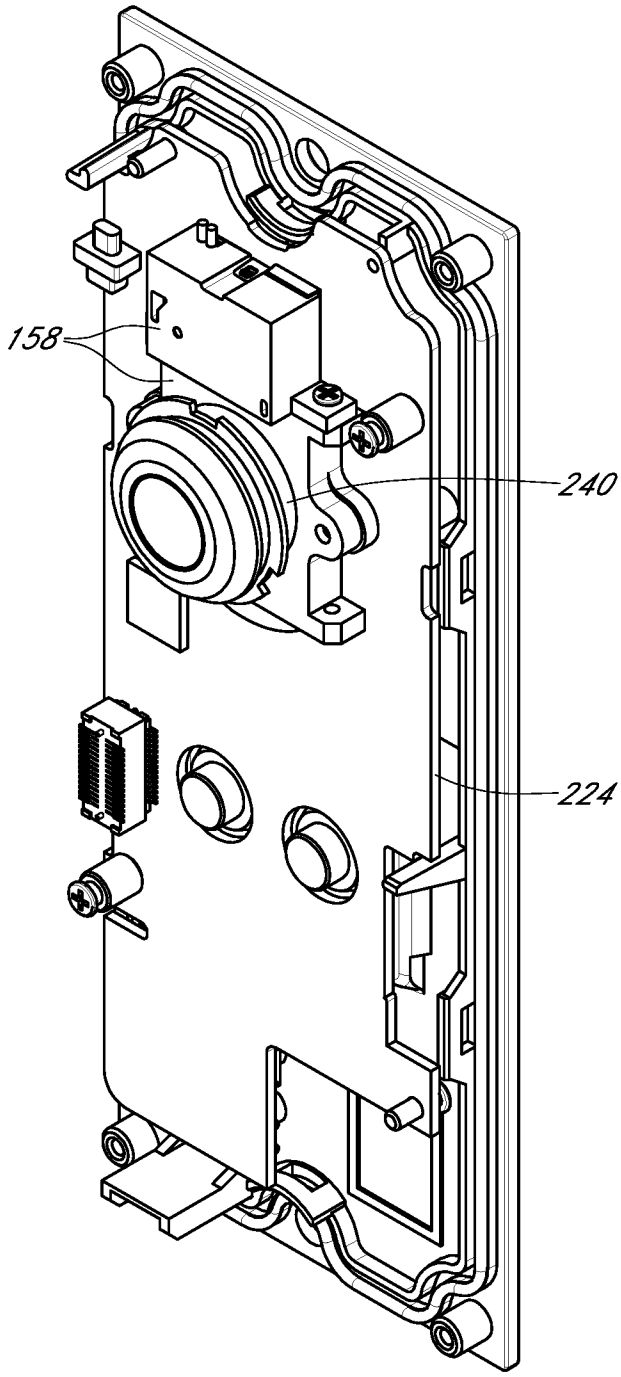

FIG. 9

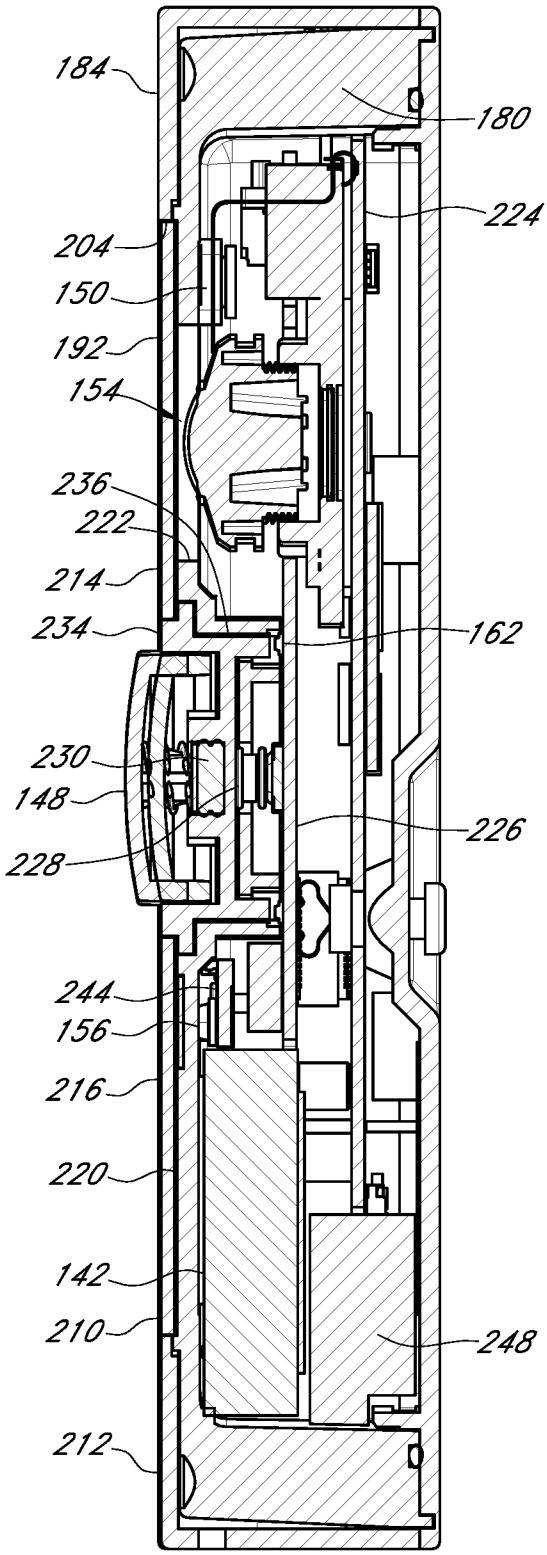
184
180
224
204
150
192
154
236
222
214
234
162
230
148
226
228
244
156
216
220
142
210
248
212

