



(51) International Patent Classification:
H04L 9/12 (2006.01)

(21) International Application Number:
PCT/US2014/027863

(22) International Filing Date:
14 March 2014 (14.03.2014)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
61/794,933 15 March 2013 (15.03.2013) US

(71) Applicants: **MASTER LOCK COMPANY** [US/US]; 137 West Forest Hill Avenue, Oak Creek, Wisconsin 53154 (US). **VARDR PTY. LTD.** [AU/AU]; 35 Upper Almora Street, Mosman, New South Wales 2088 (AU).

(72) Inventors: **SMITH, Geoff**; 7 Panorama Place, Mt. Gravatt East, Queensland 4122 (AU). **FITZPATRICK, Matthew**; 35 Upper Almora Street, Mosman, New South Wales 2088 (AU). **CELINSKI, Tom**; 35 Upper Almora Street, Mosman, New South Wales 2088 (AU).

(74) Agents: **REICHENBERGER, Karl, F.** et al.; Foley & Lardner LLP, 3000 K. Street N.W., Suite 600, Washington, District of Columbia 20007-5109 (US).

(81) Designated States (*unless otherwise indicated, for every kind of national protection available*): AE, AG, AL, AM,

AO, AT, AU, AZ, BA, BB, BG, BH, BN, BR, BW, BY, BZ, CA, CH, CL, CN, CO, CR, CU, CZ, DE, DK, DM, DO, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, GT, HN, HR, HU, ID, IL, IN, IR, IS, JP, KE, KG, KN, KP, KR, KZ, LA, LC, LK, LR, LS, LT, LU, LY, MA, MD, ME, MG, MK, MN, MW, MX, MY, MZ, NA, NG, NI, NO, NZ, OM, PA, PE, PG, PH, PL, PT, QA, RO, RS, RU, RW, SA, SC, SD, SE, SG, SK, SL, SM, ST, SV, SY, TH, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, ZA, ZM, ZW.

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

Declarations under Rule 4.17:

— *as to applicant's entitlement to apply for and be granted a patent (Rule 4.17(ii))*

Published:

— *without international search report and to be republished upon receipt of that report (Rule 48.2(g))*

(54) Title: SYSTEMS AND METHODS FOR CONFIGURATION OF WIRELESS CAMERA

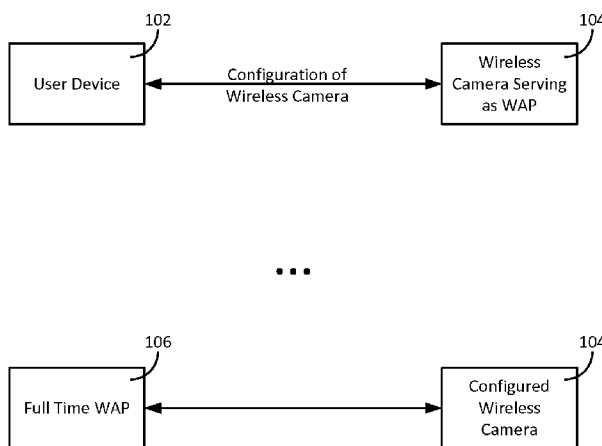


FIG. 1

(57) Abstract: Systems and methods for configuring a wireless camera to connect to a wireless access point are provided. The systems and methods include wirelessly connecting to a client device and transmitting an encryption key to the client device. The systems and methods also include receiving encrypted data from the client device and decrypting the data using the encryption key. The encrypted data may include an identifier and an access code. The systems and methods further include wirelessly connecting to the wireless access point using the decrypted data.



SYSTEMS AND METHODS FOR CONFIGURATION OF WIRELESS CAMERA

CROSS-REFERENCE TO RELATED PATENT APPLICATION

[0001] This application claims the benefit of and priority to U.S. Provisional Patent Application Serial Number U.S. 61/794,933, filed March 15, 2013, which is incorporated by reference.

BACKGROUND

[0002] The present disclosure relates generally to cameras, and, more specifically, to wireless cameras that may be used for security or other monitoring purposes.

[0003] Cameras may be used to monitor locations, items, and/or people. In some instances, cameras may be positioned about a building to monitor entrances, exits, rooms inside of the building, objects within the building and/or other aspects of a building or the items inside the building. Some camera systems include wiring to transmit video to a monitor and/or recording device such that the video captured by the security camera may be viewed at a remote position relative to the position of the security camera. In some instances, the video that is transmitted from one or more of the cameras may be stored on a storage device, such as a hard drive, for later viewing or reference.

