TITLE OF THE INVENTION

Systems and Methods for Communication between a Security Device and a Remote Device

CROSS-REFERENCE TO RELATED APPLICATIONS

[0001] [Not Applicable]

- good background
- Excellent Validation

A

BACKGROUND OF THE INVENTION

[0002] The present invention generally relates to a home security system. More particularly, the present invention relates to a home security system that provides for communication with a mobile device.

[0003] In an increasingly mobile world, the ability to access our home as well as ensure its safety is certainly a concern for homeowners who find themselves frequently away from home. Providing homeowners with the knowledge that they will be immediately notified of a home invasion while away not only provides them with peace of mind, but also an effective way to respond to emergency situations. Because of safety concerns, various security systems have been developed to allow homeowners to receive notification in the event of a security breach.

[0004] For example, a home security system which notifies homeowners of a security breach is disclosed in Elliot et al., U.S. Pat. No. 7,593,512. The Elliot system discloses a security system connected through a Voice-over-IP ("VOIP") service (using Broadband Internet) rather than through the standard telephone line. The VOIP connection offers an advantage by monitoring the security system in real time. In the Elliot security system, the VOIP connection alerts the homeowner if the connection is broken – consequently signaling a security breach. The alert may then be used appropriately by the homeowner, for instance to contact emergency services.

[0005] Another example of a home security system which notifies homeowners of a security breach is disclosed in Bennett, III et al., U.S. Pat. No. 7,349,682. The Bennett security system discloses a system which integrates a security system with automation features and information services. The automation features are composed of an

automation controller which sends and receives messages through a wireless local transceiver. The security system also contains a controller that sends and receives messages from a wireless transceiver. Through the integration of security and automation systems, a homeowner may activate, deactivate, and monitor the security system or any home appliance (e.g., a sprinkler) from a remote location through a variety of media, such as an internet connection or a telephone line.

[0006] Many door security systems, which allow a homeowner a view of their entryway, have also been developed – not unlike that from a typical peephole – when a person or package is present.

[0007] For example, a surveillance system is disclosed in Tamayo, U.S. Pub. No. 2009/0273670. The Tamayo system discloses a video camera positioned by an entryway to transmit video images of the entryway to either a viewing panel on the inside of a door or a remote viewing station. The system is activated by a sensor placed under a door mat which detects a mass (e.g., from a person or package).

[0008] A last example of a remote viewing system is disclosed in Wang, U.S. Pub. No. 2009/0284600. Wang discloses a surveillance system which may be installed directly into the door viewer of an existing door. This system contains an image sensor, an audio sensor, and a speaker, all of which allow homeowners the ability to monitor the entryway of their home from a remote device and to engage in auditory communication with a third-party located at the entryway.

[0009] Despite the functions they provide, the prior art systems that address the problem of remote home security have various disadvantages.

[0010] The Elliot system, while providing a real-time status of a security system, is limited in the information it provides to the homeowner as well as the options the homeowner may exercise in the event of a security breach. Although the Elliot system notifies a homeowner if the VOIP connection is interrupted, that homeowner has no way to know whether the security breach was triggered by an intruder, a faulty power line, or even a forgetful family member. Homeowners not only do not know whether a genuine security breach occurred, but also are further disadvantaged by the system because they must take the additional step of contacting emergency services with limited information – a delay which could potentially compromise the safety of these homeowners' homes.

[0011] The Bennett system, while providing homeowners access to home automation and security features from a remote location, suffers from many of the same disadvantages as the Elliot system. Although an embodiment of the Bennett system does automatically contact emergency services upon detection of a forceful entry signal, again, the homeowner is provided no information regarding the cause of the forceful entry signal. Additionally, while homeowners are given the ability to remotely access the various security features of the security system, because homeowners lack specific information regarding what caused the security breach, the ability of the homeowner to determine the appropriate course of action – for instance whether to activate the system, deactivate the system, or call emergency services – is effectively impaired.

[0012] The Tamayo surveillance system provides homeowners with a convenient view of their entryway from a remote location yet nevertheless suffers from various disadvantages as well. Although able to view who may be at their door, homeowners may only passively watch the third-party at their entryway. This impairs the homeowner's

ability to effectively assess the situation; without communicating with the third-party, a homeowner may be unsure whether it is appropriate to contact emergency services. Consequently, homeowners only have the limited choice of viewing what is occurring at their entryway and deciding whether or not to contact emergency services.

[0013] Finally, the Wang remote viewing system, although providing solutions for some of the shortcomings of the Tamayo system, still suffers from serious flaws. The Wang system allows a homeowner to speak with a third-party while simultaneously viewing the third-party from a remote location. However, as with the Tamayo system, the Wang system suffers disadvantages because homeowners again are unable to respond to what they are viewing aside from contacting emergency services.

BRIEF SUMMARY OF THE INVENTION

[0014] One or more of the embodiments of the present invention provide systems and methods for video communication between a remote device and a security device and the receipt and transfer of command data between a remote device and a security device.

[0015] The system for two-way communication between a security device and a remote device includes an entryway security device, a first communication network, an external central processing unit ("CPU"), a second communication network, and a remote device. In this system, the entryway security device is in two-way communication with the external CPU through the first communication network and the external CPU is in two-way communication with the remote device through the second communication network.

[0016] In operation, the remote device provides the user with the choice of effectuating a change to the security device – for example locking a door. If the user chooses to effectuate a change to the security device, the user may do so through a user input interface which is part of the remote device. The remote device transmits command data representing information from the user input interface from the remote device to the external CPU through the second communication network. The command data is then transmitted from the external CPU to the security device through the first communication network. The security device, upon receiving the command data effectuates a change upon the security device including, for example, locking the lock on a door.

[0017] Additionally, the present invention provides a method for video communication from the remote device to the security device. In operation, video data recorded by the remote device is transmitted from the remote device to the external CPU

through the second communication network. The video data is then transmitted from the external CPU to the security device through the first communication network. The security device then displays the video data from the remote device on its display.

BRIEF DESCRIPTION OF THE DRAWINGS

[0018] Figure 1 illustrates a flow chart of an embodiment of the system for two-way communication between a security device and a remote device.

[0019] Figure 2 illustrates an entryway security device according to an embodiment of the present invention.

[0020] Figure 3 illustrates a preferred embodiment of an entryway security device 110 according to an embodiment of the present invention.

[0021] Figure 4 illustrates a remote device according to an embodiment of the present invention.

[0022] Figure 5 illustrates a preferred embodiment of a remote device according to an embodiment of the present invention.

[0023] Figure 6 illustrates an external central processing unit according to an embodiment of the present invention.

[0024] Figure 7 illustrates a flow chart of an embodiment of the method for initiating contact between an entryway security device and a remote device.

[0025] Figure 8 illustrates a flow chart of an embodiment of the method for audio and video communication from an entryway security device to a remote device.

[0026] Figure 9 illustrates a flow chart of an embodiment of the method for audio and video communication from a remote device to an entryway security device.

[0027] Figure 10 illustrates a flow chart of an embodiment of the method for communicating status data of at least one security feature on an entryway security device to a remote device.

[0028] Figure 11 illustrates a flow chart of an embodiment of the method for effectuating command data for at least one security feature on an entryway security device from a remote device to an entryway security device.

[0029] Figure 12 illustrates a flow chart of a preferred embodiment of the method for controlling features of an entryway security system from an interface on a remote device.

[0030] Figure 13 illustrates a flow chart of a preferred embodiment of the method for monitoring features of an entryway security system from an interface on a remote device.

DETAILED DESCRIPTION OF THE INVENTION

[0031] Figure 1 illustrates a block diagram of a system 100 for two-way communication between a security device and a remote device according to an embodiment of the present invention. The two-way communication system 100 includes an entryway security device 110, a first communication network 120, an external central processing unit ("CPU") 130, a second communication network 140, and a remote device 150.

[0032] In the two-way communication system 100, the entryway security device 110 is in two-way communication with the external CPU 130 through the first communication network 120 and the external CPU 130 is in two-way communication with the remote device 150 through the second communication network 140.

[0033] In operation, data representing information from the entryway security device 110 is transmitted from the entryway security device 110 to the external CPU 130 through the first communication network 120. The data representing information from the entryway security device 110 may represent audio, video, and entryway security device status data. The external CPU 130 then receives the data representing information from the entryway security device 110 from the entryway security device 110 through the first communication network 120. The data representing information from the entryway security device 110 is then converted by the external CPU 130 into data that may be processed by the remote device 150. The converted data representing information from the entryway security device 110 is then transmitted from the external CPU 130 to the remote device 150 through the second communication network 140.

[0034] In further operation, data representing information from the remote device 150 is transmitted from the remote device 150 to the external CPU 130 through the second communication network 140. The data representing information from the remote device 150 may represent audio, video, and command data. The external CPU 130 then receives the data representing information from the remote device 150 from the remote device 150 through the second communication network 140. The data representing information from the remote device 150 is then converted by the external CPU 130 from data representing information from the remote device 110 into data that may be processed by the entryway security device 110. The converted data representing information from the remote device 150 is then transmitted from the external CPU 130 to the entryway security device 110 through the first communication network 110.

[0035] In a preferred embodiment, the entryway security device 110 replaces the preexisting doorknob hardware of a door. In another embodiment, the entryway security device 110 is affixed to a wall near an entryway where the entryway security device 110 is viewable from the entryway.

[0036] In a preferred embodiment, the first communication network 120 is a Bluetooth network. In another embodiment, the first communication network 120 is a hardwired communication network or a wireless communication network, for instance an 802.11 connection or radio frequency.

[0037] In a preferred embodiment, the external CPU 130 is a personal computer within the home. In another embodiment, the external CPU 130 is unnecessary and the entryway security device 110 communicates directly with the remote device 150.

[0038] In a preferred embodiment, the second communication network 140 is a VOIP network. In another embodiment, the second communication network 140 uses a SKYPE platform.

[0039] In another embodiment, the data representing information from the entryway security device 110 may represent any type of data the entryway security device 110 may need to transmit to the remote device 150.

[0040] In a preferred embodiment, the data representing information from the remote device 150 may represent any type of data the remote device 150 may need to transmit to the entryway security device 110.

[0041] In a preferred embodiment, the remote device 150 is a mobile device with capabilities to display an interface allowing a user to record audio and video data and to control features of the entryway security device 110 remotely. In another embodiment, the remote device 150 is an external CPU such as a personal computer that provides for two-way communication with the entryway security device 110. In another embodiment, the remote device 150 is any mobile device such as a pager where the user may receive information from the entryway security device 110 and sends command data to the entryway security device 110.

[0042] Figure 2 illustrates a block diagram an entryway security device 110 according to an embodiment of the present invention. The entryway security device 110 includes a central processing unit ("CPU") 205, a communication system 210, a door sensor 215, a locking mechanism 220, a power source 225, and an external device 230. The external device 230 includes a system activator 235, an image sensor 240, an audio sensor 245, a display 250, an audio speaker 255, and an internal audio speaker 260.

[0043] In the entryway security device 110, the CPU 205 is in two-way communication with the external device 230 (including a system activator 235, an image sensor 240, an audio sensor 245, a display 250, an audio speaker 255), the communication system 210, and the door sensor 215. The CPU 205 is in one-way communication with the locking mechanism 220 where one-way communication occurs from the CPU 205 to the locking mechanism 220. The communication system 210 is in two-way communication with an external device. The system activator 235 is in one-way communication with the internal audio speaker 260 where one-way communication occurs from the system activator 235 to the internal audio speaker 260. The power source 225 is electrically connected with the external device 230 (including a system activator 235, an image sensor 240, an audio sensor 245, a display 250, and an audio speaker 255), the locking mechanism 220, the door sensor 215, the CPU 205, and the internal audio speaker 260.

[0044] In operation, the system activator 235 activates the entryway security device 110 when the system activator 235, a doorbell, is effectuated. The system activator 235 sends a signal to the internal audio speaker 260 which broadcasts an audio signal into the home. The CPU 205 receives video data from the image sensor 240, audio data from the audio sensor 245, and status data from the door sensor 215 representing the status of the door security system 220. The CPU 205 transmits the video data, audio data, and status data to the communication system 210. The communication system 210 then transmits the video data, audio data, and status data to an external device.

[0045] In further operation, the communication system 210 receives external data from an external device representing audio data, video data, and command data. The

communication system 210 transmits audio data, video data, and command data to the CPU 205. The CPU 205 transmits audio data to the audio speaker 255 and transmits video data to the display 250. The CPU 205 transmits command data to the door security system 220, where the door security system 220 then effectuates the appropriate change. This may include, for example, causing a locking mechanism to lock or unlock.

[0046] In a preferred embodiment, the external device 230 is affixed on the outside of a door around the doorknob. In another embodiment, the external device 230 is affixed near the entryway where it is viewable by a user by the entryway. The external device 230 may be affixed, for example, on a wall or a post next to the entryway.

[0047] In another embodiment, the system activator 235 activates the system through the detection of a variety of signals. The system activator may be, for example: a mass sensor, a heat sensor, a motion sensor, or a wireless device sensor.

[0048] In a preferred embodiment, the internal audio speaker 260 is a speaker that broadcasts a predetermined audio signal similar to any standard doorbell.

[0049] In a preferred embodiment, the image sensor 240 is a video camera.

[0050] In a preferred embodiment, the audio sensor 245 is a microphone.

[0051] In a preferred embodiment, the display 250 is an LCD. In another embodiment, the display 250 is a plasma display or a black & white LCD screen.

[0052] In a preferred embodiment, the audio speaker 255 is a speaker.

[0053] In a preferred embodiment, the power source 225 is a local battery, for example an AA or AAA battery. In an alternative embodiment, the power source 225 is from a hardwire connection to the power source in a home. In another embodiment, the power source 225 is from solar panels located in a home or near the door. In another

embodiment, the power source 225 may include a variety of sources, for example gas lines or wind turbines.

[0054] In a preferred embodiment, the door security system 220 is a solenoid locking mechanism. In another embodiment, the door security system 220 is a locking mechanism that is composed of, for example, a magnetic lock or a mechanical servo motor.

[0055] In a preferred embodiment, the door sensor 215 is a magnetic sensor that detects whether the door is opened or closed. In another embodiment, the door sensor 215 detects whether the door is locked or unlocked. In another embodiment, the door sensor 215 is a mass detector may detect, for example, the presence of a person or a package.

[0056] In a preferred embodiment, the communication system 210 is a Bluetooth device. In another embodiment, the communication system 210 is a hardwire connection to internet access. In another embodiment, the communication system 210 is a wireless device that connects to an external device through an 802.11 wireless network. In another embodiment, the communication system 210 is a wireless device that connects to an external device through radio frequency.

[0057] Figure 3 illustrates a preferred embodiment of an entryway security device 110 according to an embodiment of the present invention. The preferred embodiment of the entryway security device 110 is located on a door 310 and includes an exterior door knob 320, an interior door knob 330, an external device 230, a door security system 220, a door sensor 215, and a communication system 210. The external device 230 includes a system activator 235, an image sensor 240, an audio sensor 245, a display 250, and an audio speaker 255.