FIG. 10

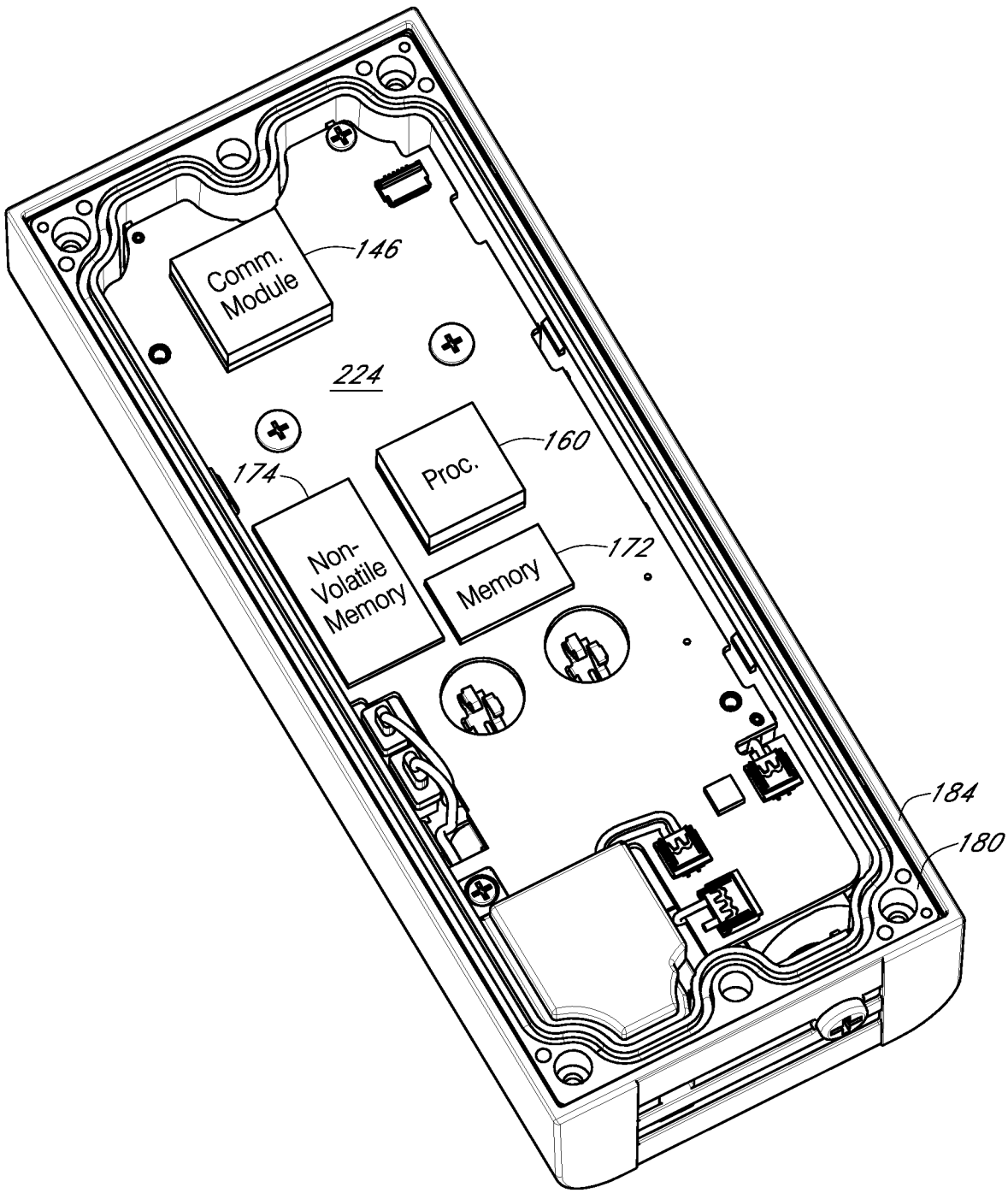
Comm. Module
146
224
Proc.
160
174
Non-Volatile Memory
Memory
172
184
180