SUMMARY

[0004] One embodiment relates to a method for configuring a wireless camera to connect to a wireless access point. The method includes wirelessly connecting to a client device. The method further includes transmitting an encryption key to the client device. The method further includes receiving encrypted data from the client device. The encrypted data includes an identifier and an access code. The method further includes decrypting, using a processing circuit of the wireless camera and the encryption key, the encrypted data. The method further includes wirelessly connecting to the wireless access point using the decrypted data.

[0005] Another embodiment relates to a method for connecting a wireless camera to a wireless access point. The method includes activating the wireless camera to serve as a temporary wireless access point. The method further includes wirelessly connecting to the wireless camera as the temporary wireless access point via a client device. The method further includes transmitting, at the client device, an encryption key from the wireless camera. The method further includes encrypting, at the client device, one or more identifiers and one or more access codes. The one or more identifiers and the one or more access codes are associated with one or more wireless access points. The method further includes transmitting the encrypted one or more identifiers and one or more access codes to the wireless camera.

[0006] Another embodiment relates to a computer-implemented method for configuring a wireless camera to connect to a wireless access point. The method includes activating an access point mode of the wireless camera. The method further includes providing speech audio via a speaker of the wireless camera indicating that the access point mode is activated. The method further includes broadcasting an SSID associated with the wireless camera. The method further includes receiving a request from a client device to connect to the wireless camera. The method further includes wirelessly connecting to the client device. The method further includes transmitting an encryption key to the client device. The encryption key is uniquely associated with the wireless camera. The method further includes receiving encrypted data from the client device. The encrypted data is encrypted using the encryption key and the encrypted data includes an identifier and an access code. The method further includes decrypting, using a processing circuit of the wireless camera, the encrypted data. The method further includes identifying a wireless device based, at least in part, on the identifier. The method further includes wirelessly connecting to the wireless device using the identifier and access code.

[0007] Another embodiment relates to a method for configuring a wireless camera to connect to a wireless access point. The method includes placing the wireless camera into an access point emulation mode, where the wireless camera appears to be an access point to other client devices such as smartphones and laptops. The method further includes connecting a client device to the wireless camera which is acting like an access point, the client having asked for information from the user of the client device. The client device

passes to the wireless camera the following information: (a) one or more pairs of SSID & Passphrase that provide the information for the wireless camera to connect as a client to one or more true access points, and (b) an invitation token acquired by the client device from a cloud service that identifies the account and location to which the wireless camera should be attached. Having received the above information from the client device, the wireless camera exits the emulated access point mode. The wireless camera uses the SSID/passphrase information provided to connect as a client to one of the access points.

[0008] If successful in associating to the access point, the wireless camera can then connect to the cloud service. The wireless camera sends the invitation token it received from the client device to the cloud service. The cloud service verifies the token as one that it has recently issued and if valid associates the wireless camera into the location and account of the user. In varying embodiments, the client device may send, along with the invitation token and SSID/passphrases, the internet domain of the service to which the wireless camera should connect. There may be two sets of SSID/passphrases given: a first set for the main access point to be used by the wireless camera and the second set for a backup access point. The wireless camera may give priority to using the main access point. The client device may be at least one of a desktop, laptop, and mobile phone. An audio message may be played to the user when the wireless camera enters the emulated access point mode. An audio message of success or failure is played when the wireless camera successfully associates with the access point and connects to the cloud service (or not). The wireless camera may maintain the emulated access point mode and interleave a client mode with the emulated mode to test that the wireless camera can associate with every SSID/passphrase which the wireless camera has been given. The wireless camera may return the status of these tests to the client while operating in its emulated access point mode. The information may be passed back and forth between the client device and the wireless camera using JSON encoded data formats, either encrypted or in plain text. The client device can automatically identify devices in emulated access point mode by the fact that there is well defined prefix to the SSID that the device broadcasts (e.g. "EMAPP-"). In some embodiments, a first device (e.g., camera) may be in an emulated access point mode while a second device (e.g., camera) may act like a client and associate with the first device. The first device may then pass to the second device the information that the first device

contains about the SSID/passphrase of available access points and information about the account/location to which the camera is attached.

BRIEF DESCRIPTION OF THE FIGURES

[0009] The disclosure will become more fully understood from the following detailed description, taken in conjunction with the accompanying figures, wherein like reference numerals refer to like elements, in which:

[0010] FIG. 1 is a block diagram providing an overview of the configuration activity of systems and methods described herein, according to varying exemplary embodiments;

[0011] FIG. 2 is a block diagram of a wireless camera according to an exemplary embodiment;

[0012] FIG. 3 is a flow diagram of an exemplary process for configuring a wireless camera to connect to a device according to an exemplary embodiment;

[0013] FIG. 4 is an overview of an example sequence of transmissions between a wireless camera, user device, and device associated with wireless access information;

[0014] FIG. 5 is an overview of an example user interface webpage for configuring a wireless camera according to an exemplary embodiment; and

[0015] FIG. 6 is an overview of an example user guide having a link to a configuration webpage for configuring a wireless camera according to an exemplary embodiment.