[0058] In this preferred embodiment of the entryway security device 110, the entryway security device replaces the preexisting door knob hardware in the door 310. The external device 230 is affixed to the exterior face of the door 310 around where the exterior door knob 320 and the interior door knob 330 are connected. The external device 230 includes a communication interface 340 located above the exterior door knob 320 wherein this communication interface includes the system activator 235, the image sensor 240, the audio sensor 245, the display 250 and the audio speaker 255. The communication system 210 and the door sensor 215 are connected to the interior face of the door 310, with the communication system 210 located above the interior door knob 330 and the door sensor 215 located below the interior door knob 330. The door security system 220 is located in the door 310 between the exterior door knob 320 and the interior door knob 330 and replaces the preexisting locking mechanism of the door 310.

[0059] In operation, the system activator 235 activates the entryway security device 110 when the system activator 235, a doorbell, is pushed. Upon activation, the communication interface 340 records audio data from the audio sensor 245 and image data from the image sensor 240. As well, sensor data representing whether the door is opened or closed is generated by the door sensor 215. The audio data, image data, and sensor data, representing whether the door is opened or closed, is sent to a remote device through the communication system 210.

[0060] In further operation, the communication system 210 receives remote device data from a remote device representing audio data, video data, and command data. The audio data is sent to the communication interface 340 where it is relayed to the audio speaker 255 to be played as audio output. The video data is sent to the communication

interface 340 where it is relayed to the display 250 to be displayed as video output. The command data effectuates a change by the door security system 220. For example, if the door security system 220 was a locking mechanism, the door security system 220 would lock or unlock the door 310.

[0061] In further operation, the door 310 may be opened by a user if the door security system 220 allows for ingress of the entryway. The user may either enter the entryway by turning the exterior doorknob 320 or exit the entryway by turning the interior doorknob 330 and opening the door 310.

[0062] In a preferred embodiment, the communication system 210 is a Bluetooth device. In another embodiment, the communication system 210 is a hardwire connection to internet access. In another embodiment, the communication system 210 is a wireless device that connects to an external device through 802.11 wireless network. In another embodiment, the communication system 210 is a wireless device that connects to an external device through radio frequency.

[0063] In a preferred embodiment, the communication system 210 is located on the interior side of the door 310. In an alternative embodiment, the communication system 210 is located on the exterior side of the door 310.

[0064] In a preferred embodiment, the door security system 220 is a solenoid locking mechanism. In another embodiment, the door security system 220 is a locking mechanism that is composed of, for example, a magnetic lock or a mechanical servo motor.

[0065] In a preferred embodiment, the door sensor 215 is a magnetic sensor that detects whether the door is opened or closed.

[0066] In a preferred embodiment, the door sensor 215 is located on a portion of the entryway security device 110 on the interior side of the door. In another embodiment, the door sensor 215 is located on a portion of the entryway security device 110 on the exterior side of the door. In another embodiment, the door sensor 215 is flush with the door jamb of the door 310.

[0067] In a preferred embodiment, the external device 230 is located on the door 310 around the exterior door knob 320. In another embodiment, the external device 230 is affixed near the entryway where it is viewable by a user by the entryway. For example, the external device 230 may be affixed on a wall or post by the door 310. In another embodiment, the external device 230 is not included and the system activator 235, the image sensor 240, the audio sensor 245, the display 250 and the audio speaker 255 are split up separately and may be affixed in a variety of locations (e.g. on the exterior face of the door 310, on the interior face of the door 310, or inside the door 310).

[0068] In a preferred embodiment, the communication interface 340 is located above the exterior door knob 320. In another embodiment, the communication interface 340 is located near the entryway where it is viewable by a user by the entryway. For example, the communication interface 340 may be affixed to the door 310 or by the entryway on a wall or post by the door.

[0069] In a preferred embodiment, the communication interface 340 is composed of an LCD touch screen. In another embodiment, the communication interface 340 is composed of mechanical buttons that a user may interact with.

[0070] In another embodiment, the system activator 235 activates the system through the detection of a variety of signals. The system activator may be, for example: a mass sensor, a heat sensor, a motion sensor, or a wireless device sensor.

[0071] Figure 4 illustrates a block diagram of a remote device 150 according to an embodiment of the present invention. The remote device 150 includes a video display 410, a video recording device 420, a central processing unit ("CPU") 430, a power source 440, a user input interface 450, an audio playback device 460, an audio recording device 470, and a communication system 480. The user input interface 450 may include user actuated buttons and displays such as: an entryway status display 482, a door locking button 484, a door unlocking button 486, a camera on button 488 for turning on the video recording device 420, a camera off button 490 for turning off the video recording device 420, a microphone on button 492 for turning on the audio recording device 470, a microphone off button 494 for turning off the audio recording device 470, and a third-party contacting button 496.

[0072] In the remote device 150, the CPU 430 is in two-way communication with the video display 410, the video recording device 420, the user input interface 450, the audio playback device 460, the audio recording device 470, and the communication system 480. Because the user input interface 450 may include user actuated buttons and displays, the CPU 430 may also be in two-way communication with user actuated buttons and displays which may include, for example, the entryway status display 482, the door locking button 484, the door unlocking button 486, the camera on button 488 for turning on the video recording device 420, the camera off button 490 for turning off the video recording device 420, the microphone on button 492 for turning on the audio recording

device 470, the microphone off button 494 for turning off the audio recording device 470, and the third-party contacting button 496. The power source 440 is electrically connected with the video display 410, the video recording device 420, the CPU 430, the user input interface 450, the audio playback device 460, the audio recording device 470 and the communication system 480.

[0073] In operation, data representing video data from the video recording device 420 and audio data from the audio recording device 470 are transmitted to the CPU 430. The video and audio data are received by the CPU 430 that transmits the video and audio data to the communication system 480. The video and audio data are received by the communication system 480 which then transmits the video and audio data to an external device.

[0074] In further operation, data representing video and audio data is received by the communication system 480 from an external device. The communication system 480 transmits the video and audio data to the CPU 430. The video data is received by the CPU 430 and is then transmitted to the video display 410 which then displays the video data as video images. The audio data is received by the CPU 430 and is then transmitted to the audio playback device 460 which plays the audio data.

[0075] In further operation, the user input interface 450, which may include user actuated buttons, transmits signals to the CPU 430. The CPU 430 receives the signal and effectuates a change in the form of lighting up the display of the user actuated button that was activated and dimming the corresponding user actuated button (if there is one) on the user input interface 450. For example, if the door locking button 484 was activated, then the interface would light up the door locking button 484 on the input interface 450. As

well, the corresponding door unlocking button 486 would be dimmed on the input interface 450.

[0076] In further operation, the user input interface 450, which may include user actuated buttons, transmits signals to the CPU 430. The CPU 430 receives the signal and transmits the signal to the communication system 480. The communication system 480 receives the signal and transmits the signal to an external device in response to data sent from the user actuated button.

[0077] In further operation, the user input interface 450, which may include user actuated displays, receives signals from the CPU 430 and effectuates a change in the form of displaying information about the external security device 110 of Figure 1 on the user input interface 450. For example, upon receiving data representing that the door 310 of Figure 3 is closed, the entryway status display 482 would display on the user input interface 450 that the "door is closed."

[0078] In a preferred embodiment, the remote device 150 is a mobile device.

[0079] In a preferred embodiment, the user input interface 450 includes the camera on button 488 which, if actuated, transmits a signal to the CPU 430 which receives the signal and allows the transmission of video data from the video recording device 420 to the CPU 430.

[0080] In a preferred embodiment, the user input interface 450 includes the camera off button 490 which, if actuated, transmits a signal to the CPU 430 which receives the signal and stops the transmission of video data from the video recording device 420 to the CPU 430.

[0081] In a preferred embodiment, the user input interface 450 includes the microphone on button 492 which, if actuated, transmits a signal to the CPU 430 which receives the signal and allows the transmission of audio data from the audio recording device 470 to the CPU 430.

[0082] In a preferred embodiment, the user input interface 450 includes the microphone off button 494 which, if actuated, transmits a signal to the CPU 430 which receives the signal and stops the transmission of audio data from the audio recording device 470 to the CPU 430.

[0083] In a preferred embodiment, the user input interface 450 includes the door locked button 484 which, if actuated, transmits a door locked signal to the CPU 430. The CPU 430 receives the door locked signal and transmits the door locked signal to the communication system 480 which receives the door locked signal and transmits the door locked signal to an external device.

[0084] In a preferred embodiment, the user input interface 450 includes the door unlocked button 486 which, if actuated, transmits a door unlocked signal to the CPU 430. The CPU 430 receives the door unlocked signal and transmits the door unlocked signal to the communication system 480 which receives the door unlocked signal and transmits the door unlocked signal to an external device.

[0085] In a preferred embodiment, the user input interface 450 includes the third-party contacting button 496 which, if actuated, transmits a third-party contacting signal to the CPU 430. The CPU 430 receives the third-party contacting signal and transmits the third-party contacting signal to the communication system 480 which receives the third-party contacting signal and contacts an external device.

[0086] In a preferred embodiment, the user input interface 450 includes the entryway status display 482. Data representing entryway status is received by the communication system 480 from an external device and transmitted to the CPU 430. The CPU 430 receives the entryway status data and transmits the entryway status data to the user input interface 450 where it is displayed on the entryway status display 482.

[0087] In a preferred embodiment, the remote device 150 is a cellular phone. In another embodiment, the remote device 150 is any handheld device with a wireless connection that provides an interface for sending and receiving commands from an external device. This may include, for example: a smart phone, a portable music player, a portable video player, or a pager. In another embodiment, the remote device 150 is a central processing unit that provides for sending and receiving commands from an external device.

[0088] In a preferred embodiment, the video recording device 420 is a video camera.

[0089] In a preferred embodiment, the audio recording device 470 is a microphone.

[0090] In a preferred embodiment, the video display 410 is an LCD. In another embodiment, the display 410 is a plasma display or a black & white LCD screen.

[0091] In a preferred embodiment, the audio playback device 460 is a speaker.

[0092] In a preferred embodiment, the user input interface 450 is an LCD touch screen. In another embodiment, the user input interface 450 is a set of mechanical buttons that provide for user actuation. In another embodiment, the user input interface 450 provides user actuation options through voice activation.

[0093] In a preferred embodiment, the communication system 480 is a Bluetooth device. In another embodiment, the communication system 480 is a hardwire connection to internet access. In another embodiment, the communication system 480 is a wireless device that connects to an external device through an 802.11 wireless network. In another embodiment, the communication system 480 is a wireless device that connects to an external device through radio frequency.

[0094] In a preferred embodiment, the user input interface 450 is an LCD touch screen and any interaction with any of the user actuated buttons (for example: the door locking button 484, the door unlocking button 486, the camera on button 488, the camera off button 490, the microphone on button 492 or the microphone off button 494) causes the activated user actuated button to change (for example: to light up) on the user input interface 450.

[0095] Figure 5 illustrates a preferred embodiment of a remote device 150 according to an embodiment of the present invention. The preferred embodiment of the remote device 150 includes a communication panel 500 which includes a video display 410, a video recording device 420, and a user input interface 450. The user input interface 450 may include user actuated buttons and displays such as: an entryway status display 482, a door locking button 484, a door unlocking button 486, a camera on button 488 for turning on the video recording device 420, a camera off button 490 for turning off the video recording device 420, a microphone on button 492 for turning on an audio recording device, a microphone off button 494 for turning off an audio recording device, and a third-party contacting button 496.

[0096] In this preferred embodiment of the remote device 150, the communication panel 500 is located on the surface of the remote device 150 and includes the video display 410, the video recording device 420 and the user input interface 450. The user input interface 450 may include user actuated buttons and displays such as: an entryway status display 482, a door locking button 484, a door unlocking button 486, a camera on button 488 for turning on the video recording device 420, a camera off button 490 for turning off the video recording device 420; a microphone on button 492 for turning on an audio recording device, a microphone off button 494 for turning off an audio recording device, and a third-party contacting button 496.

[0097] In operation, the video recording device 420 records video data for transmission and the video display 410 displays received video data.

[0098] In further operation, the user input interface 450 presents at least one user actuated button for control of the remote device 150 or an external device. In further operation, the user input interface 450 responds to received signals and effectuates a change to the interface in the form of lighting up the display of the user actuated button that was activated and dimming the corresponding user actuated button (if there is one). For example, if the door locking button 484 was activated, then the interface would light up the door locking button 484 on the input interface 450. As well, the corresponding door unlocking button 486 would be dimmed on the input interface 450.

[0099] In a preferred embodiment, the remote device 150 is a cellular phone. In another embodiment, the remote device 150 is any handheld device with a wireless connection that provides an interface for sending and receiving commands from an external device. This may include, for example: a smart phone, a portable music player, a

portable video player, or a pager. In another embodiment, the remote device 150 is a central processing unit that provides for sending and receiving commands from an external device.

[00100] In a preferred embodiment, the video display 410 is an LCD. In another embodiment, the display 410 is a plasma display or a black & white LCD screen.

[00101] In a preferred embodiment, the video recording device 420 is a video camera.

[00102] In a preferred embodiment, the user input interface 450 is an LCD touch screen. In another embodiment, the user input interface 450 is a set of mechanical buttons that provide for user actuation. In another embodiment, the user input interface 450 provides user actuation options through voice activation.

[00103] In a preferred embodiment, the user input interface 450 is an LCD touch screen and any interaction with any of the user actuated buttons (for example: the door locking button 484, the door unlocking button 486, the camera on button 488, the camera off button 490, the microphone on button 492 or the microphone off button 494) causes the activated user actuated button to change (for example: to light up) on the user input interface 450 and the user actuated button's counterpart to change as well (for example: to dim) on the user input interface 450.

[00104] Figure 6 illustrates a block diagram of an external central processing unit ("external CPU") 130 according to an embodiment of the present invention. The external central processing unit 130 includes a communication system 610, a display 620, a user input system 640, a central processing unit ("CPU") 630, and a power source 650.

[00105] In the external CPU 130, the CPU 630 is in two-way communication with the communication system 610. The CPU 630 is in one-way communication with the display 620, with the display 620 receiving data from the CPU 630. The CPU 630 is in one-way communication with the user input system 640, with the CPU 630 receiving data from the user input system 640. The power source 650 is electrically connected with the CPU 630, the communication system 610, the display 620, and the user input system 640.

[00106] In operation, the communication system 610 receives the data transmitted from the communication system 210 of Figure 2 of the security device 110 of Figure 1 through the first communication system 120 as described above in Figure 1 and transmits the security device data to the CPU 630. The security device data represents audio, video, and security device sensor data from the security device 110 of Figure 1 representing whether the door is opened or closed. The CPU 630 receives the security device data and converts the security device data into data that may be received by the remote device 150 of Figure 1. The CPU 430 then transmits this remote device receivable data to the communication system 610. The communication system 610 receives the remote device receivable data from the CPU 430 and transmits the remote device receivable data to the communication system 480 of Figure 4 of the remote device 150 of Figure 1 through the second communication network 140 as described in Figure 1.