FIG. 11

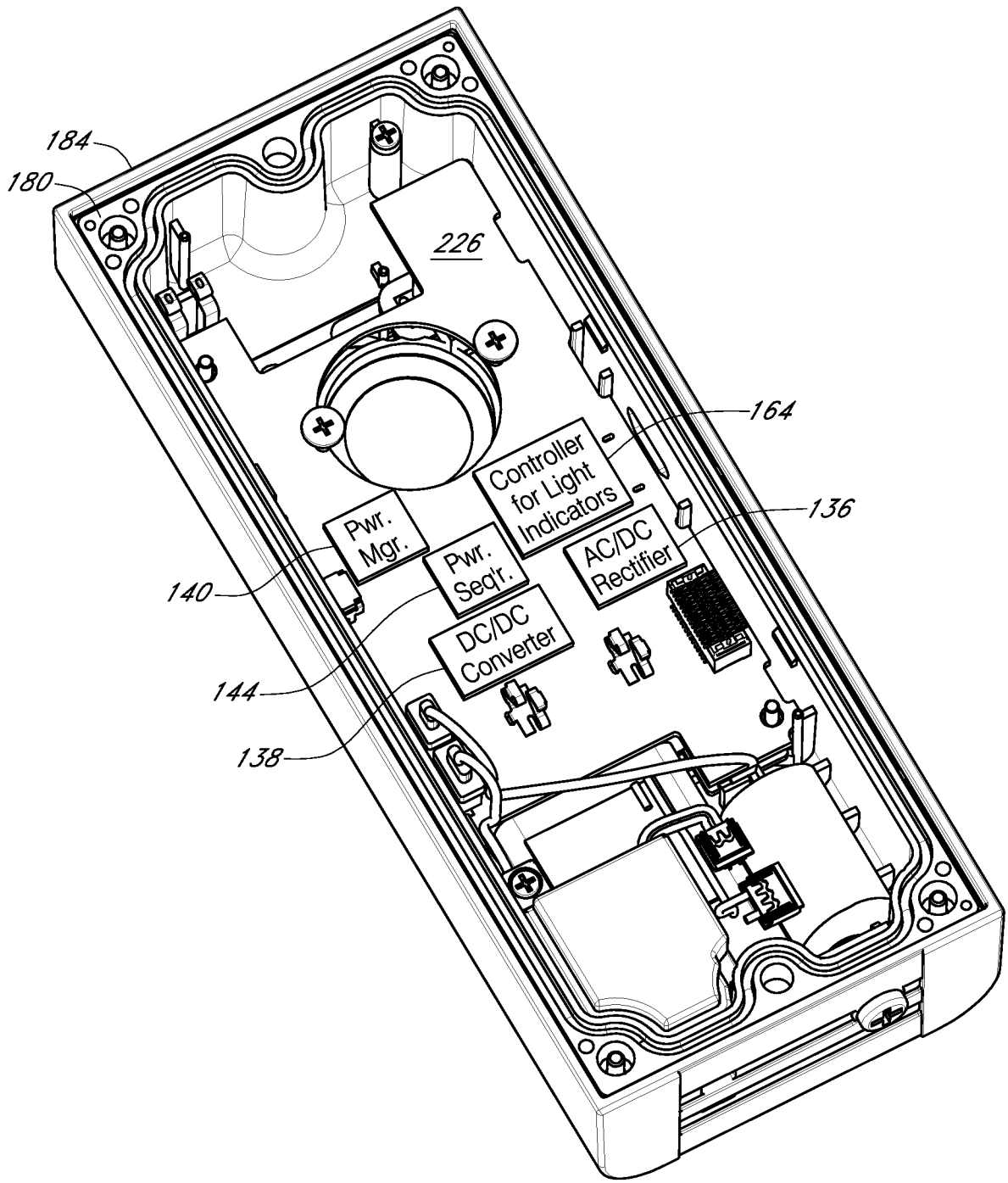
184
180
226
164
Controller for Light Indicators
136
Pwr. Mgr.
Pwr. Seq'r.
AC/DC Rectifier
140
DC/DC Converter
144
138