DETAILED DESCRIPTION

[0016] Before turning to the figures, which illustrate the exemplary embodiments in detail, it should be understood that the application is not limited to the details or methodology set forth in the description or illustrated in the figures. It should also be understood that the terminology is for the purpose of description only and should not be regarded as limiting.

[0017] Referring generally to the figures, systems and methods for configuring a wireless camera to regularly transmit to and receive data from a wireless access point are shown and described. A process to configure the wireless camera may include initially connecting to the wireless camera with a client device (e.g., a mobile phone, a laptop computer, a desktop computer, a tablet, etc.) and transmitting access information to the wireless camera such that

the wireless camera may subsequently communicate with a wireless access point using the information. The process may include one or more security measures to prevent unauthorized access to the wireless camera configuration information. Some examples of such security measures may include password protection or encryption for one or more aspects of the wireless camera configuration information. The systems and methods of the present disclosure may be of use when the wireless camera does not include buttons or any other user interface controls for viewing and/or entering information for configuring communications.

[0018] Once the wireless camera is configured for regular communication to the wireless access point, the wireless camera may provide video information (e.g., pictures, videos, etc.) to remote sources (e.g., an Internet connected server, other devices connected to the WLAN, etc.). For example, if the wireless camera includes and/or is associated with a motion detector, a motion notification may be transmitted over the Internet to one or more servers and/or user devices. In some instances, the notification may be sent to more than one user such that at least one individual may notify the owner of the camera or the police of activity that is occurring in view of the camera. Thus, a social-network based neighborhood watch may be formed using such wireless cameras.

[0019] FIG. 1 is a block diagram providing an overview of the configuration activity of systems and methods described herein. The first communicating nodes in FIG. 1 illustrate a user device 102 (i.e., a client device) in communication with a wireless camera 104 serving as a wireless access point (WAP). During the direct connection with user device 102 (e.g., a mobile phone, a tablet, a laptop, a desktop, etc.) wireless camera 104 serving as the WAP can provide user interfaces (e.g., web pages) to user device 102. The user interfaces may include fields for population by a user (e.g., using user interface controls of user device 102). The user interfaces may prompt the user for configuration information that may allow camera 104 to connect for regular communications to a full time wireless access point 106. Once the fields are populated and the configuration information is received by wireless camera 104 serving as a WAP, wireless camera 104 serving as a WAP can disconnect user device 102 and continue serving as a WAP. Then, wireless camera 104 can use the received configuration information to form a regular and authenticated communications connection to full time WAP 106. Thereafter, the configured wireless camera 104 can regularly

communicate with the Internet, servers on the Internet, or other networks or devices via full time WAP 106. The systems and methods for forming the connections and exchanging the connection information will be described in greater detail below in reference to FIGS. 2-6.

[0020] Referring to FIG. 2, an example block diagram of wireless camera 104 is shown. The wireless camera 104 is shown to include a housing 110. The housing 110 may house or carry a power source 120. The wireless camera 104 is shown to include a wireless camera imaging sensor and circuitry 130. The wireless camera 104 is further shown to include a processing circuit 151.

[0021] The processing circuit 151 is shown to include a wireless circuit 140, a processor 150, and memory 152, a user interface 190, a motion sensor 160, a feedback indicator 180, and a light 170. As shown in FIG. 2, processing circuit 151 may include a subset of the components of wireless camera 104 (e.g., wireless circuit 140, processor 150, memory 152) and the processing circuit 151 may be communicably coupled to other components of wireless camera 104 (e.g., sensor and circuitry 130, power source 120, motion sensor 160, light 170, feedback indicator 180). Power source 120 may be coupled to wireless camera imaging sensor and circuitry 130, processing circuit 151, and user interface 190 either directly or indirectly (e.g., electrical power from power source 120 may be directly coupled to circuitry 130 or power may be provided to processing circuit 151 and thereafter provided to circuitry 130). In addition, wireless camera imaging sensor and circuitry 130 may be communicatively coupled to processing circuit 151 such that video data from sensor and circuitry 130 may be transmitted to processing circuit 151. The processing circuit 151 may subsequently transmit the video data via wireless circuit 140 to a user device. User interface 190 may also be communicatively coupled to processing circuit 151 such that a user may directly interact with one or more features of wireless camera 104, as will be described in greater detail below.