[00107] In further operation, the communication system 610 receives the data transmitted from the communication system 480 of Figure 4 of the remote device 150 of Figure 1 through the second communication system 140 as described above in Figure 1 and transmits the security device data to the CPU 630. The remote device data represents audio, video, and command data from the remote device 150 of Figure 1. The CPU 630

receives the remote device data and converts the remote device data into data that may be received by the security device 110 of Figure 1. The CPU 430 then transmits this security device receivable data to the communication system 610. The communication system 610 receives the security device receivable data from the CPU 430 and transmits the security device receivable data to the communication system 210 of Figure 2 of the security device 110 of Figure 1 through the first communication network 120 as described in Figure 1.

[00108] In a preferred embodiment, the external CPU 130 is a personal computer. In another embodiment, the external CPU 130 is a laptop computer. In another embodiment, the external CPU 130 is any processing unit that may convert digital signals from one format to another and relay the data between the security device 110 of Figure 1 and the remote device 150 of Figure 1.

[00109] In a preferred embodiment, the user input system 640 is a keyboard and mouse. In another embodiment, the user input system 640 is the touch screen of a personal computer such a tablet.

[00110] In a preferred embodiment, the display 620 is a monitor. In another embodiment, the display 620 is not a separate device but embodied within the external CPU 130. For example, the display 620 may be a screen on a laptop or a tablet.

[00111] In a preferred embodiment, the power source 650 is a battery. In another embodiment, the power source 650 is a hardwired electrical connection to a power outlet.

[00112] In a preferred embodiment, the communication system 610 is a Bluetooth connection. In another embodiment, the communication system 610 is a hardwire connection to internet access. In another embodiment, the communication system 610 is a

wireless device that connects to an external device through an 802.11 wireless network. In another embodiment, the communication system 610 is a wireless device that connects to an external device through radio frequency.

[00113] In a preferred embodiment, the external CPU 130 transmits information to the security device 110 of Figure 1 through the first communication network 120 of Figure 1 where the first communication network 120 of Figure 1 uses VOIP. In another embodiment, the external CPU 130 transmits information to the security device 110 of Figure 1 through the first communication network 120 of Figure 1 where the second communication network 120 uses a SKYPE platform.

[00114] In a preferred embodiment, the external CPU 130 transmits information to the remote device 150 of Figure 1 through the second communication network 140 of Figure 1 where the second communication network 120 of Figure 1 uses VOIP. In another embodiment, the external CPU 130 transmits information to the remote device 150 of Figure 1 through the second communication network 140 of Figure 1 where the second communication network 120 of Figure 1 uses a SKYPE platform.

[00115] In another embodiment, the CPU 630 may display the information received from either the security device 110 of Figure 1 or the remote device 150 of Figure 1 on the display 620. In this embodiment, the user may interact with the aforementioned display through the user input system 640.

[00116] Figure 7 illustrates a flow chart of a method for initiating contact between an entryway security device and a remote device 700. First, at step 710, the entryway security device 110 of Figure 1 is activated by the system activator 235 of Figure 2 when the system activator 235 of Figure 2, a doorbell, is pushed.

[00117] Next, at step 720, the entryway security device 110 of Figure 1 communicates entryway security device data to the external CPU 130 of Figure 1 through the first communication network 120 of Figure 1. The entryway security data may include, for example, audio data, video data and sensor data representing whether the door is opened or closed.

[00118] Next, at step 730, the external CPU 130 of Figure 1 attempts to communicate the entryway security data to the remote device 150 of Figure 1 through the second communication network 140 of Figure 1. If there is a communication between the external CPU 130 of Figure 1 and the remote device 150 of Figure 1 through the second communication network 140 of Figure 1, the method for initiating contact between an entryway security device and a remote device 700 proceeds to step 740. If there is no communication between the external CPU 130 of Figure 1 and the remote device 150 of Figure 1 through the second communication network 140 of Figure 1, the method for initiating contact between an entryway security device and the remote device 700 proceeds to step 740.

[00119] Next, at step 740, because there is no communication between the external CPU 130 of Figure 1 and the remote device 150 of Figure 1 through the second communication network 140 of Figure 1, the entryway security data is discarded.

[00120] Next, at step 750, the external CPU 130 of Figure 1 queries the remote device 150 of Figure 1 in order to determine whether the remote device 150 will accept communication from the external CPU 130 of Figure 1 through the second communication network 140 of Figure 1. If the remote device 150 of Figure 1 accepts communication through the second communication network 140 of Figure 1, the method

for initiating contact between an entryway security device and the remote device 700 proceeds to step 770. If the remote device 150 of Figure 1 rejects the communication through the second communication network 140 of Figure 1, the method for initiating contact between an entryway security device and the remote device 700 proceeds to step 780.

[00121] Next, at step 760, the external CPU 130 of Figure 1 is connected to an automatic audio recording system through the second communication network 140 of Figure 1. The automatic audio recording system accepts entryway security data in the form of audio device from the external CPU 130 of Figure 1 through the second communication network 140 of Figure 1.

[00122] Next, at step 770, the external CPU 130 of Figure 1 establishes a two-way communication with the remote device 150 of Figure 1 through the second communication network 140 of Figure 1. The remote device 150 of Figure 1 receives entryway security data through the second communication network 140 of Figure 1 and the external CPU 130 of Figure 1 receives remote device data through the second communication network 140 of Figure 1.

[00123] In another embodiment, the communication of data from the entryway security device 110 of Figure 1 is communicated directly to the remote device 150 of Figure 1 and obviating the need for step 720.

[00124] In a preferred embodiment, the sending of any entryway security device data from the entryway security device 110 of Figure 1 occurs upon the receipt of an outside stimulus by the system activator 235 of Figure 2 regardless of whether communication to the remote device 150 of Figure 1 has been established at step 750.

[00125] In another embodiment, the sending of any entryway security device data from the entryway security device 110 of Figure 1 does not occur until communication to the remote device 150 of Figure 1 has been established at step 750.

[00126] Figure 8 illustrates a flow chart of a method for audio and video communication from an entryway security device to a remote device 800. First, at step 806, the image sensor 240 of Figure 2 and the audio sensor 245 of Figure 2 records video data and audio data respectively from the entryway security device 110 of Figure 1.

[00127] Next, at step 808, the entryway video data and entryway audio data are communicated to the CPU 205 of Figure 2 of the entryway security device 110 of Figure 1.

[00128] Next, at step 812, the entryway video data and entryway audio data are compressed by the CPU 205 of Figure 2 of the entryway security device 110 of Figure 1 into a low bandwidth signal.

[00129] Next, at step 818, the entryway low bandwidth signal is transmitted through the first communication network 120 of Figure 1 from the entryway security device 110 of Figure 1 to the external CPU 130 of Figure 1.

[00130] Next, at step 824, the entryway low bandwidth signal is received by the external CPU 130 of Figure 1 from the entryway security device 110 of Figure 1 through the first communication network 120 of Figure 1.

[00131] Next, at step 822, the entryway low bandwidth signal is converted by the external CPU 130 of Figure 1 into remote device audio data and remote device video data that may be received by the remote device 150 of Figure 1.

[00132] Next, at step 826, the entryway remote device audio data and entryway remote device video data is transmitted through the second communication network 140 of Figure 1 from the external CPU 130 of Figure 1 to the remote device 150 of Figure 1.

[00133] Next, at step 828, the entryway remote device audio data and entryway remote device video data is received by the remote device 150 of Figure 1 from the external CPU 130 of Figure 1 through the second communication network 140 of Figure 1.

[00134] Next, at step 832, the entryway remote device audio data and entryway remote device video data is converted by the CPU 430 of Figure 4 of the remote device 150 of Figure 1 into audio data that may be played by the audio playback device 460 of Figure 4 and into video data that may be displayed by the video display 410 of Figure 4 respectively.

[00135] Next, at step 838, the entryway audio data and entryway video data are communicated from the CPU 430 of Figure 4 of the remote device 150 of Figure 1 to the audio playback device 460 of Figure 4 and the video display 410 of Figure 4 respectively.

[00136] Next, at step 840, the video display 410 of Figure 4 of the remote device 150 of Figure 1 and the audio playback device 460 of Figure 4 of the remote device 150 of Figure 1 display video data and play audio data respectively.

[00137] In a preferred embodiment, the compression of data by the CPU 205 of Figure 2 of the entryway security device 110 of Figure 1 is through H.263 compression. In another embodiment, the compression of data by the CPU 205 of Figure 2 of the entryway security device 110 of Figure 1 is through any other type of data compression that produces data that may be sent through a low bandwidth connection.

[00138] In another embodiment, the first communication network 120 of Figure 1 is a high bandwidth connection and consequently obviates the need for data compression at step 812.

[00139] In another embodiment, the second communication network 140 of Figure 1 is a high bandwidth connection and consequently obviates the need for data conversion into a low bandwidth signal at step 820.

[00140] In a preferred embodiment, the external CPU 130 of Figure 1 converts the low bandwidth signal into remote device data that may be sent over a VOIP network. In another embodiment, the external CPU 130 of Figure 1 converts the low bandwidth signal into remote device data that may be sent over a SKYPE platform. In another embodiment, if the remote device 150 of Figure 1 is a central processing unit ("CPU") then no conversion need occur as the second communication network 140 of Figure 1 would be a hardwired broadband connection.

[00141] In a preferred embodiment, the CPU 430 of Figure 4 of the remote device 150 of Figure 1 converts audio and video input into remote device data that may be sent over a VOIP network. In another embodiment, the CPU 430 of Figure 4 of the remote device 150 of Figure 1 converts audio and video input into remote device data that may be sent over a SKYPE platform. In another embodiment, if the remote device 150 of Figure 1 is a central processing unit ("CPU") then no conversion need occur as the second communication network 140 of Figure 1 would be a hardwired broadband connection.

[00142] In another embodiment, entryway security device data generated by the entryway security device 110 of Figure 1 is communicated directly to the remote device

150 of Figure 1 and remote device data generated by the remote device 150 of Figure 1 is communicated directly to the entryway security device 110 of Figure 1.

[00143] Figure 9 illustrates a flow chart of method for audio and video communication from a remote device to an entryway security device 900. First, at step 934, the video recording device 420 of Figure 4 of the remote device 150 of Figure 1 records video data and the audio recording device 470 of Figure 4 of the remote device 150 of Figure 1 records audio data.

[00144] Next, at step 936, the video data and audio data are communicated to the CPU 430 of Figure 4 of the remote device 150 of Figure 1.

[00145] Next, at step 930, the video data and audio data are converted by the CPU 430 of Figure 4 of the remote device 150 of Figure 1 into remote device data.

[00146] Next, at step 942, the remote device data are transmitted through the second communication network 140 of Figure 1 from the remote device 150 of Figure 1 to the external CPU 130 of Figure 1.

[00147] Next, at step 944, the remote device data is received by the external CPU 130 of Figure 1 from the remote device 150 of Figure 1 through the second communication network 140 of Figure 1.

[00148] Next, at step 920, the remote device data is converted by the external CPU 130 of Figure 1 into a low bandwidth signal that may be received by the entryway security device 110 of Figure 1.

[00149] Next, at step 916, the remote device low bandwidth signal is transmitted through the first communication network 120 of Figure 1 from the external CPU 130 of Figure 1 to the entryway security device 110 of Figure 1.

[00150] Next, at step 914, the remote device low bandwidth signal is received by the entryway security device 110 of Figure 1 from the external CPU 130 of Figure 1 through the first communication network 120 of Figure 1.

[00151] Next, at step 910, the remote device low bandwidth signal is converted by the CPU 205 of Figure 2 of the entryway security device 110 of Figure 1 into audio data that may be played by the audio speaker 255 of Figure 2 and into video data that may be displayed by the display 250 of Figure 2 respectively.

[00152] Next, at step 904, the remote device audio data and remote device video data are communicated from the CPU 205 of Figure 2 of the entryway security device 110 of Figure 1 to the audio speaker 255 of Figure 2 of the entryway security device 110 of Figure 1 and to the display 250 of Figure 2 of the entryway security device 110 of Figure 1 respectively.

[00153] Next, at step 902, the display 250 of Figure 2 of the entryway security device 110 of Figure 1 and the audio speaker 255 of Figure 2 of the entryway security device 110 of Figure 1 display video data and play audio data respectively.

[00154] In a preferred embodiment, the compression of data by the CPU 205 of Figure 2 of the entryway security device 110 of Figure 1 is through H.263 compression. In another embodiment, the compression of data by the CPU 205 of Figure 2 of the entryway security device 110 of Figure 1 is through any other type of data compression that produces data that may be sent through a low bandwidth connection.

[00155] In another embodiment, the first communication network 120 of Figure 1 is a high bandwidth connection and consequently obviates the need for data compression at step 912.

[00156] In another embodiment, the second communication network 140 of Figure 1 is a high bandwidth connection and consequently obviates the need for data conversion into a low bandwidth signal at step 920.

[00157] In a preferred embodiment, the external CPU 130 of Figure 1 converts the low bandwidth signal into remote device data that may be sent over a VOIP network. In another embodiment, the external CPU 130 of Figure 1 converts the low bandwidth signal into remote device data that may be sent over a SKYPE platform. In another embodiment, if the remote device 150 of Figure 1 is a central processing unit ("CPU") then no conversion need occur as the second communication network 140 of Figure 1 would be a hardwired broadband connection.

[00158] In a preferred embodiment, the CPU 430 of Figure 4 of the remote device 150 of Figure 1 converts audio and video input into remote device data that may be sent over a VOIP network. In another embodiment, the CPU 430 of Figure 4 of the remote device 150 of Figure 1 converts audio and video input into remote device data that may be sent over a SKYPE platform. In another embodiment, if the remote device 150 of Figure 1 is a central processing unit ("CPU") then no conversion need occur as the second communication network 140 of Figure 1 would be a hardwired broadband connection.

[00159] In another embodiment, entryway security device data generated by the entryway security device 110 of Figure 1 is communicated directly to the remote device 150 of Figure 1 and remote device data generated by the remote device 150 of Figure 1 is communicated directly to the entryway security device 110 of Figure 1.

[00160] Figure 10 illustrates a flow chart of a method for communicating status data of at least one security feature on an entryway security device to a remote device 1000. First, at step 1005, the door sensor 215 of Figure 2 of the entryway security device 110 of Figure 1 monitors the status of the door security system 220 of Figure 2.

[00161] Next, at step 1010, the door sensor 215 of Figure 2 of the entryway security device 110 of Figure 1 communicates status data representing the status of the at least one sensor to the CPU 205 of Figure 2 of the entryway security device 110 of Figure 1.

[00162] Next, at step 1015, the CPU 205 of Figure 2 of the entryway security device 110 of Figure 1 communicates the status data to the communication system 210 of Figure 2 of the entryway security device 110 of Figure 1.

[00163] Next, at step 1020, the communication system 210 of Figure 2 of the entryway security device 110 of Figure 1 transmits the status data to the external CPU 130 of Figure 1 through the first communication network 120 of Figure 1.

[00164] Next, at step 1025, the external CPU 130 of Figure 1 receives the status data from the communication system 210 of Figure 2 of the entryway security device 110 of Figure 1 through the first communication network 120 of Figure 1.

[00165] Next, at step 1030, the external CPU 130 of Figure 1 converts the status data into remote device status data that may be received by the remote device 150 of Figure 1.

[00166] Next, at step 1035, the external CPU 130 of Figure 1 transmits the remote device status data to the communication system 480 of Figure 4 of the remote device 150 through the second communication network 140 of Figure 1.