FIG. 12

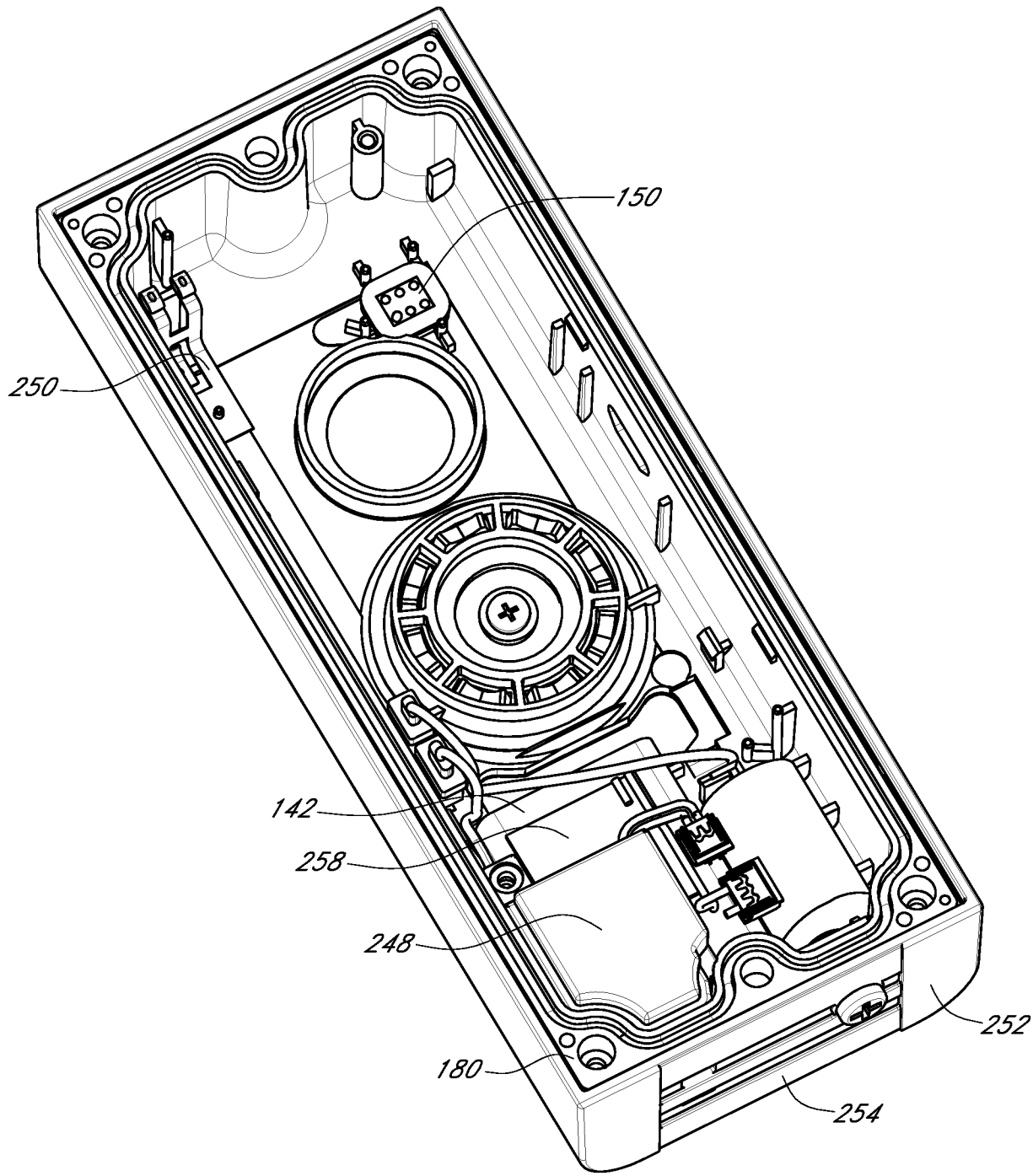

FIG. 13

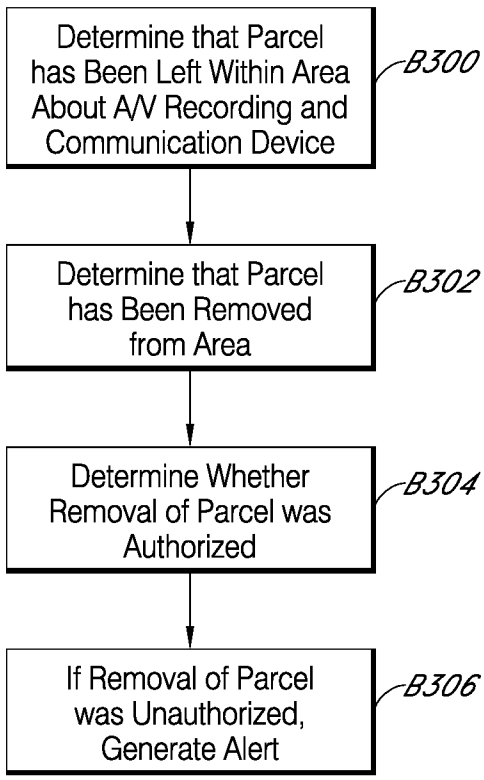
Determine that Parcel has Been Left Within Area About A/V Recording and Communication Device
B300
Determine that Parcel has Been Removed from Area
B302
Determine Whether Removal of Parcel was Authorized
B304
If Removal of Parcel was Unauthorized, Generate Alert
B306

FIG. 14

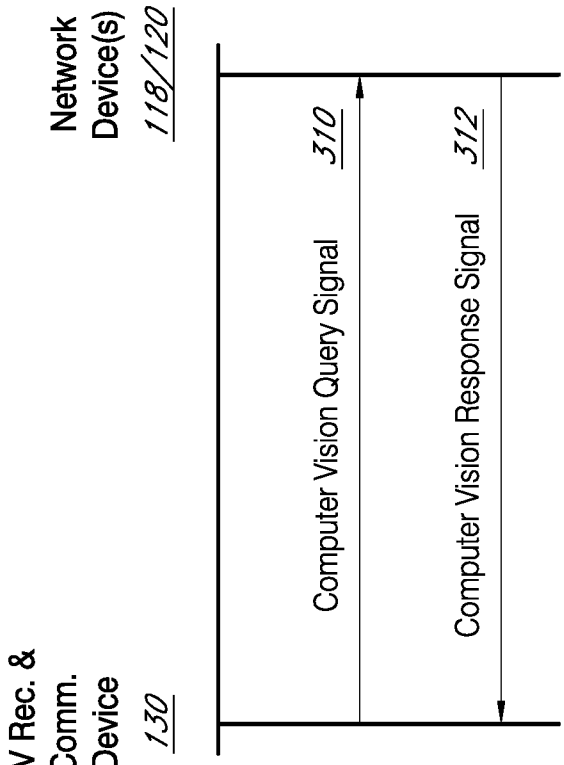
A/V Rec. & Comm. Device
130
Network Device(s)
118/120
Computer Vision Query Signal
310
Computer Vision Response Signal
312