[0022] Power source 120 of the present example includes one or more batteries such that wireless camera 104 is provided electrical power and is portable. Power sources other than or in addition to a battery may be used, in various embodiments. For example, a power cord for wireless camera 104 may be provided. Wireless camera 104 may not use a portable power source, in some embodiments. In some versions, a back-up power source may be provided such that wireless camera 104 may continue to operate if power source 120 fails

and/or is otherwise unable to provide electrical power to one or more components of wireless camera 104 (e.g., batteries may be provided as a back-up power source for a corded camera and/or a secondary battery may be provided as a back-up power source for a primary battery).

[0023] Wireless camera imaging sensor and circuitry 130 may include any kind of camera configuration to capture and transmit video, including, but not limited to, digital charged-coupled devices (CCD) sensors, complementary metal-oxide-semiconductor (CMOS) active pixel sensors, hybrid CMOS/CCD sensors, thermal sensors, or any other type of camera sensors.

[0024] Wireless circuit 140 may include any kind of wireless circuitry for transmitting and/or receiving data from another wireless device. Examples of wireless circuit 140 may include a wireless network interface controller configured for a radio-based network (e.g., a WiFi adapter or the like), a Bluetooth® adapter, and/or any other wireless circuit. In some versions, wireless circuit 140 may instead include an RFID or NFC module configured to transmit and/or receive data via an RF signal, though this is merely optional. Thus it should be understood that wireless circuit 140 may include any device, component, etc. that is capable of transmitting and/or receiving data wirelessly.

[0025] Processing circuit 151 may include a processor 150 and a memory 152. Memory 152 may store machine instructions that, when executed by processor 150 cause processor 150 to perform one or more of the operations described herein. Processor 150 may include a microprocessor, ASIC, FPGA, etc., or combinations thereof. Memory 152 may include, but is not limited to, electronic, optical, magnetic, and/or any other storage or transmission device capable of providing the processor with program instructions. Memory 152 may be a non-transient computer-readable medium. Memory 152 may include a floppy disk, CD-ROM, DVD, magnetic disk, memory chip, ROM, RAM, EEPROM, EPROM, flash memory, optical media, or any other suitable memory from which the processor can read instructions. The instructions may include code from any suitable computer programming language such as, but not limited to, C, C++, C#, Java, JavaScript, Perl, HTML, XML, Python and Visual Basic.

[0026] User interface 190 of the present example is communicatively coupled to processing circuit 151 such that a user may interact with one or more features of wireless

camera 104. For example, user interface 190 may include a mechanical switch or button that, when toggled or depressed, causes processing circuit 151 to perform one or more processes. By way of example only, user interface 190 may include more than one button, such that a plurality of processes may be activated via a user's interaction with user interface 190. In other versions, user interface 190 may include a touch screen such that a user may activate one or more processes via touching a corresponding region of the touch screen. In still other versions, user interface 190 may include a voice recognition module such that one or more vocal commands by a user may be used to activate one or more processes via processing circuit 151. Still further user interfaces 190 may be implemented according to other embodiments.

[0027] Optionally, a motion sensor 160, a light 170, and/or a feedback indicator 180 may also be included with wireless camera 104 and be communicably coupled to processing circuit 151. Motion sensor 160 may be communicatively coupled to processing circuit 151 such that processing circuit 151 may utilize output from the motion sensor 160 as input. Such input may be used to trigger or otherwise cause to be executed one or more instructions, such as activating sensor and circuitry 130, transmitting video data via wireless circuit 140, activating light 170 and/or otherwise. Light 170 is communicatively coupled to processing circuit 151 and may include any suitable device that may serve as a light source. For example, light 170 may be one or more light emitting diodes (LEDs), an incandescent bulb, or another light source.

[0028] Feedback indicator 180 is also communicatively coupled to processing circuit 151. Feedback indicator 180 may include any device capable of providing audible, visual, and/or tactile feedback to a user. For example, feedback indicator 180 may include a speaker which may output one or more sounds, such as a reproduced or synthesized voice, to provide feedback to the user. Such feedback may include a status of wireless camera 104 during various steps of a configuration process, such as those described in reference to process 300 shown in FIG. 3. In other situations, such feedback may be of a status of wireless camera 104 before and/or after such a configuration. In other implementations, feedback indicator 180 may include a visual indicator, such as an LED light, an LCD display, etc. such that visual indications may be provided to the user for any or all of the aforementioned feedback. In still further implementations, feedback indicator 180 may

include tactile feedback indicators, such as haptic feedback. Other feedback indicators 180 may be utilized according to varying embodiments.