[00167] Next, at step 1040, the communication system 480 of Figure 4 of the remote device 150 of Figure 1 receives the remote device status data from the external CPU 130 of Figure 1 through the second communication network 140 of Figure 1.

[00168] Next, at step 1045, the communication system 480 of Figure 4 of the remote device 150 of Figure 1 communicates the remote device status data to the CPU 430 of Figure 4 of the remote device 150 of Figure 1.

[00169] In a preferred embodiment, the external CPU 130 of Figure 1 converts the low bandwidth signal into remote device data that may be sent over a VOIP network. In another embodiment, the external CPU 130 of Figure 1 converts the low bandwidth signal into remote device data that may be sent over a SKYPE platform. In another embodiment, if the remote device 150 of Figure 1 is a central processing unit ("CPU") then no conversion need occur as the second communication network 140 of Figure 1 would be a hardwired broadband connection.

[00170] In another embodiment, entryway security device data generated by the entryway security device 110 of Figure 1 is communicated directly to the remote device 150 of Figure 1.

[00171] In a preferred embodiment, the first communication network 120 of Figure 1 is a Bluetooth network. In another embodiment, the first communication network 120 of Figure 1 is a hardwired communication network or a wireless communication network, for instance an 802.11 connections or radio frequency.

[00172] In a preferred embodiment, the second communication network 140 of Figure 1 is a VOIP network. In another embodiment, the second communication network 140 of Figure 1 uses a SKYPE platform.

[00173] Figure 11 illustrates a flow chart of a method for effectuating command data for at least one security feature on an entryway security device from a remote device to an entryway security device 1100. First, at step 1105, command data is generated by the user input interface 450 of Figure 4 of the remote device 150 of Figure 1.

[00174] Next, at step 1110, the remote device command data is communicated from the user input interface 450 of Figure 4 of the remote device 150 of Figure 1 to the CPU 430 of Figure 4 of the remote device 150 of Figure 1.

[00175] Next, at step 1115, the CPU 430 of Figure 4 of the remote device 150 of Figure 1 communicates the remote device command data to the communication system 480 of Figure 4 of the remote device 150 of Figure 1.

[00176] Next, at step 1120, the communication system 480 of Figure 4 of the remote device 150 of Figure 1 transmits the remote device command data to the external CPU 130 of Figure 1 through the second communication network 140 of Figure 1.

[00177] Next, at step 1125, the external CPU 130 of Figure 1 receives the remote device command data from the communication system 480 of Figure 4 of the remote device 150 of Figure 1 through the second communication network 140 of Figure 1.

[00178] Next, at step 1130, the external CPU 130 of Figure 1 converts the remote device command data into a low bandwidth command signal that may be received by the entryway security device 110 of Figure 1.

[00179] Next, at step 1135, the external CPU 130 of Figure 1 transmits the low bandwidth command signal to the communication system 210 of Figure 2 of the entryway security device 110 of Figure 1 through the first communication network 120 of Figure 1.

[00180] Next, at step 1140, the communication system 210 of Figure 2 of the entryway security device 110 of Figure 1 receives the low bandwidth command signal from the external CPU 130 of Figure 1 through the first communication network 120 of Figure 1.

[00181] Next, at step 1145, the communication system 210 of Figure 2 of the entryway security device 110 of Figure 1 communicates the low bandwidth command signal to the CPU 250 of Figure 2 of the entryway security device 110 of Figure 1.

[00182] Next, at step 1150, the CPU 250 of Figure 2 communicates the low bandwidth command signal to the door security system 220 of Figure 2 of the entryway security device 110 of Figure 1.

[00183] Next, at step 1155, the door security system 220 of Figure 2 of the entryway security device 110 of Figure 1 effectuates a change to the door security system 220 of Figure 2 of the entryway security device 110 of Figure 1 in accordance to the low bandwidth command signal. In the preferred embodiment of Figure 2, the change effectuated would be locking or unlocking the lock of a door.

[00184] In a preferred embodiment, the external CPU 130 of Figure 1 converts the low bandwidth signal into remote device data that may be sent over a VOIP network. In another embodiment, the external CPU 130 of Figure 1 converts the low bandwidth signal into remote device data that may be sent over a SKYPE platform. In another embodiment, if the remote device 150 of Figure 1 is a central processing unit ("CPU") then no conversion need occur as the second communication network 140 of Figure 1 would be a hardwired broadband connection.

[00185] In another embodiment, remote device data generated by the remote device 150 of Figure 1 is communicated directly to the entryway security device 110 of Figure 1.

[00186] In a preferred embodiment, the first communication network 120 of Figure 1 is a Bluetooth network. In another embodiment, the first communication network 120 of Figure 1 is a hardwired communication network or a wireless communication network, for instance an 802.11 connections or radio frequency.

[00187] In a preferred embodiment, the second communication network 140 of Figure 1 is a VOIP network. In another embodiment, the second communication network 140 of Figure 1 uses a SKYPE platform.

[00188] In a preferred embodiment, the security feature actuated is one that locks or unlocks a door using the door security system 220 of Figure 2. The door security system 220 of Figure 2 may be, for example: a solenoid locking mechanism, a magnetic lock or a mechanical servo motor.

[00189] Figure 12 illustrates a flow chart of a method for controlling features of an entryway security system from an interface on a remote device 1200 in the preferred embodiment.

[00190] First, at step 1206, the user input interface 450 of Figure 4 of the remote device 150 of Figure 1 determines whether the third-party contacting button 496 of Figure 4 of the user input interface 450 of Figure 4 has been actuated. If the third-party contacting button 496 of Figure 4 of the user input interface 450 of Figure 4 has been actuated, the method for controlling features of an entryway security system from an interface on a remote device 1200 proceeds to step 1210. If the third-party contacting

button 496 of Figure 4 of the user input interface 450 of Figure 4 has not been actuated, the method for controlling features of an entryway security system from an interface on a remote device 1200 proceeds to step 1208.

[00191] Next, at step 1208, the user input interface 450 of Figure 4 of the remote device 150 of Figure 1 remains on standby and does not communicate any data to the CPU 430 of the remote device 150 of Figure 1.

[00192] Next, at step 1210, the user input interface 450 of Figure 4 of the remote device 150 of Figure 1 communicates command data representing contacting a third-party to the CPU 430 of the remote device 150 of Figure 1.

[00193] Next, at step 1248, the CPU 430 of the remote device 150 of Figure 1 transmits the command data representing contacting a third-party to an external device.

[00194] First, at step 1218, either the door locking button 484 of Figure 4 of the user input interface 450 of Figure 4 is actuated or the door unlocking button 486 of Figure 4 of the user input interface 450 of Figure 4 is actuated. If the door locking button 484 of Figure 4 of the user input interface 450 of Figure 4 has been actuated, the method for controlling features of an entryway security system from an interface on a remote device 1200 proceeds to step 1222. If the door unlocking button 486 of Figure 4 of the user input interface 450 of Figure 4 has not been actuated, the method for controlling features of an entryway security system from an interface on a remote device 1200 proceeds to step 1226.

[00195] Next, at step 1222, the user input interface 450 of Figure 4 of the remote device 150 of Figure 1 communicates command data representing locking a lock on a door to the CPU 430 of the remote device 150 of Figure 1.

[00196] Next, at step 1226, the user input interface 450 of Figure 4 of the remote device 150 of Figure 1 communicates command data representing unlocking a lock a door to the CPU 430 of the remote device 150 of Figure 1.

[00197] Next, at step 1248, the CPU 430 of the remote device 150 of Figure 1 either transmits the command data representing locking a lock on a door or transmits the command data representing unlocking a lock on a door to an external device.

[00198] First, at step 1228, either the camera on button 488 of Figure 4 of the user input interface 450 of Figure 4 is actuated or the camera off button 490 of Figure 4 of the user input interface 450 of Figure 4 is actuated. If the camera on button 488 of Figure 4 of the user input interface 450 of Figure 4 has been actuated, the method for controlling features of an entryway security system from an interface on a remote device 1200 proceeds to step 1236. If the camera off button 490 of Figure 4 of the user input interface 450 of Figure 4 has been actuated, the method for controlling features of an entryway security system from an interface on a remote device 1200 proceeds to step 1232.

[00199] Next, at step 1236, the user input interface 450 of Figure 4 of the remote device 150 of Figure 1 communicates command data representing turning an image sensor on to the CPU 430 of the remote device 150 of Figure 1.

[00200] Next, at step 1232, the user input interface 450 of Figure 4 of the remote device 150 of Figure 1 communicates command data representing turning an image sensor off to the CPU 430 of the remote device 150 of Figure 1. \

[00201] Next, at step 1248, the CPU 430 of the remote device 150 of Figure 1 either transmits the command data representing turning an image sensor on or transmits the command data representing turning an image sensor off to an external device.

[00202] First, at step 1238, either the microphone on button 492 of Figure 4 of the user input interface 450 of Figure 4 is actuated or the microphone off button 494 of Figure 4 of the user input interface 450 of Figure 4 is actuated. If the microphone on button 492 of Figure 4 of the user input interface 450 of Figure 4 has been actuated, the method for controlling features of an entryway security system from an interface on a remote device 1200 proceeds to step 1246. If the microphone off button 494 of Figure 4 of the user input interface 450 of Figure 4 has been actuated, the method for controlling features of an entryway security system from an interface on a remote device 1200 proceeds to step 1242.

[00203] Next, at step 1246, the user input interface 450 of Figure 4 of the remote device 150 of Figure 1 communicates command data representing turning an audio recording device on to the CPU 430 of the remote device 150 of Figure 1.

[00204] Next, at step 1242, the user input interface 450 of Figure 4 of the remote device 150 of Figure 1 communicates command data representing turning an audio recording device off to the CPU 430 of the remote device 150 of Figure 1.

[00205] Next, at step 1248, the CPU 430 of the remote device 150 of Figure 1 either transmits the command data representing turning an audio recording device on or transmits the command data representing turning an audio recording device off to an external device.

[00206] In a preferred embodiment, the user input interface 450 is an LCD touch screen and any interaction with any of the user actuated buttons (for example: the door locking button 484, the door unlocking button 486, the camera on button 488, the camera off button 490, the microphone on button 492 or the microphone off button 494) causes

the activated user actuated button to change (for example: to light up) on the user input interface 450 and the user actuated button's counterpart to change as well (for example: to dim) on the user input interface 450.

[00207] Figure 13 illustrates a flow chart of a method for monitoring features of an entryway security system from an interface on a remote device 1300 in the preferred embodiment. First, at step 1360, the CPU 430 of Figure 4 of the remote device 150 of Figure 1 receives status data representing whether a door of an entryway security system is open or closed.

[00208] Next, at step 1320, the CPU 430 of Figure 4 of the remote device 150 of Figure 1 determines whether the status data represents that the door of an entryway security system is opened or closed. If the status data represents that the door of an entryway security system is opened, then the method for monitoring features of an entryway security system from an interface on a remote device 1300 proceeds to step 1325. If the status data represents that the door of an entryway security system is closed, then the method for monitoring features of an entryway security system from an interface on a remote device 1300 proceeds to step 1327.

[00209] Next, at step 1325, the CPU 430 of Figure 4 of the remote device 150 of Figure 1 communicates status data representing that the door of an entryway security system is opened with the entryway status display 482 of Figure 4 on the user input interface 450 of Figure 4.

[00210] Next, at step 1340, the entryway status display 482 of Figure 4 on the user input interface 450 of Figure 4 responds to the data representing that the door of an entryway security system is opened.

[00211] Next, at step 1327, the CPU 430 of Figure 4 of the remote device 150 of Figure 1 communicates status data representing that the door of an entryway security system is closed with the entryway status display 482 of Figure 4 on the user input interface 450 of Figure 4.

[00212] Next, at step 1330, the entryway status display 482 of Figure 4 on the user input interface 450 of Figure 4 responds to the data representing that the door of an entryway security system is closed.

[00213] In a preferred embodiment, the user input interface 450 of Figure 4 is an LCD touch screen and any status data generated by an external device is displayed on the user input interface 450 of Figure 4 on a user actuated display (for example: the entryway status display 482 of Figure 4). In another embodiment, the user input interface 450 is an LCD touch screen that effectuates change on the user input interface 450 (for example: to light a button up) in response to any status data. In another embodiment, the audio playback device 460 of Figure 4 of the remote device 150 of Figure 1 plays a sound in response to any status data.

[00214] In a preferred embodiment, the status data generated by an external device is status data representing whether the door 310 of Figure 3 on which an entryway security device 110 of Figure 1 is located is opened or closed. In another embodiment, the status data generated by an external device is status data representing other aspects of the entryway that the entryway security device 110 of Figure 1 controls. This may include status data that represents, for example: the presence of a person or a package at an entryway).

[00215] In view of the foregoing teaching, embodiments of the present invention provide numerous advantages over the systems, methods, and devices described in the prior art for providing a homeowner the ability to communicate with a security system from a remote location and respond more effectively to perceived security breaches. Additionally, the system for two-way communication between a security device and a remote device 100 also provide homeowners practical and non-security-related capabilities not present in the prior art.

[00216] First, unlike the surveillance systems described in the Tamayo and Wang applications, the system for two-way communication between a security device and a remote device 100 provides a homeowner with both audio and video communication capabilities. While the Wang system discloses audio communication between homeowners and a third-party at an entryway, the added video communication capabilities of the present ~~invention~~ provide for more effective and candid communication between a homeowner and a third-party. Although not a complete deterrent, the visual presentation of the homeowner to the third-party at the entryway may deter a potential intruder as it fosters the impression that the homeowner is present at the door and watching. From a functional standpoint, in situations where homeowners are unable to return home to receive a house call, the video communication capability provides an effective way for the homeowner to communicate with guests. As well, the video communication may assist in conducting business at one's doorway – whether in receiving packages from the post office or speaking with a work associate. The video communication allows for an added security check for the third-party who may not feel comfortable speaking with someone he or she cannot see about private matters.

either or "present system" "one or more embodiments"

[00217] Second, the present invention presents homeowners with notifications on their remote device both actively and passively. The system for two-way communication between a security device and a remote device 100 actively calls the homeowner's remote device when the security system is activated. If the homeowner fails to answer, the preferred embodiment of the present invention provides the third-party with the opportunity to leave a message on the homeowner's voicemail. While the prior art systems provide for methods of sending signals to the homeowner – whether through a remote device or by email – these systems do not provide for a method of dealing with situations where the homeowner fails to timely receive the incoming communication. The present invention provides an added functional purpose. The ability for the third-party to leave a message provides homeowners with the ability to receive some kind of communication from a visitor in circumstances when they are unable to receive the communication when it is initially sent.

[00218] Third, the system for two-way communication between a security device and a remote device 100 provides the homeowner with controlled communication capabilities with a third-party. The present invention, through the method for two-way audio and video communication between an entryway security device and a remote device 700, allows homeowners to prevent the third-party from either viewing or hearing them. This allows for an added privacy function for homeowners who may not want the third-party to selectively hear or see what is occurring around them at their remote location.