FIG. 15

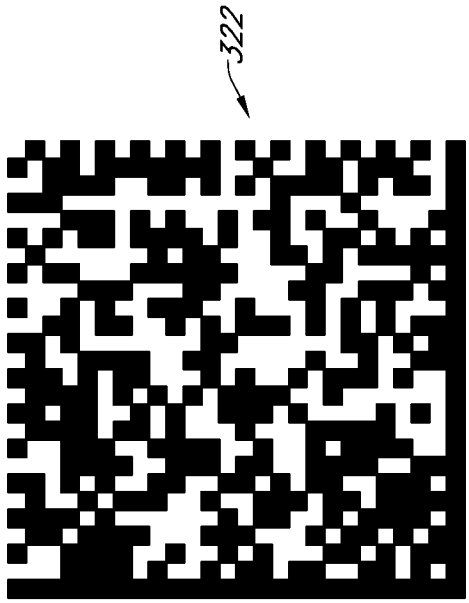

FIG. 17

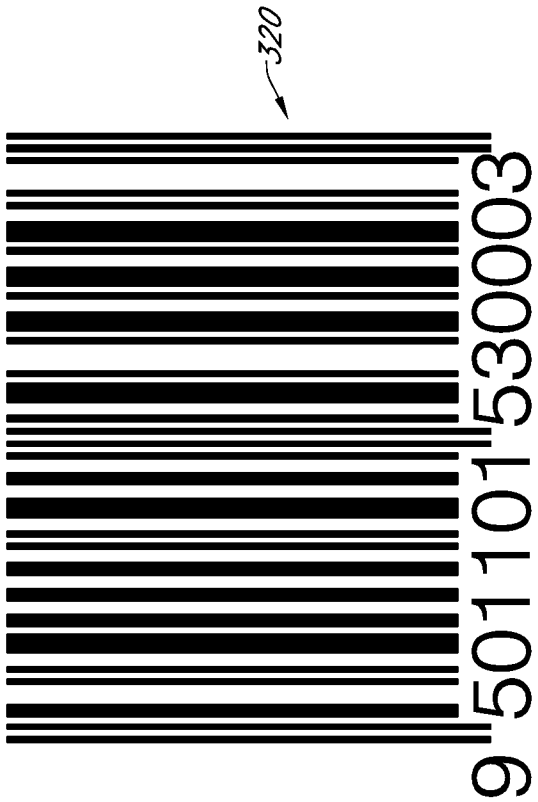

FIG. 16

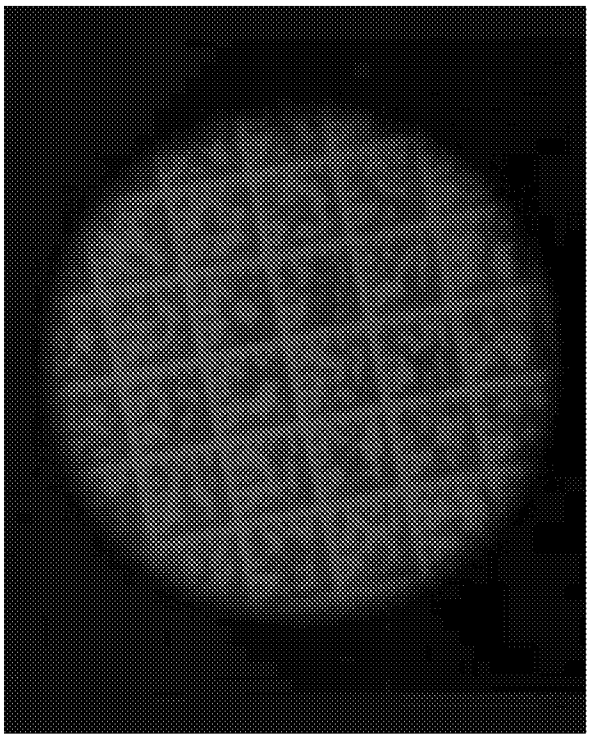

FIG. 18

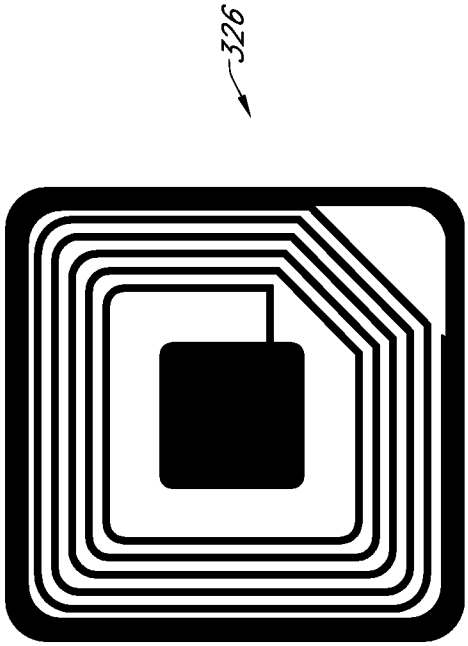

FIG. 19

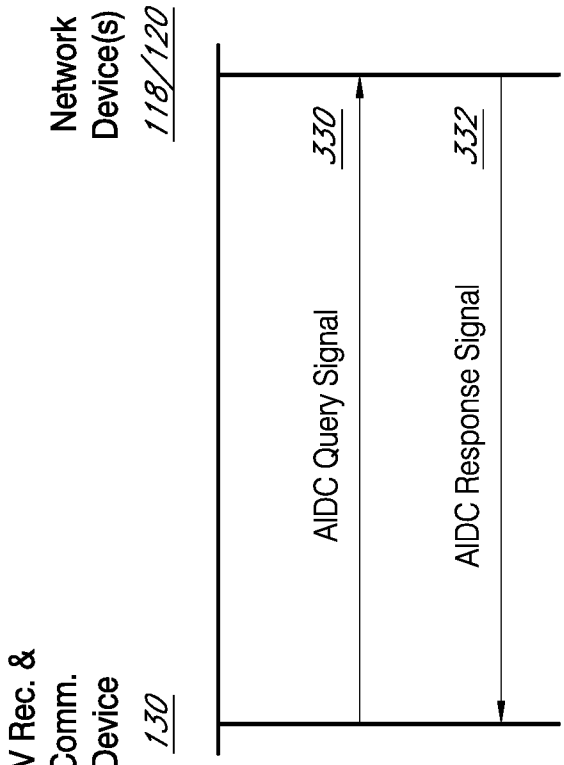
A/V Rec. & Comm. Device
130
Network Device(s)
118/120
AIDC Query Signal
330
AIDC Response Signal
332

FIG. 20

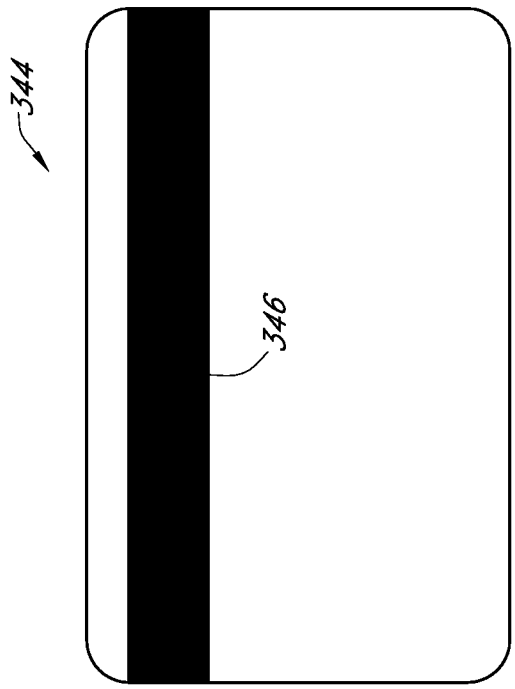