[0029] Still further configurations and/or components for wireless camera 104 may be provided. In addition, one or more of the components mentioned herein may be omitted, added, combined with other components, and/or otherwise. While the foregoing has generally described some example environments for wireless camera 104, a user may desire that output of wireless camera 104 be accessible to the user, a device, and/or to other persons or devices. For example, as noted above, in some instances video data from wireless camera 104 may be implemented on a local webpage (e.g., as a streaming video feed or otherwise) to be viewable by a user (e.g., user device) who has access to such a local webpage. In some versions, the video data may be output to any suitable device having a display, such as a television, smart television, laptop computer, desktop computer, tablet, mobile phone, etc. such that the video data may be displayed in substantially real-time.

[0030] In other versions, the video data from wireless camera 104 may be stored as one or more video files, either locally on a storage device of wireless camera 104, such as the memory 152 of processing circuit 151 and/or otherwise, or remotely stored on another storage device, such as a remote hard drive, a flash drive, etc. Such video files may then be accessible at a later time, date, and/or place for viewing and/or archiving.

[0031] In yet another example, if wireless camera 104 is connected to a wireless access point that is connected to the internet, a user may remotely access the video data via a webpage, mobile application, and/or otherwise. Examples of such remote access may include access via a customized webpage, via a social networking webpage, via a mobile or other application on the user's mobile phone, tablet, or other electronic device (e.g., via FaceTime™ by Apple®, Skype®, video chat or Hangout™ by Google®, etc.), and/or otherwise.

[0032] In still further versions, wireless camera 104 and/or another device may transmit notifications or other information to the user regarding the status or other aspect of wireless camera 100. For example, if wireless camera 104 includes and/or is associated with a motion detector, such as motion sensor 160, a notification may be transmitted over the Internet to one or more users through one or more notification methods. In another version, if processing circuit 151 detects that power source 120, such as batteries, has a low output

and/or a back-up power source is activated, a notification of such a power failure may be transmitted through one or more notification methods. Still further triggers for notifications may be implemented as well. Such notification methods may include a Facebook® message or notification, a tweet via Twitter®, an SMS message sent to a user's mobile phone, a mobile application notification, an e-mail, a Google® chat message, an iChat™ by Apple® message, a phone call, and/or the like. In some instances, the notification may be sent to more than one user such that at least one individual may notify the owner of the camera or the police of activity that is occurring in view of the camera. Thus, a social-network based neighborhood watch may be formed using such wireless cameras.

[0033] To implement one or more of the foregoing examples, a user may initially configure wireless camera 104 to access a wireless device. Referring to FIG. 3, an example process 300 for configuring wireless camera 104 to access a wireless access point or other wireless device is shown.

[0034] Process 300 may begin with a user activating an access point mode via a user interface, such as user interface 190 described above (step 302). For example, a button having an indicator for "Access Point Mode Configuration" may be provided with which a user may activate the access point mode. Other user interfaces, such as a touch screen icon, a voice command, and/or otherwise may be provided such that the user may activate the access point mode. Further still, in some versions, initially powering on wireless camera 104, such as by inserting batteries, removing a non-conductive tab, and/or plugging in wireless camera 104, may automatically initiate access point mode for wireless camera 104.

[0035] Wireless camera 104 may be configured to behave in a similar manner to a wireless access point when the wireless access point mode is activated. For instance, process 300 may continue by wireless camera 104 broadcasting a service set identifier (SSID) (step 304). The SSID may include any identifier, including one associated with wireless camera 104. One example of an SSID for wireless camera 104 may be "VR-12-34-56" shown as identifier 590 in FIG. 5. The SSID may include a model name and one or more alphanumeric characters of the wireless camera's Media Access Control (MAC) address. In other versions, the SSID may contain one or more of a model number, serial number, company name, etc. In still further versions, the SSID may be customizable by a user before, during, and/or after configuration of wireless camera 104. In some versions,

the SSID may be randomly generated and/or generated using an encryption algorithm such that entry of the SSID may be unique for each wireless camera 104. In yet further versions, the SSID may not be broadcasted and instead an unnamed network may be indicated at a user device such that the user may connect to the unnamed network and enter the correct SSID to successfully connect to and/or access wireless camera 104, though this is merely optional. Still other variations for broadcasting the SSID and/or activating the access point mode may be provided.

[0036] Process 300 may include providing feedback that the access point mode is activated (step 306). In some versions, the feedback may be provided via a feedback indicator 180 including a speaker to provide audible feedback. For example, the speaker may emit an audio of a voice that states “I am in AP Configuration mode, please connect to me.” Other dialogue and/or other user feedback may be provided to indicate that the access point mode is activated (e.g., an LED light turning on or changing to a specific color, providing haptic feedback, etc.).