[00219] Fourth, the preferred embodiment of the present invention presents homeowners with control over individual features of the security system that, in addition

to the ability for audio-visual communication, provide for both security and functional benefits not available in prior art systems. Although the Elliot and Wang systems allow for a homeowner to remotely activate and deactivate the system, because of the dearth of information provided to homeowners regarding the surrounding circumstances of the home, the homeowner would arguably be activating and deactivating the system blindly. In the preferred embodiment of the present invention, the option of locking and unlocking the door as well as the ability to tell the status of whether the door is closed or not, allow homeowners to respond accordingly to the audio-video communication they are receiving. Aside from the obvious security benefits of locking a door and ensuring that it is closed from a remote location, the present invention provides homeowners with the practical ability of allowing a visitor entry into the home. For example, a family member who may have locked him or herself out of the home may activate the preferred embodiment of the present invention by ringing the door bell. The homeowner may then communicate with the family member, verifying through video communication the identity of the family member, and subsequently unlocking the door from his or her mobile device to allow the family member entry into the home. Once the family member enters the home, the homeowner further has the capability to check whether the door is closed and to subsequently lock the door.

[00220] Lastly, the system for two-way communication between a security device and a remote device 100 integrates all of the features available to the homeowner on a single platform which provides with an efficient and effective way to respond to security breaches or communicate with a third-party at the entryway. The prior art systems of Elliot and Bennett require homeowners to separately contact emergency services upon

the receipt of a security breach. In emergency situations where homeowners must respond quickly in order to ensure the safety of their homes, the additional time a homeowner needs to take in order to respond effectively to a notification to a security breach is both detrimental to the security of the homeowner's home, but also creates an added layer of inconvenience. The present invention, by providing for both security system and communication control options on one interface, allows homeowners to effectively and immediately respond to any emergency situation they may face. Most importantly, homeowners may contact emergency services without completely removing themselves from the user interface. This provides for a fast and effective method of getting help without excessive delay.

[00221] In summary, because of the system's unique location on the door of a home's entryway and comprehensive surveillance capabilities, the present invention provides both security and practical functionalities not embodied in prior art systems.

[00222] While particular elements, embodiments, and applications of the present invention have been shown and described, it is understood that the invention is not limited thereto because modifications may be made by those skilled in the art, particularly in light of the foregoing teaching. It is therefore contemplated by the appended claims to cover such modifications and incorporate those features which come within the spirit and scope of the invention.

CLAIMS

1. A system for communication, said system including:

an entryway security device, wherein said entryway security device includes a video display and a user actuated locking mechanism for locking a door, wherein said entryway security device may control said user actuated locking mechanism, wherein said video display is near an entryway; and

a remote device, wherein said remote device records video image data and transmits said video image data through a communication network to said video display.

2. The system of claim 1 wherein said security device fits into a standard size door knob opening and replaces the previous hardware without modification to the door.

3. The system of claim 1 wherein said video image data is first sent to an external central processing unit which converts said video image data to data which may be displayed at said video display on said entryway security device.

4. The system of claim 3 wherein said external central processing unit is connected to said entryway security device through a wireless connection.

5. The system of claim 4 wherein said entryway security device uses Bluetooth to communicate with said external central processing unit.

6. The system of claim 3 wherein said external central processing unit is connected to said entryway security device through a hardwire internet connection.

7. The system of claim 3 wherein said external central processing unit communicates with said remote device using a VOIP network.

8. The system of claim 3 wherein said external central processing unit communicates with said remote device using a SKYPE platform.

9. A method for communication, said method including:

recording video image data at a remote device;

transmitting said video image data from said remote device to a video display located on an entryway security device, wherein said entryway security device contains a user actuated locking mechanism;

receiving said video image data at said video display; and

displaying said video image data as video on said video display.

10. The method of claim 9 wherein said video image data is first transmitted to and received by an external central processing unit before being transmitted to and received by said entryway security device.

11. The method of claim 10 wherein said external central processing unit is connected to said entryway security device through a wireless connection.

12. The method of claim 11 wherein said entryway security device uses Bluetooth to communicate with said external central processing unit.

13. The method of claim 10 wherein said external central processing unit is connected to said entryway security device through a hardwire internet connection.

14. The method of claim 10 wherein said transmitting and receiving of data between said remote device and said external central processing unit occurs using a VOIP network.

15. The method of claim 10 wherein said transmitting and receiving of data between said remote device and said external central processing unit occurs using a SKYPE platform.

16. A system for actuating a locking mechanism, said system including:

a remote device, wherein said remote device transmits command data to an entryway security device to initiate the locking of a lock; and

a locking mechanism, wherein said locking mechanism is part of said entryway security device, wherein said locking mechanism locks said lock in response to said command data received.

17. The system of claim 16 wherein said entryway security device fits into a standard size door knob opening and replaces the previous hardware without modification of the door.

18. The system of claim 16 wherein said command data is first sent to an external central processing unit that converts said command data to data that can be read by said entryway security device.

19. The system of claim 18 wherein said external central processing unit is connected to said entryway security device through a wireless connection.

20. The system of claim 19 wherein said security device uses Bluetooth to communicate with said external central processing unit.

21. The system of claim 18 wherein said external central processing unit is connected to said entryway security device through a hardwire internet connection.

22. The system of claim 18 wherein said external central processing unit communicates with said remote device using a VOIP network.

23. The system of claim 18 wherein said external central processing unit communicates with said remote device using a SKYPE platform.

24. A method for actuating a locking mechanism, said method including:

providing an interface on a remote device, wherein said interface includes a switch allowing the actuation of a locking mechanism in an entryway security device;

transmitting locking data to said entryway security device, wherein said locking data represents whether said locking mechanism is to be actuated;

receiving locking data from said remote device; and

actuating said locking mechanism on said entryway security device in response to said locking data.

25. The method of claim 24 wherein said video image data is first transmitted to and received by an external central processing unit before being transmitted to and received by said entryway security device.

26. The method of claim 25 wherein said external central processing unit is connected to said entryway security device through a wireless connection.

27. The method of claim 26 wherein said entryway security device uses Bluetooth to communicate with said external central processing unit.

28. The method of claim 25 wherein said external central processing unit is connected to said entryway security device through a hardwire internet connection.

29. The method of claim 25 wherein said transmitting and receiving of data between said remote device and said external central processing unit occurs using a VOIP network.

30. The method of claim 25 wherein said transmitting and receiving of data between said remote device and said external central processing unit occurs using a SKYPE platform.

ABSTRACT

Systems and methods are provided for communication between a remote device and an entryway security device which is preferably located on or near an entryway. In the aforementioned systems and methods, the remote device may control video communication between the remote device and the entryway security device. Additionally, the remote device may send commands to effectuate a change on a security feature of an entryway security device. This may include, for instance, a command to actuate a locking mechanism to lock the lock of a door.

FIGURE 1.

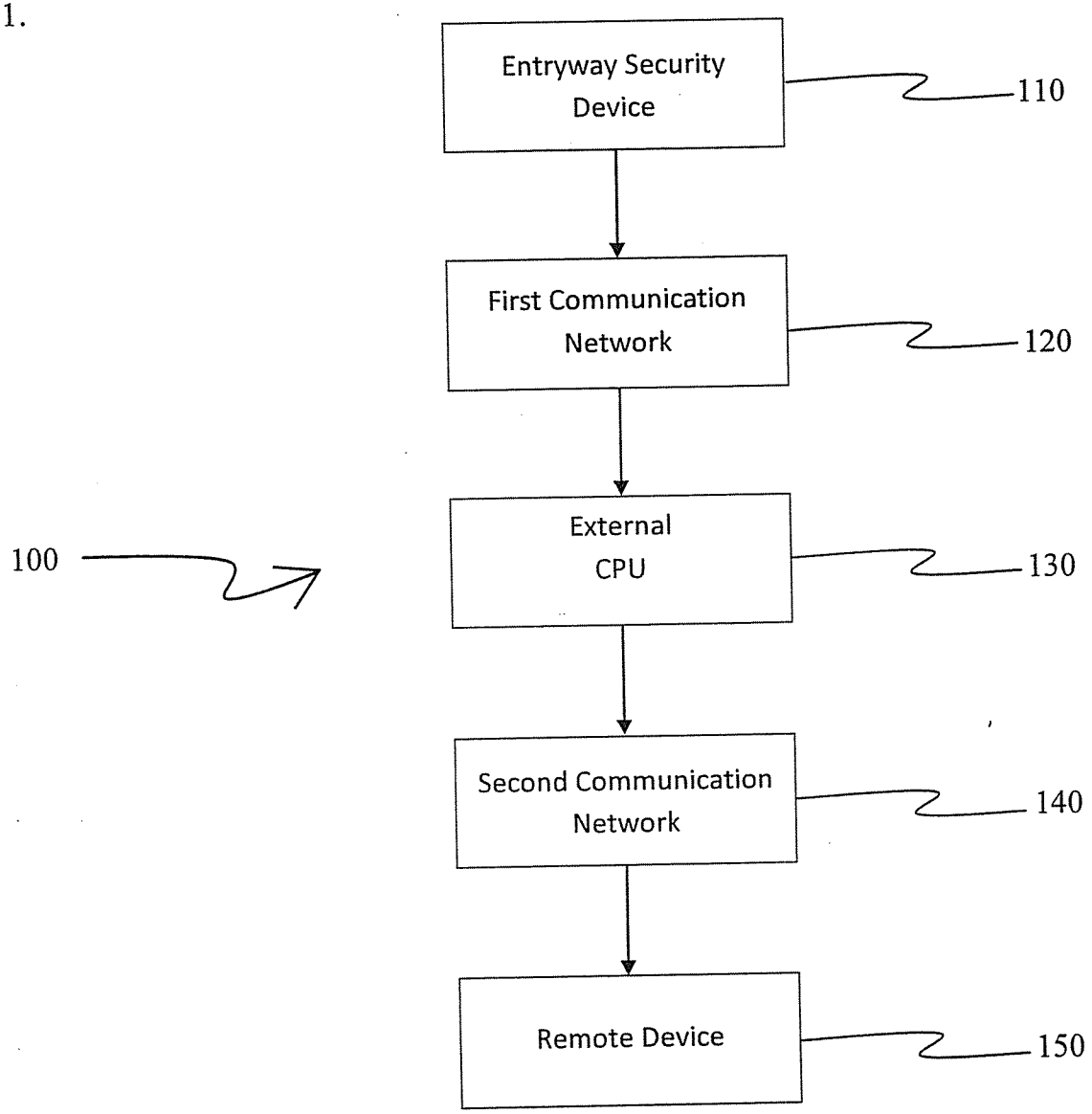

Entryway Security Device
110
First Communication Network
120
100
External CPU
130
Second Communication Network
140
Remote Device
150

FIGURE 2.

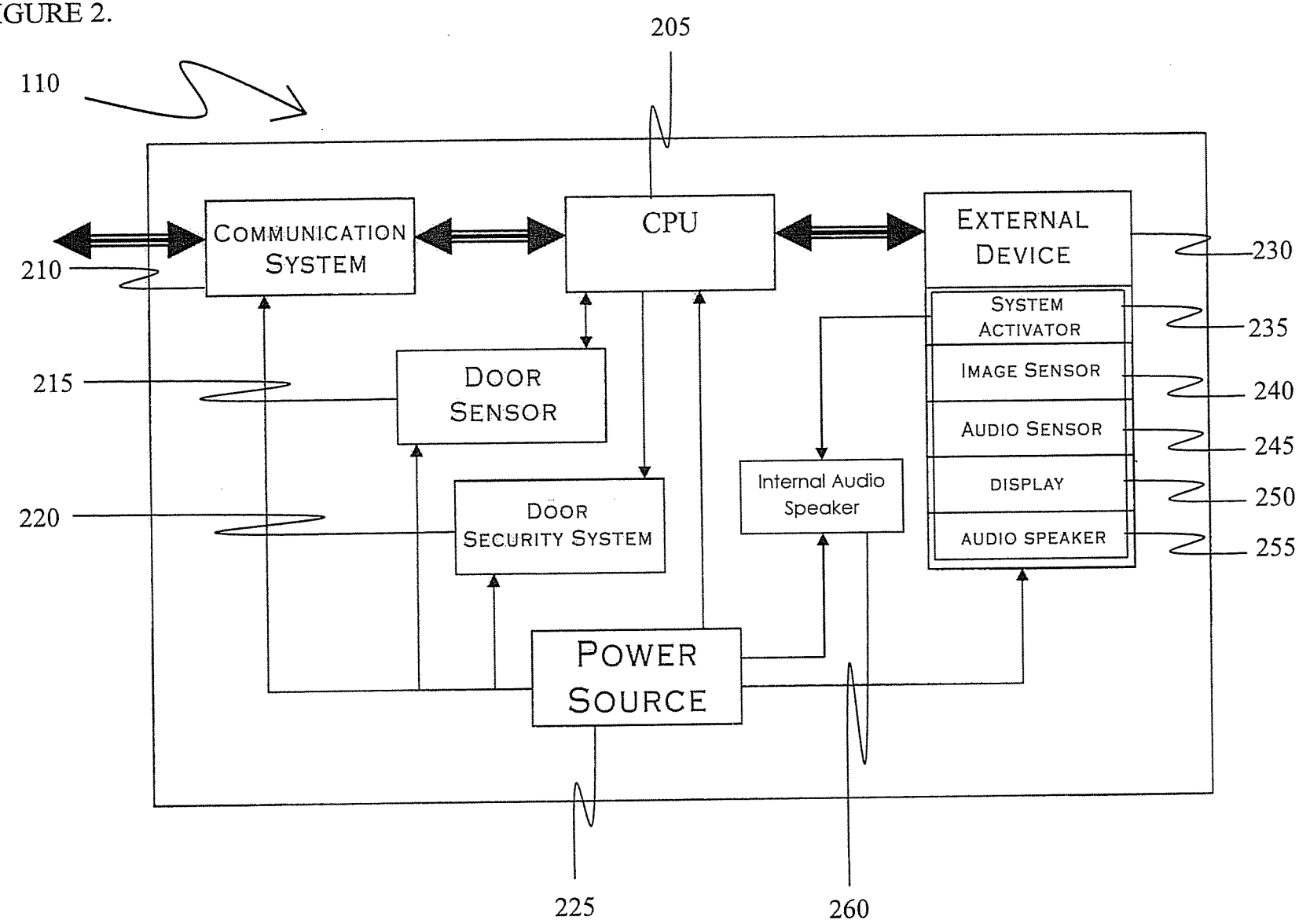

205
110
COMMUNICATION SYSTEM
CPU
EXTERNAL DEVICE
210
230
SYSTEM ACTIVATOR
235
215
DOOR SENSOR
IMAGE SENSOR
240
AUDIO SENSOR
245
Internal Audio Speaker
DISPLAY
250
220
DOOR SECURITY SYSTEM
AUDIO SPEAKER
255
POWER SOURCE
225
260

FIGURE 3.