FIG. 22

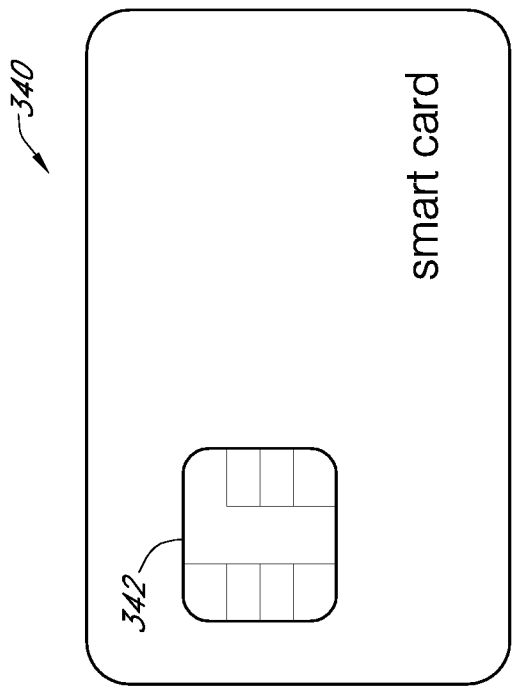

FIG. 21

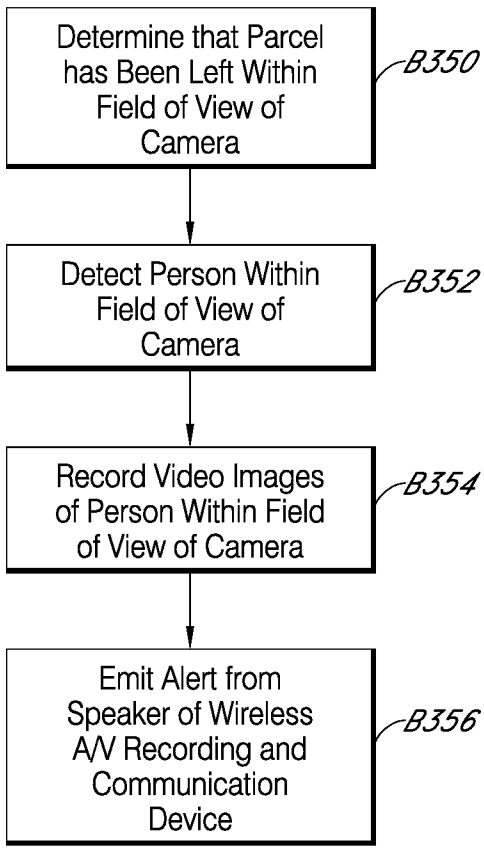
Determine that Parcel has Been Left Within Field of View of Camera
B350
Detect Person Within Field of View of Camera
B352
Record Video Images of Person Within Field of View of Camera
B354
Emit Alert from Speaker of Wireless A/V Recording and Communication Device
B356