[0037] A user may then connect with wireless camera 104 using a user device (step 308), such as user device 102 shown in FIG. 1. Examples of such user devices include one or more of a desktop computer, a laptop computer, a mobile phone, a tablet, a gaming system, a vehicle, a smart television, a server, a watch, a personal digital assistant (PDA), etc.

[0038] In the instance of a laptop computer and/or mobile phone, the user may access a wireless networking menu and/or dialogue that displays one or more SSIDs. The user may select the SSID corresponding to the SSID for wireless camera 104 to connect with wireless camera 104. In some versions, an application (mobile or otherwise) may be downloaded and/or otherwise provided to the laptop computer and/or mobile phone. The user may utilize the application to select the SSID and/or other information may be input to the application to connect to wireless camera 104. By way of example only, an application may be configured such that the user inputs one of more pieces of data related to wireless camera 104 (e.g., serial number, MAC address, unique code provided, etc.) into an entry field of the application and the application may retrieve an SSID or other data such that the device running the application may connect with wireless camera 104. In some embodiments, the foregoing is optional.

[0039] In some versions, wireless camera 104 may include a dynamic host configuration protocol (DHCP) server such that the user device accessing wireless camera 104 can receive configuration information and be allocated an IP address on the network hosted by wireless camera 104 when in the access point mode. In some versions, wireless camera may be further configured to provide DNS services such that a web address, such as <http://VRCamera/>, may be translated into an IPv4 or IPv6 address, e.g., 192.168.2.1 or 2001:db8:85a3:42::8a2e:370:7334, though this is optional. In still further versions, wireless camera 104 may be configured to act as a miniature web server.

[0040] In some versions, in response to a request from the user device (step 310), wireless camera 104 may be configured to provide display data for a configuration webpage, such as webpage 500 shown in FIG. 5 (step 312). For example, processing circuit 151 may include one or more webpages that a user may request using the user device during the configuration process. For example, the user may request a webpage by typing in a site address into a web browser of the user device, if DNS services are available, by typing an IPv4 or IPv6 address into the web browser of the user device, and/or by utilizing an application configured to request the webpage. In some versions, a link may be provided on a configuration guide page, such as link 620 shown in FIG. 6, such that the user can request the webpage merely by clicking on the link and need not enter in the web or IP address, though this is merely optional. Wireless camera 104 may be configured to translate the request and transmit the requested data to the user device such that the requested webpage may be displayed to the user on the user device. In addition to the display data, wireless camera 104 may also include an encryption key. As will be discussed in further detail below, the encryption key may be used to encrypt information transmitted from the user device to wireless camera 104. In some implementations utilizing an application, the application may not need to access and/or receive display data for a webpage (e.g., an application may provide a form or other user interface locally on the user device), and may simply request the encryption key, though this is merely an example.

[0041] In some implementations, wireless camera 104 may scan for wireless access points or other wireless devices broadcasting an SSID or other identifier and may compile those SSIDs or other identifiers into a list. The list may be included with the display data for the webpage such that the user may simply select an identified SSID or other identifier. For

example, the webpage may include a dropdown menu, a plurality of radio buttons, or the like to list the SSIDs for the user to from. It should be understood that scanning for the SSIDs or other identifiers associated with wireless devices may be performed at a variety of different points, including, but not limited to, before, during, or after activation of the access point mode (step 302), before, during, or after the broadcast of the access point SSID of wireless camera 104 (step 304), before, during, or after connecting with the user device (step 308), before, during, or after the user device requests display data for the configuration webpage and/or encryption key (step 310), and/or before or during when wireless camera 104 provides display data for the configuration webpage and/or encryption key (step 312). In other embodiments, the scan for SSIDs or other identifiers for wireless devices may occur at any other point in time.

[0042] At the user device, such as a laptop computer, mobile phone, tablet, desktop computer, etc., the user may input wireless access information into designated fields of a displayed configuration webpage, such as fields 514, 516 of webpage 500 shown in FIG. 5, and/or into fields of an application (which may be similar to fields 514, 516). Wireless access information may include an SSID and access code for a wireless access point or other wireless device to which the user desires wireless camera 104 to connect. In some versions the access code may include, but is not limited to, a wired equivalent privacy (WEP) code, a Wi-Fi® Protected Access (WPA) code, a WPA2 code, a Bluetooth® PIN code, passphrase, and/or other access codes. The foregoing are exemplary. Other wireless access information may be utilized in other embodiments.