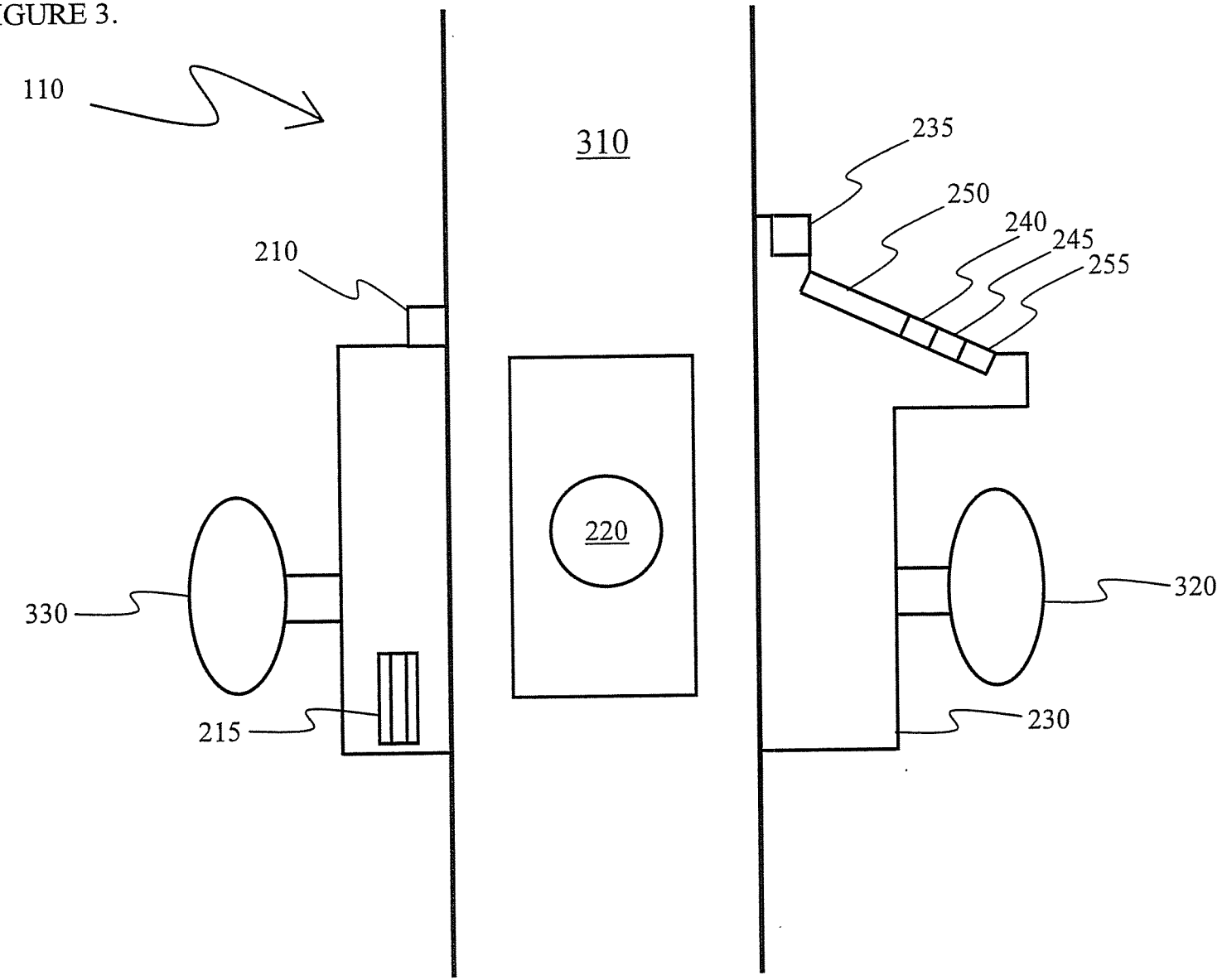


FIGURE 4.

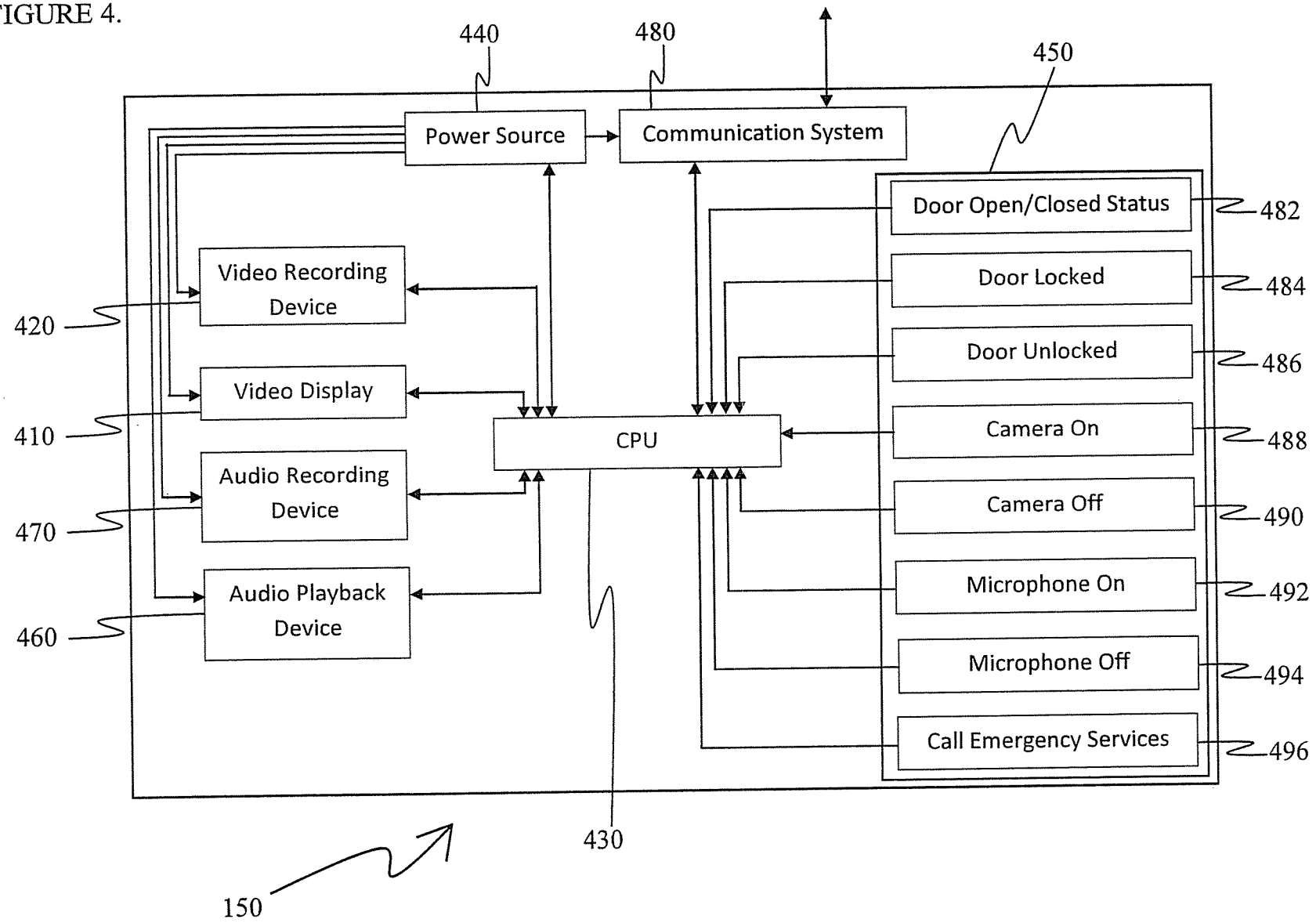

440
480
450
Power Source
Communication System
Door Open/Closed Status
482
Video Recording Device
Door Locked
484
420
Video Display
Door Unlocked
486
410
CPU
Camera On
488
Audio Recording Device
Camera Off
490
470
Audio Playback Device
Microphone On
492
460
Microphone Off
494
Call Emergency Services
496
430
150

FIGURE 5.

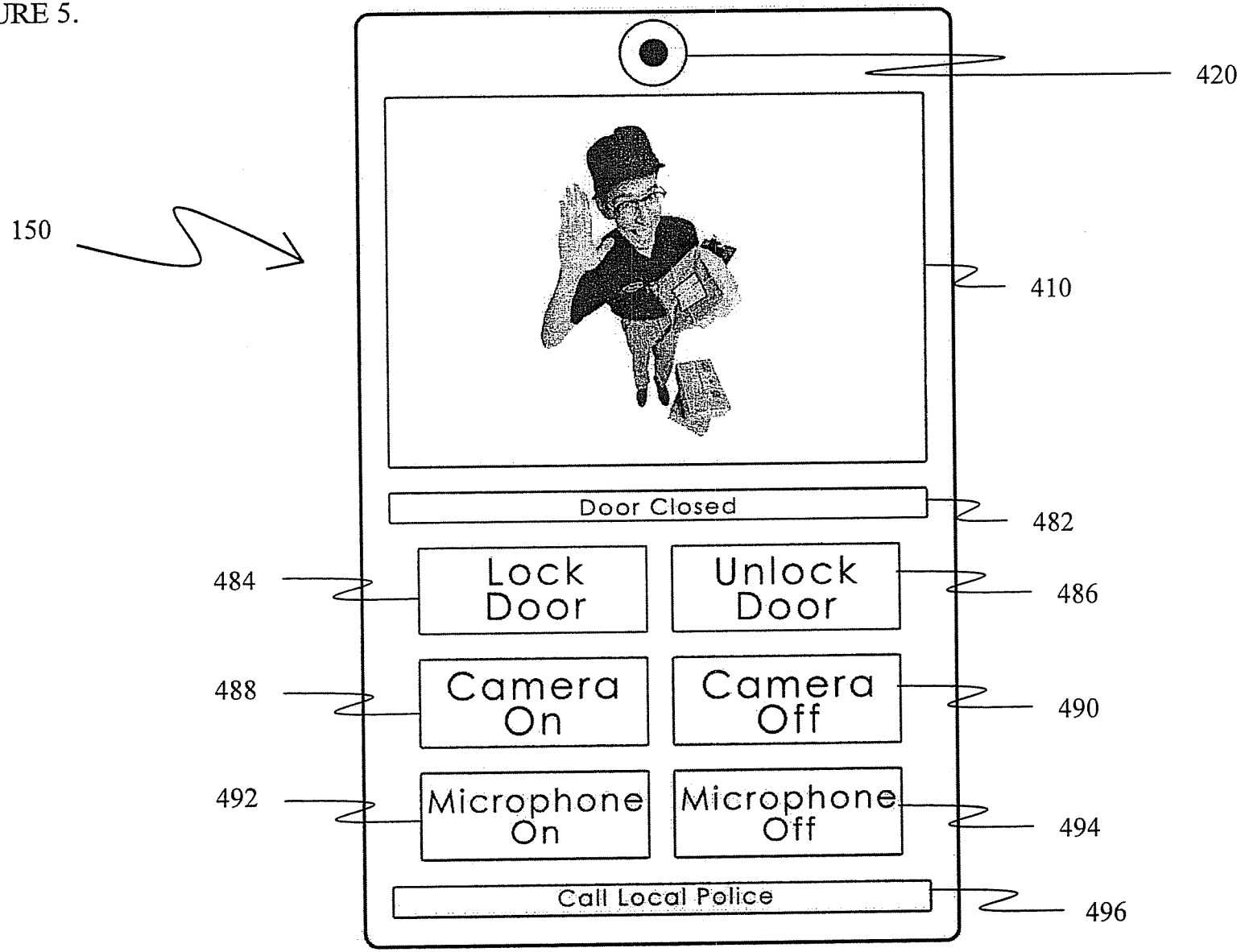

150
420
410
Door Closed
482
484
Lock Door
Unlock Door
486
488
Camera On
Camera Off
490
492
Microphone On
Microphone Off
494
Call Local Police
496

FIGURE 6.

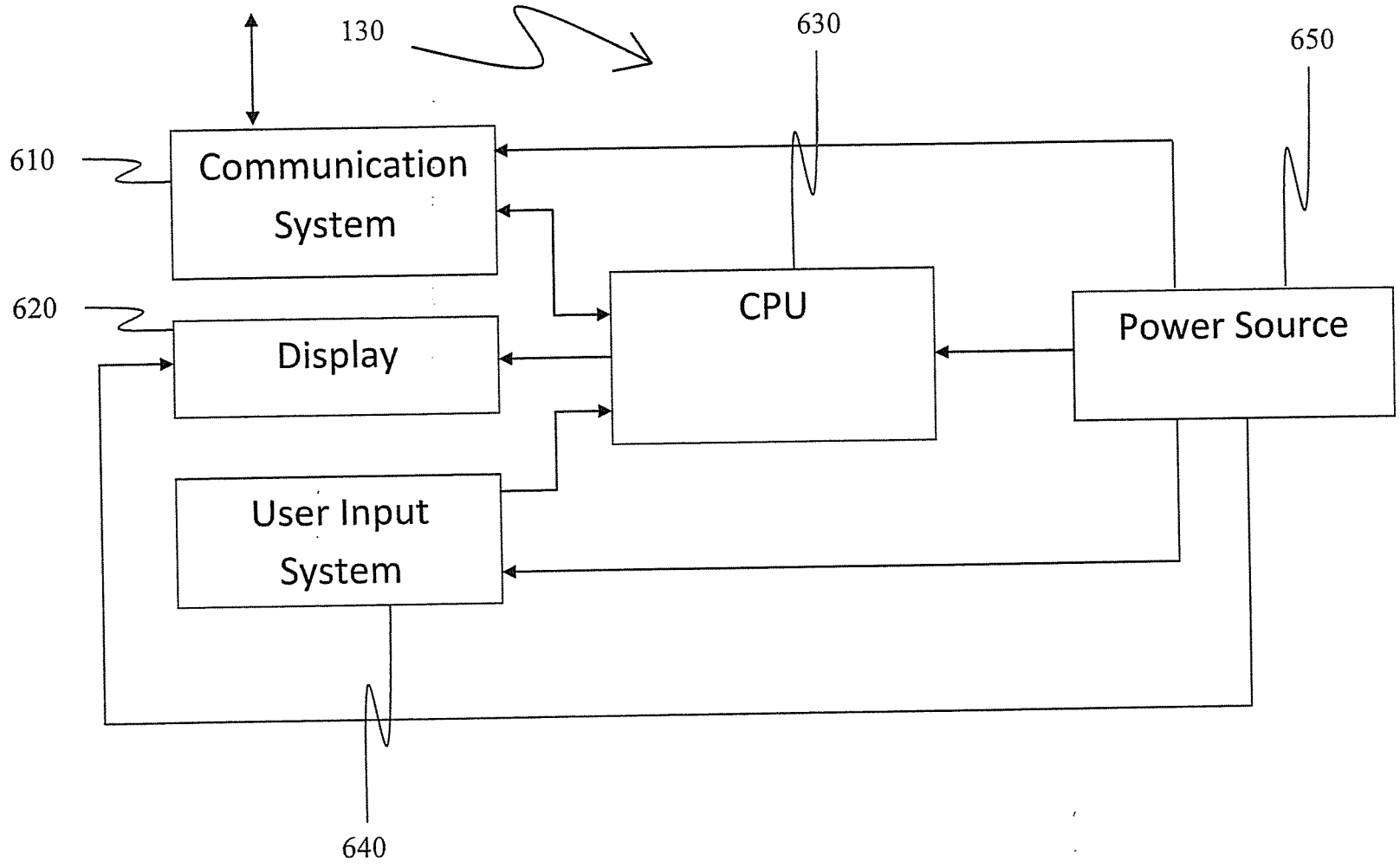

130
630
650
610
Communication System
620
Display
CPU
Power Source
User Input System
640

FIGURE 7.