FIG. 23

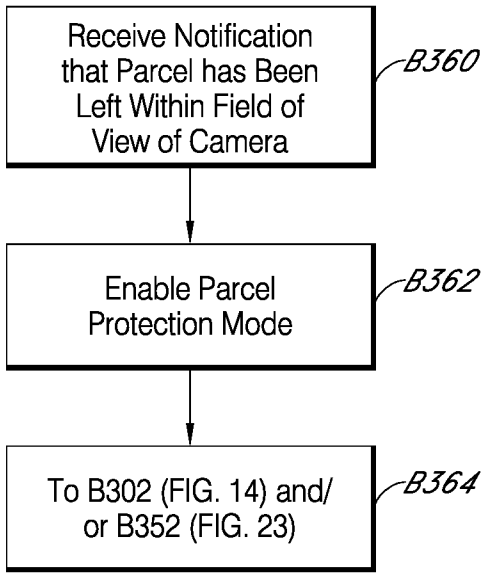
Receive Notification that Parcel has Been Left Within Field of View of Camera
B360
Enable Parcel Protection Mode
B362
To B302 (FIG. 14) and/ or B352 (FIG. 23)
B364

FIG. 24

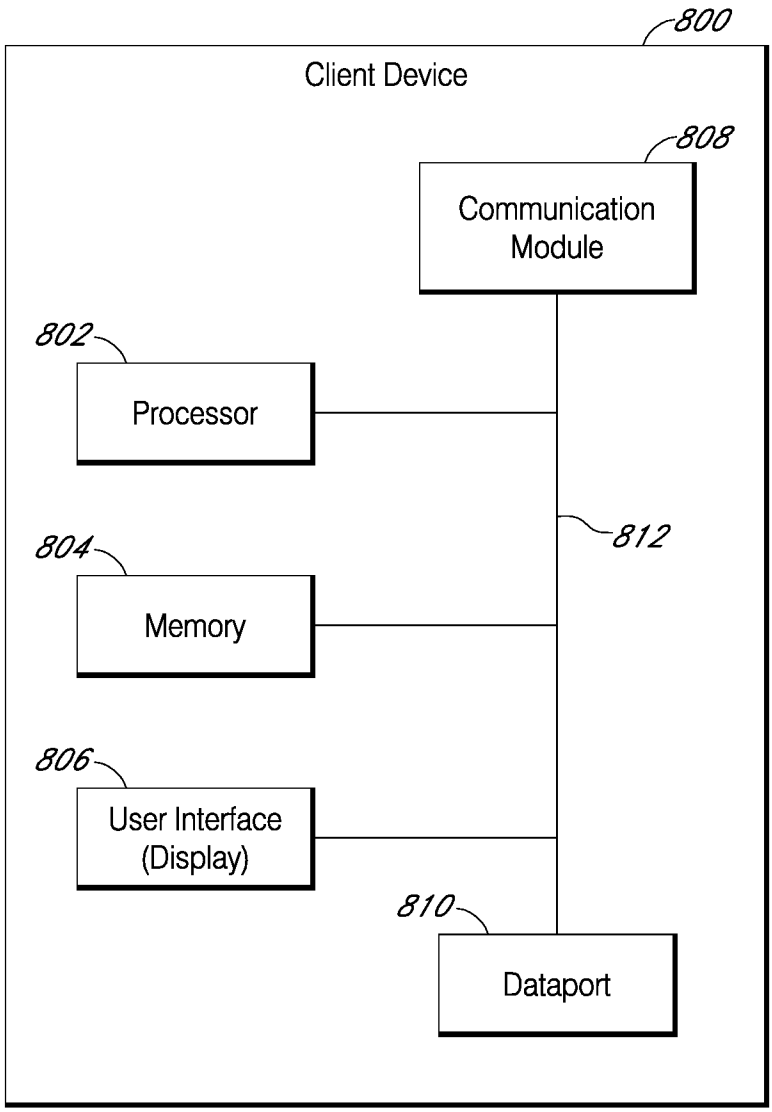
800
Client Device
808
Communication Module
802
Processor
812
804
Memory
806
User Interface (Display)
810
Dataport