[0043] In some versions, the webpage and/or the application on the user device may scan a registry or other repository for wireless access information. The webpage and/or application may display the discovered wireless access information for selection. In some instances, more than one wireless access information set may be retrieved and presented for selection. For example, the webpage may include a dropdown menu, a plurality of radio buttons, or the like for the user to indicate which wireless access information to transmit to wireless camera 104. For example, a plurality of SSIDs for wireless access points may be listed for the user to select. Each SSID may be associated with a corresponding access code previously stored on the user device. Thus, the user may select the wireless access information without having to specifically recall the access code.

[0044] Once the wireless access information is input from the user and/or otherwise determined, the user may command the user device to submit or otherwise transmit the wireless access information to wireless camera 104. In some versions, the user device may utilize the transmitted encryption key to encrypt the wireless access information prior to transmitting the data to wireless camera 104 (step 314). For example, the encryption key may include a symmetric-key for a symmetric-key encryption algorithm and may be implemented using a stream cipher or a block cipher. The encryption key may be unique to each wireless camera 104, e.g., generated from a serial number for wireless camera 104, generated from a MAC address of wireless camera 104, and/or otherwise. In some versions, the encryption key may be randomly generated. In other versions, the encryption key may include encryption information for utilizing an asymmetric encryption algorithm (e.g., RSA, DSA, Cramer-Shoup, etc.), though this is optional. In some versions, only the payload of the transmission from the user device to wireless camera 104 may be encrypted. In some versions, the transmission of the encrypted wireless access information may occur automatically (e.g., upon complete entry of an identifier and access code or otherwise). In other versions, the transmission of the encrypted wireless access information may occur after user input (e.g., after a user selects a submission feature, post feature, or the like).

[0045] Wireless camera 104 receives the transmitted data and decrypts the wireless access information using the encryption key, such as via a stored symmetric key (step 316). In some versions, wireless camera 104 may store the wireless access information in a data storage, such as memory 152 of processing circuit 151 and/or another storage device (e.g. a flash memory), such that wireless camera 104 may retrieve the wireless access information for subsequent use. For example, wireless camera 104 may become disconnected from the wireless access point and/or other wireless device and may reconnect to the wireless access point and/or other wireless device using the stored wireless access information. Examples of when such a disconnection may occur include when wireless camera 104 is powered off or otherwise loses power and/or the wireless access point and/or wireless device is powered off or otherwise loses power. The foregoing may be optional. In some embodiments, wireless access information may be re-entered each time wireless camera 104 is to connect to the wireless access point and/or wireless device.

[0046] In some embodiments, encryption of the wireless access information may not occur such that wireless access information may be transmitted between the user device and wireless camera 104 without encryption or decryption.

[0047] In some implementations wireless camera 104 may disconnect from the user device once the wireless access information is received (step 318). For example, wireless camera 104 may automatically disconnect from the user device once the wireless access information is received, decrypted, and/or stored. In other versions, wireless camera 104 may utilize user input, such as via a button of user interface 190 shown in FIG. 2 or otherwise, to disconnect from the user device. In still further versions, the user may disconnect from wireless camera 104 via the user device (e.g., by disconnecting via a wireless networking menu or application and/or via a customized application for interacting with wireless camera 104).

[0048] With wireless camera 104 disconnected, wireless camera 104 may activate an operational mode (step 320). It should be understood that an operational mode may be different from the configuration mode. By way of example only, an operational mode may include testing one or more components of wireless camera 104 (such as sensor and circuitry 130, motion sensor 160, light 170, etc.), activating one or more components of wireless camera 104 (such as sensor and circuitry 130, motion sensor 160, light 170, etc.), transmitting video data via wireless circuit 140, or the like. In some versions, wireless camera 104 may automatically enter an operational mode once disconnected from the user device. In other versions, wireless camera 104 may require user input (for example, toggling or pressing a button via user interface 190) to enter the operational mode. In some other versions, wireless camera 104 may receive user input via the user's interactions with the user device prior to disconnecting from the user device. Still other processes to enter the operational mode may be used.

[0049] In the present example, the operational mode may begin by attempting to connect with the device that is associated with the wireless access information provided by the user (step 322). In the present example, the device may include a wireless access point, such as full time WAP 106 shown in FIG. 1, though this is merely optional. Wireless camera 104 may be configured to initiate a connection with the full time WAP 106 via an identifier, such as an SSID or other identifier. Wireless camera 104 may authenticate the wireless

connection with the full time WAP 106 using the access code included in the wireless access information, though this is merely optional (e.g., the user may not provide an access code if the wireless access point is hidden such that entry of the SSID is sufficient for authentication and/or if the wireless access point does not require an access code, such as a publicly available wireless access point). In some implementations, other wireless devices may be utilized, including a laptop computer, mobile phone, tablet, desktop computer, server, smart television, gaming system, etc. Accordingly, other identifiers and/or other access codes may be utilized to establish and/or authenticate a wireless connection with the aforementioned wireless devices. Still further ways to connect wireless camera 104 with a device associated with the wireless access information may be implemented.