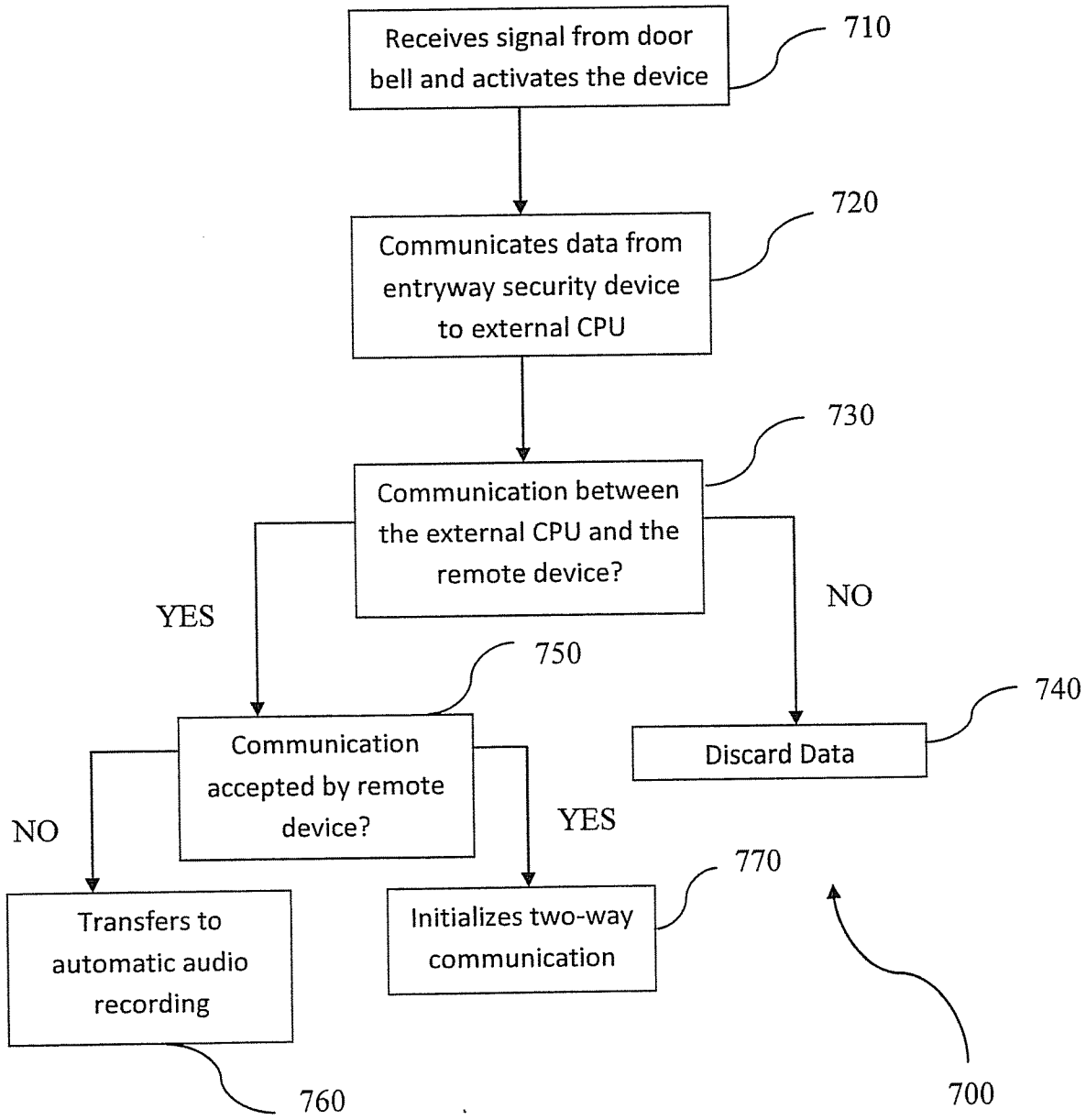

Receives signal from door bell and activates the device
710
Communicates data from entryway security device to external CPU
720
Communication between the external CPU and the remote device?
730
YES
NO
Communication accepted by remote device?
750
Discard Data
740
NO
YES
Transfers to automatic audio recording
760
Initializes two-way communication
770
700

FIGURE 8.

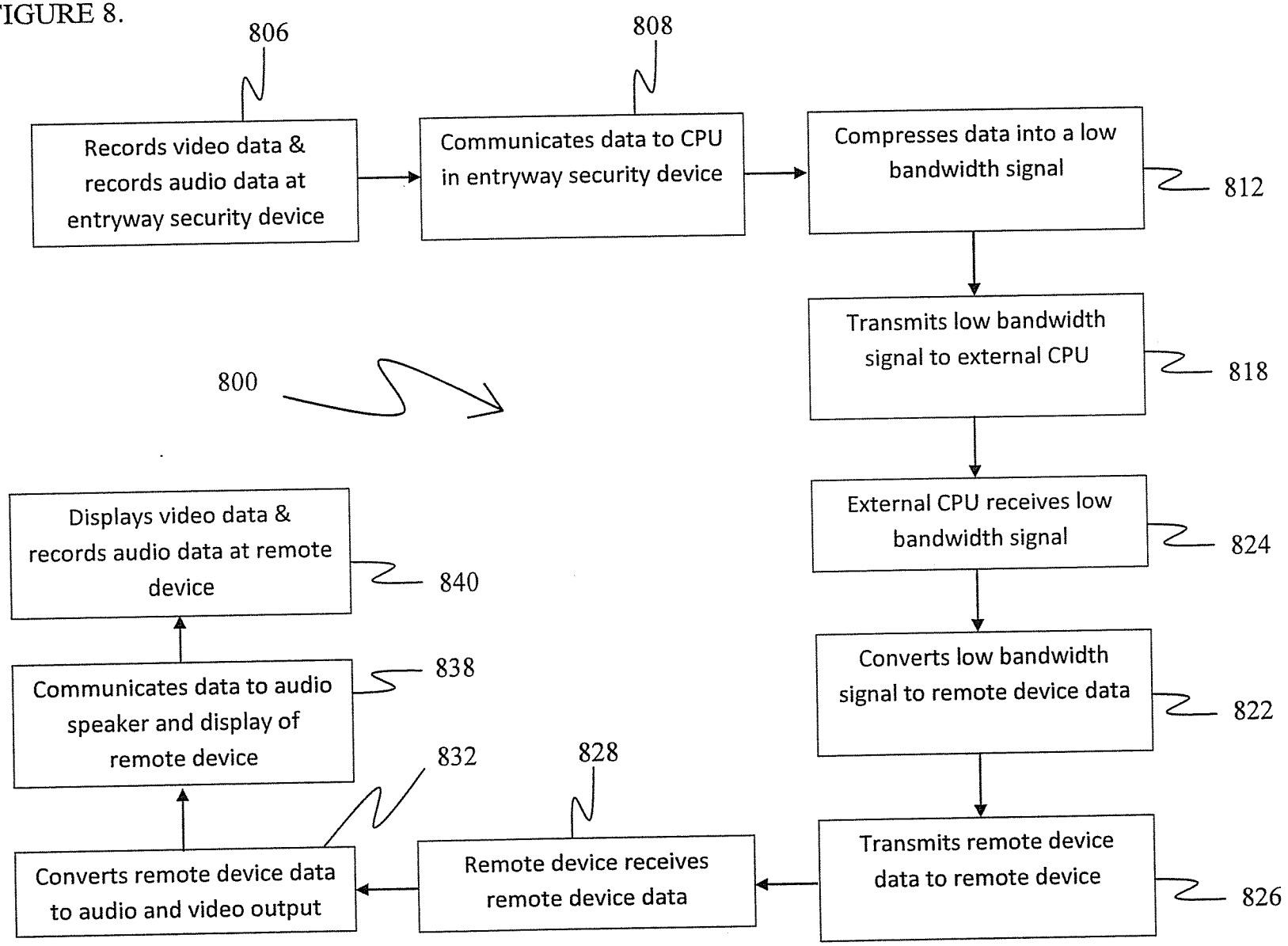

806
808
Records video data & records audio data at entryway security device
Communicates data to CPU in entryway security device
Compresses data into a low bandwidth signal
812
Transmits low bandwidth signal to external CPU
818
800
External CPU receives low bandwidth signal
824
Converts low bandwidth signal to remote device data
822
Transmits remote device data to remote device
826
Remote device receives remote device data
828
832
Converts remote device data to audio and video output
Communicates data to audio speaker and display of remote device
838
Displays video data & records audio data at remote device
840

FIGURE 9.

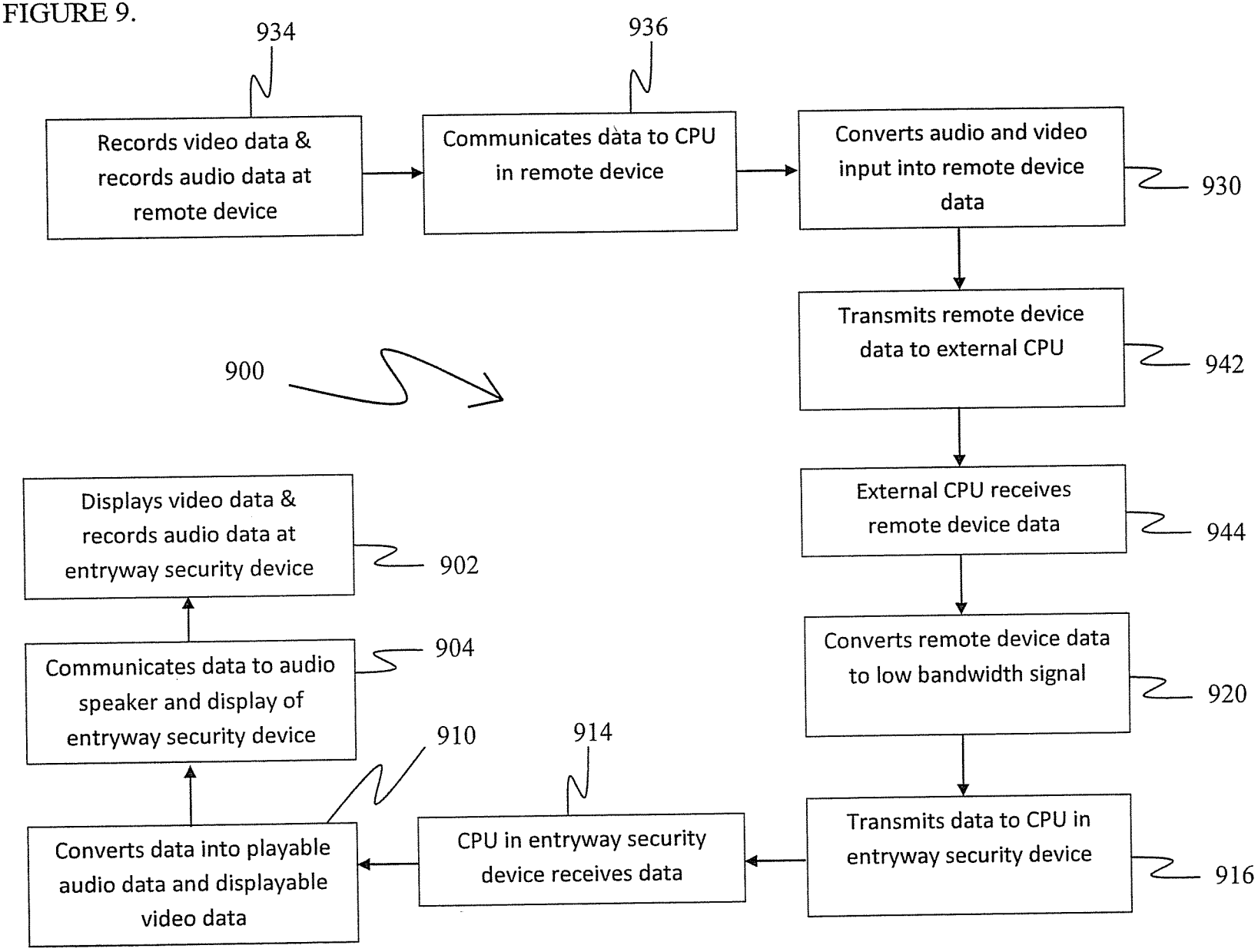

934
936
Records video data & records audio data at remote device
Communicates data to CPU in remote device
Converts audio and video input into remote device data
930
Transmits remote device data to external CPU
942
900
Displays video data & records audio data at entryway security device
902
External CPU receives remote device data
944
Communicates data to audio speaker and display of entryway security device
904
Converts remote device data to low bandwidth signal
920
910
914
Converts data into playable audio data and displayable video data
CPU in entryway security device receives data
Transmits data to CPU in entryway security device
916

FIGURE 10.