FIG. 25

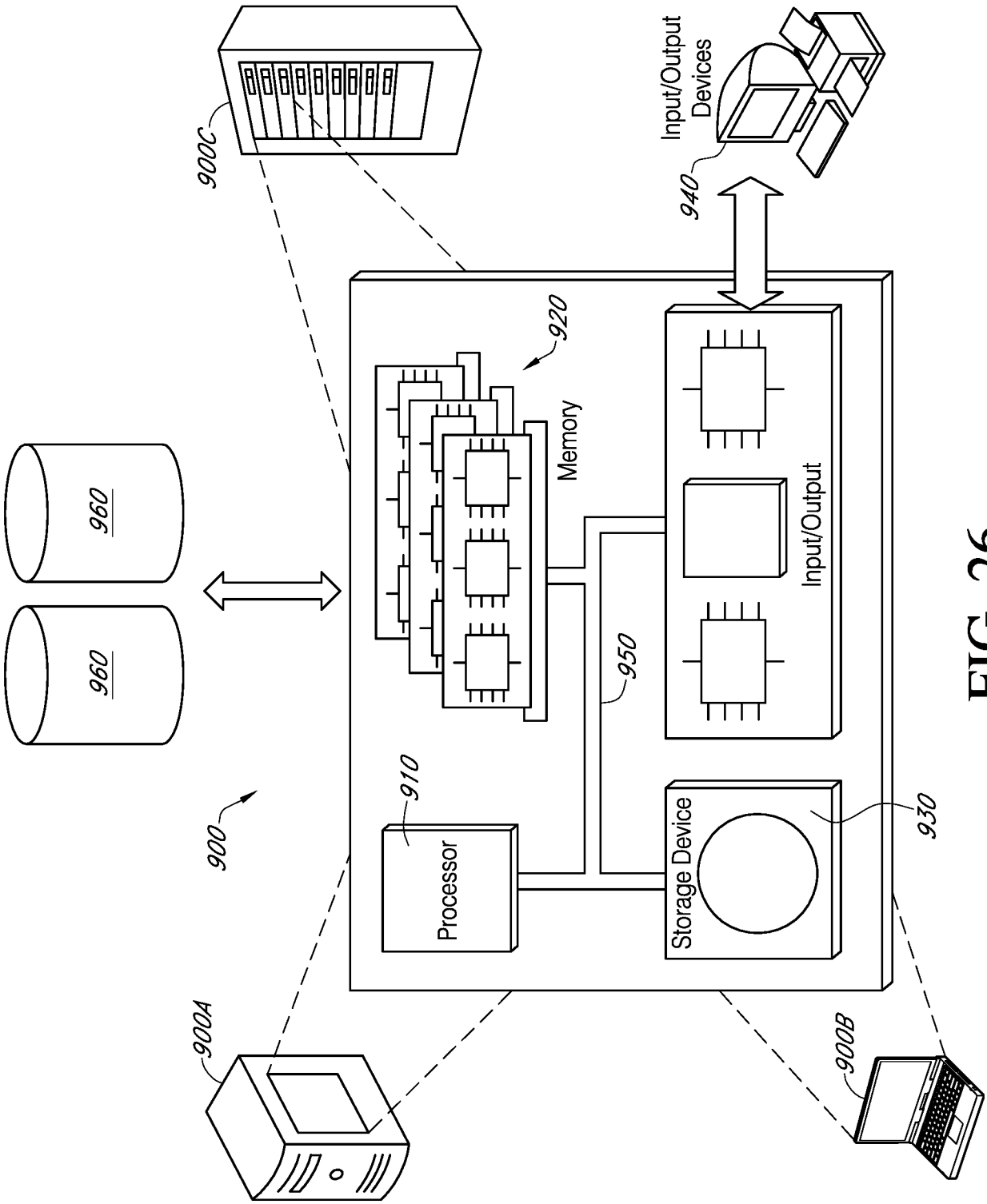
900C
Input/Output Devices
940
920
Memory
960
960
950
Input/Output
910
Processor
900
Storage Device
930
900A
900B

FIG. 26

INTERNATIONAL SEARCH REPORT

International application No.
PCT/US2017/045477

A. CLASSIFICATION OF SUBJECT MATTER

H04N 7/18(2006.01)i, H04N 5/77(2006.01)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 7/18; H04N 5/232; H04N 1/00; G08B 21/24; G08B 29/18; G06Q 10/08; H04N 5/77

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: unauthorized, removal, area, alert, parcel

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
Y	US 2016-0171435 A1 (AT&T INTELLECTUAL PROPERTY I, L.P.) 16 June 2016 See paragraphs [0016]-[0036]; claims 1-13; and figures 1-2.	1-35
Y	KR 10-2015-0055286 A (YURA CORPORATION CO., LTD.) 21 May 2015 See paragraphs [0045]-[0055]; claims 8-12; and figures 1-2.	1-35
A	KR 10-2016-0094597 A (JUNG HA SUN) 10 August 2016 See paragraphs [0023]-[0035]; claims 1-5; and figures 1-2.	1-35
A	US 2016-0212386 A1 (GOOGLE INC.) 21 July 2016 See paragraphs [0023]-[0026]; claims 1-2; and figure 1.	1-35
A	US 2016-0105644 A1 (MASTER LOCK COMPANY LLC. et al.) 14 April 2016 See paragraphs [0080]-[0089]; and figure 1.	1-35

☐ 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	Date of mailing of the international search report
09 November 2017 (09.11.2017)	**09 November 2017 (09.11.2017)**

Name and mailing address of the ISA/KR
International Application Division
Korean Intellectual Property Office
189 Cheongsa-ro, Seo-gu, Daejeon, 35208, Republic of Korea
Facsimile No. +82-42-481-8578

Authorized officer
AHN, Jeong Hwan
Telephone No. +82-42-481-8633

INTERNATIONAL SEARCH REPORT

Information on patent family members

International application No.

PCT/US2017/045477

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
US 2016-0171435 A1	16/06/2016	None	
KR 10-2015-0055286 A	21/05/2015	None	
KR 10-2016-0094597 A	10/08/2016	None	
US 2016-0212386 A1	21/07/2016	US 2015-0237238 A1	20/08/2015
		US 2016-0191756 A1	30/06/2016
		US 2016-0191757 A1	30/06/2016
		US 9071740 B1	30/06/2015
US 2016-0105644 A1	14/04/2016	WO 2014-144628 A2	18/09/2014
		WO 2014-144628 A3	18/12/2014