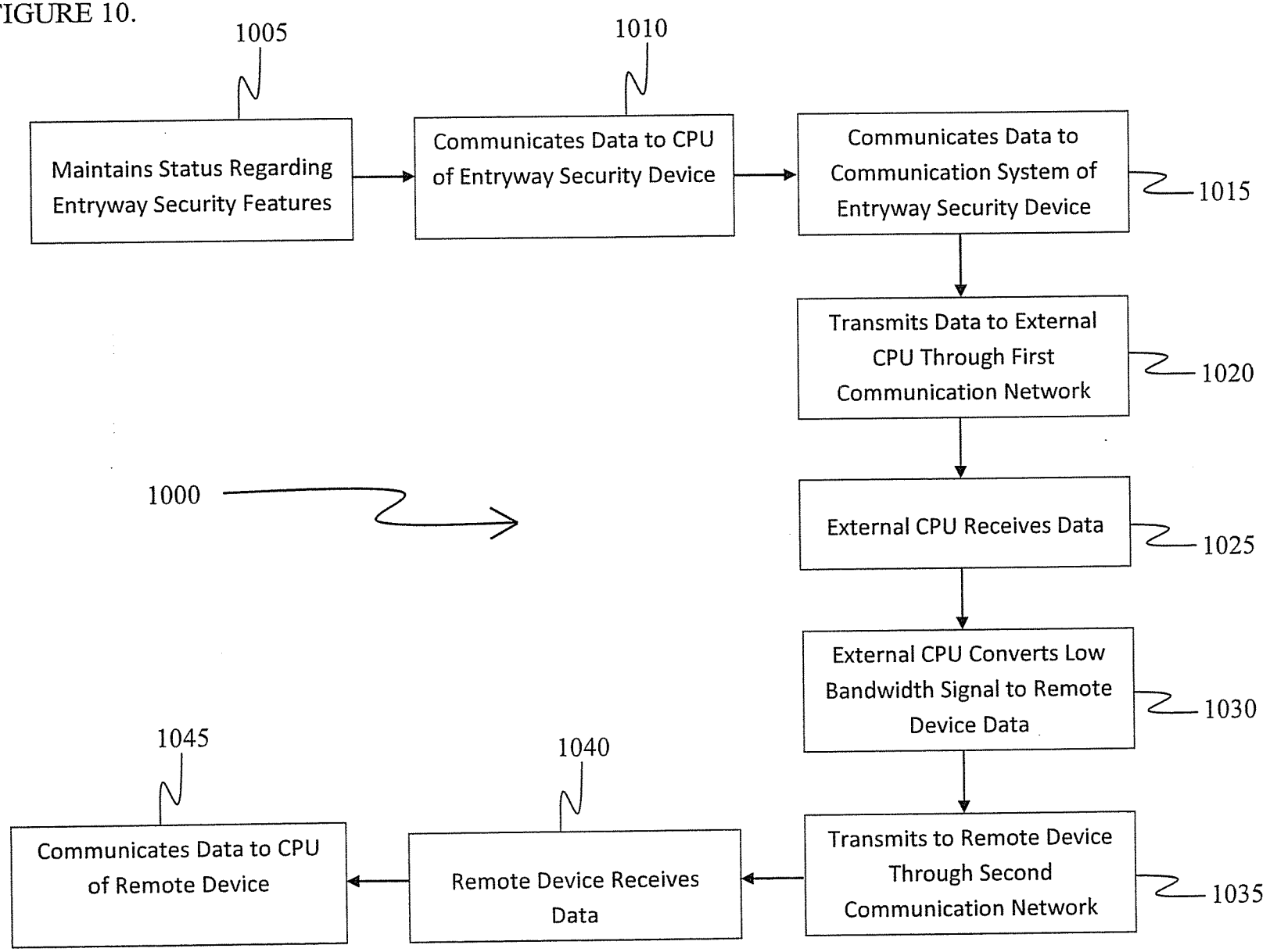

1005
1010
Maintains Status Regarding Entryway Security Features
Communicates Data to CPU of Entryway Security Device
Communicates Data to Communication System of Entryway Security Device
1015
Transmits Data to External CPU Through First Communication Network
1020
1000
External CPU Receives Data
1025
External CPU Converts Low Bandwidth Signal to Remote Device Data
1030
1045
1040
Communicates Data to CPU of Remote Device
Remote Device Receives Data
Transmits to Remote Device Through Second Communication Network
1035

FIGURE 11.

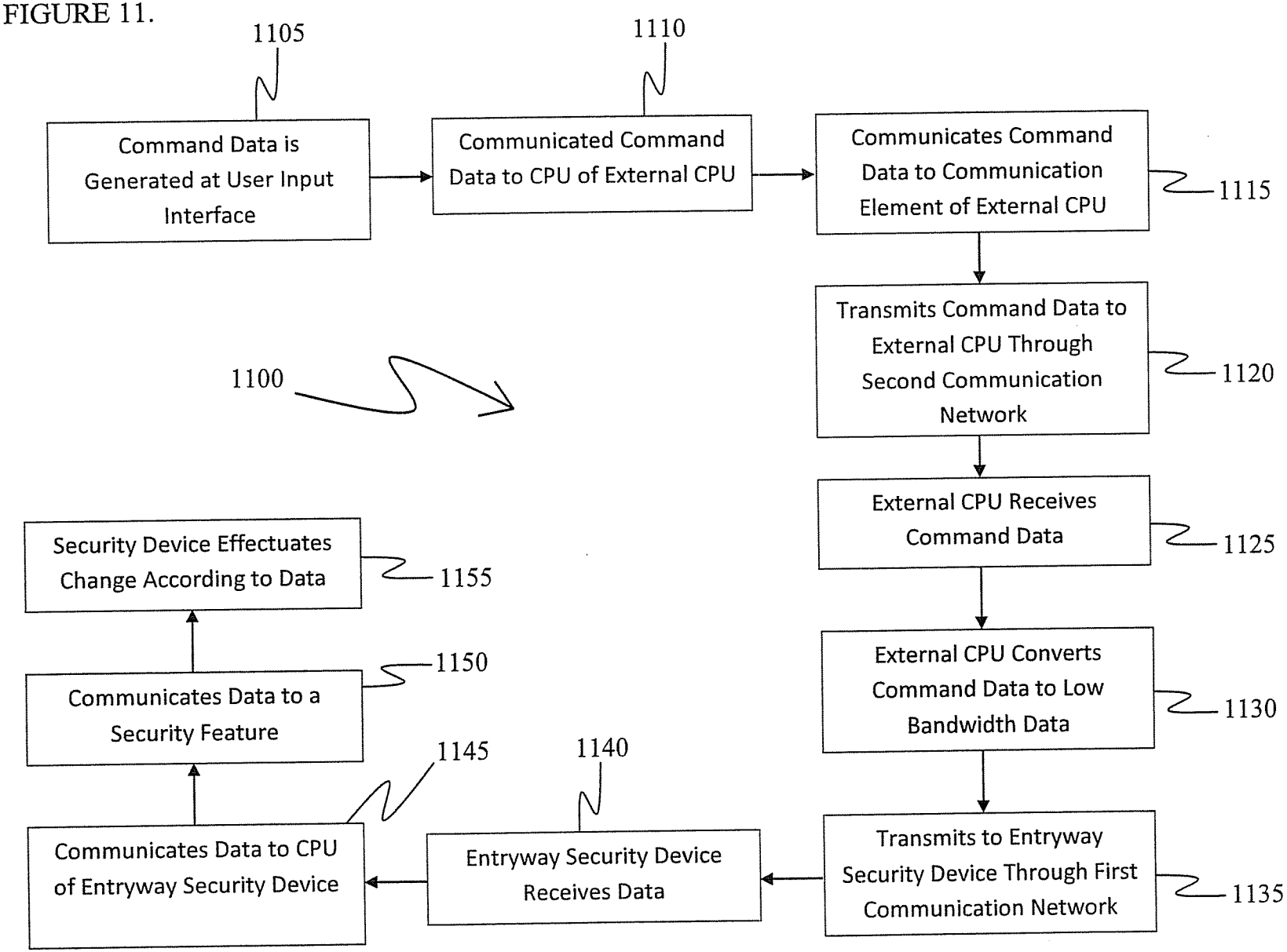

1105
Command Data is Generated at User Input Interface
1110
Communicated Command Data to CPU of External CPU
Communicates Command Data to Communication Element of External CPU
1115
Transmits Command Data to External CPU Through Second Communication Network
1120
1100
External CPU Receives Command Data
1125
External CPU Converts Command Data to Low Bandwidth Data
1130
Transmits to Entryway Security Device Through First Communication Network
1135
Entryway Security Device Receives Data
1140
Communicates Data to CPU of Entryway Security Device
1145
Communicates Data to a Security Feature
1150
Security Device Effectuates Change According to Data
1155

FIGURE 12.

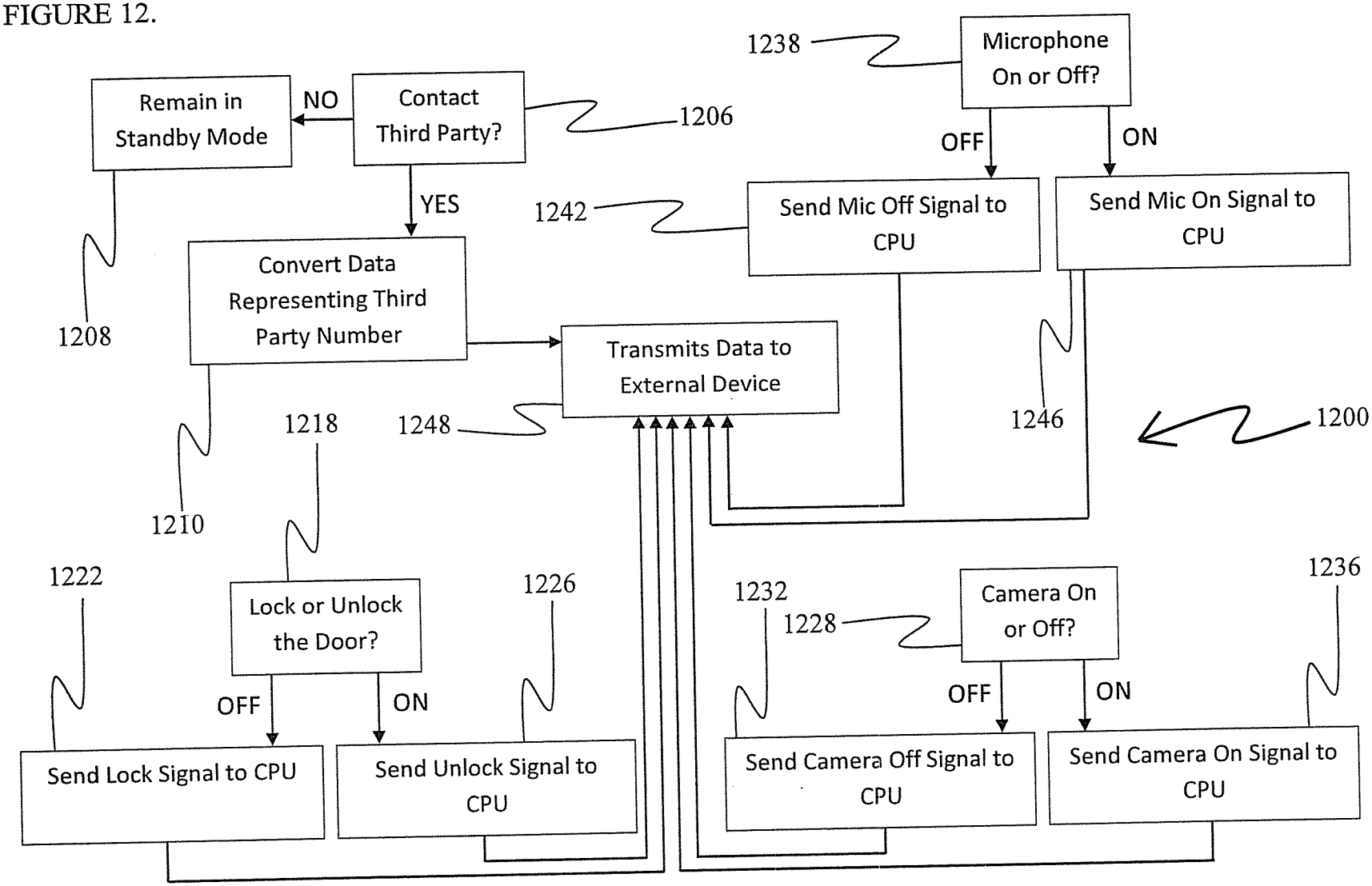
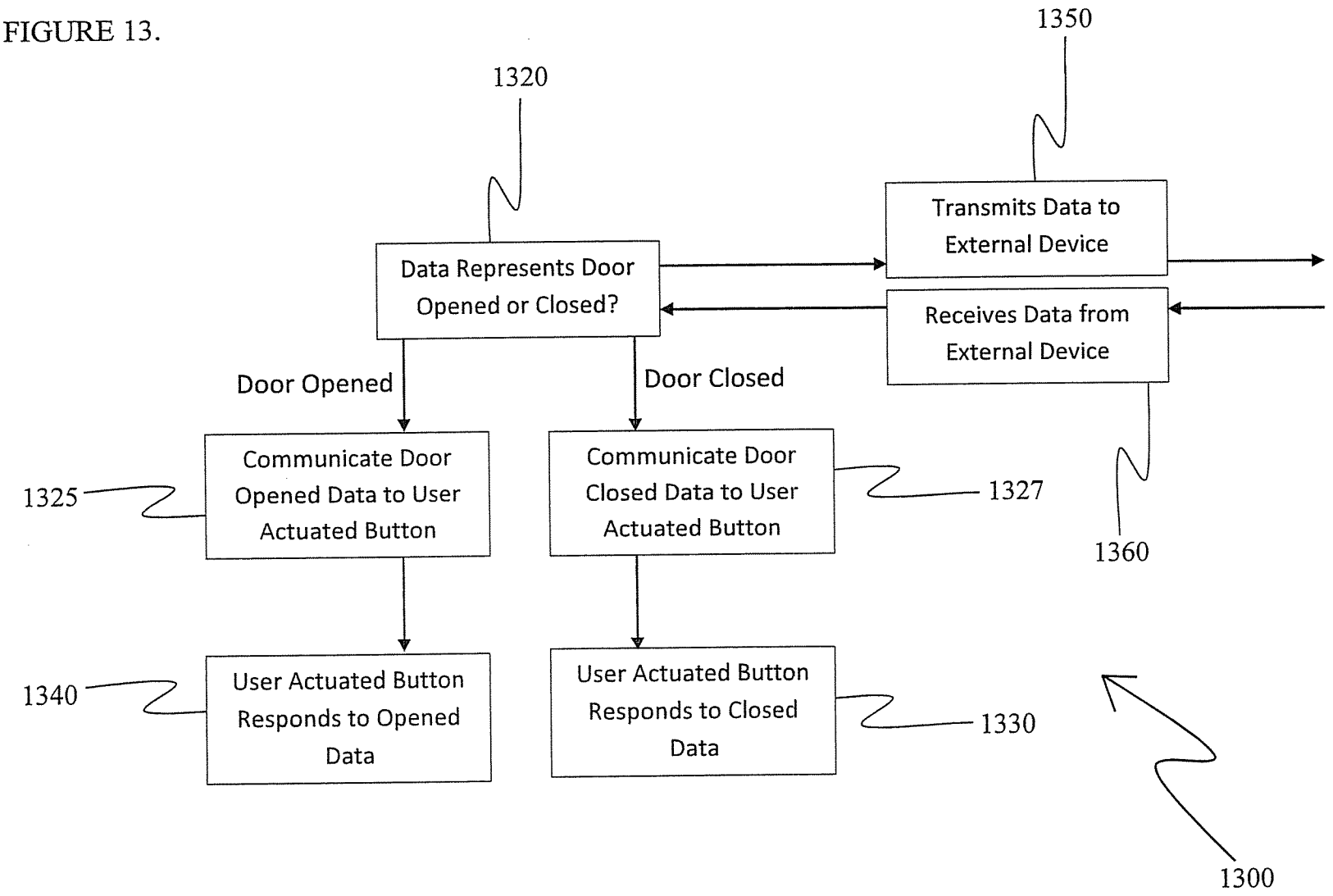

1238
Microphone On or Off?
OFF
ON
Remain in Standby Mode
NO
Contact Third Party?
1206
YES
1242
Send Mic Off Signal to CPU
Send Mic On Signal to CPU
1208
Convert Data Representing Third Party Number
Transmits Data to External Device
1248
1246
1200
1218
1210
1222
Lock or Unlock the Door?
1226
1232
1228
Camera On or Off?
1236
OFF
ON
OFF
ON
Send Lock Signal to CPU
Send Unlock Signal to CPU
Send Camera Off Signal to CPU
Send Camera On Signal to CPU

FIGURE 13.


1350
1320
Transmits Data to External Device
Data Represents Door Opened or Closed?
Receives Data from External Device
Door Opened
Door Closed
Communicate Door Opened Data to User Actuated Button
1325
Communicate Door Closed Data to User Actuated Button
1327
1360
User Actuated Button Responds to Opened Data
1340
User Actuated Button Responds to Closed Data
1330
1300