[0050] In some instances, the wireless access information may be incorrect and/or the device associated with the wireless access information may be unavailable (e.g., turned off, out of range, etc.). In such instances, wireless camera 104 may provide feedback indicating that wireless camera 104 was unable to connect with the indicated device (step 324). By way of example only, feedback indicator 180 may include a speaker that may output an audible indicator, such as audio of a voice reciting “I cannot connect to the Access Point, please check the information you provided me.” In other versions, feedback indicator 180 may include a visual indicator, such as an LED that turns red or turns on an LED indicating an error and/or other visual feedback that wireless camera 104 was unable to connect with the indicated device. In still other versions, feedback indicator 180 may provide tactile or haptic feedback indicating a failure (e.g., two sequential vibrations). If wireless camera 104 has indicated a connection failure, process 300 may return to one of the foregoing steps. In the example shown in FIG. 3, process 300 returns to step 304 such that wireless camera 104 is configured to broadcast wireless camera 104’s SSID again for the user to reconnect using a user device. Process 300 may return to any of the other steps 302, 304, 306, 308, 310, 312, 314, 316, 318, 320, 322 and/or process 300 may end (e.g., wireless camera 104 may await further user input, wireless camera 100 may power off, and/or otherwise).

[0051] In some instances, when wireless camera 104 has successfully connected with the device associated with the wireless access information (e.g., full time WAP 106), wireless camera 104 may provide feedback indicating that wireless camera 104 successfully connected with the indicated device (step 326). By way of example, feedback indicator 180

may include a speaker that may output an audible indicator, such as a voice reciting “I have successfully connected, thank you.” In other versions, feedback indicator 180 may include a visual indicator, such as an LED that turns green, blinks, or turns on another LED indicating a successful connection and/or other visual feedback that wireless camera 104 successfully connected with the indicated device. In still other versions, feedback indicator 180 may provide tactile or haptic feedback indicating a successful connection (e.g., a single vibration).

[0052] Once a successful connection is made with the indicated device, wireless camera 104 may be utilized in accordance with any of the above-mentioned examples and/or in accordance with at least some of the teachings of U.S. Pat. Pub. No. 2012/0124203, entitled “Group Monitoring System and Method,” published May 17, 2012. The user may implement wireless camera 104 for other uses as well.

[0053] It should be understood that, while the foregoing description has described identifying and providing wireless access information for a single wireless device, such as full time WAP 106 shown in FIG. 1, multiple wireless access information sets may be provided by the user to wireless camera 104. Such wireless access information sets may be stored in a storage device of wireless camera 104. For example, if a user has a wireless access point and a tetherable tablet or mobile phone, the user may provide wireless access information for both the wireless access point and the tetherable tablet or mobile phone such that wireless camera 104 may connect to either. Other devices may be used as well, according to varying embodiments, including a mobile hotspot (MiFi), an aircard, etc. In addition, in some versions the user may be able to rank or otherwise provide an order for wireless camera 104 to access the plurality of wireless devices. For example, the user may provide an indication that a wireless access point is the primary connection device and a mobile hotspot is the secondary connection device. Providing wireless access information for multiple wireless devices to wireless camera 104 may provide a back-up capability in the event the primary and/or multiple wireless devices are disabled or otherwise inaccessible.

[0054] FIG. 4 depicts a general example of a sequence of transmissions between a wireless camera 104, user device 102, and/or a full time WAP 106 (e.g., device associated with wireless access information during configuration in an access point mode of the

wireless camera). As shown, wireless camera 104 may transmit data 410 indicative of an SSID associated with wireless camera 104. Such data 410 may be received by a user device 102. As previously discussed, user device 102 may include a variety of devices, include, but not limited to, a laptop computer, a mobile phone, a tablet, a desktop computer, a gaming system, a smart television, a server, etc. Wireless camera 104 and user device 102 may transmit and/or receive data 420 to establish a wireless connection. Once a wireless connection is established, user device 102 may transmit data 430 indicative of a request for webpage display data to wireless camera 104. Wireless camera 104 may receive the data 430 indicative of the request and may transmit data 440 to user device 102 that includes display data for a configuration webpage, such as webpage 500 shown in FIG. 5, and, optionally, an encryption key. A user may interact with the configuration webpage and input wireless access information, such as a device identifier (e.g., SSID for a wireless access point) and, optionally, an access code and/or other information. In response to user input to submit the wireless access information, user device 102 may, optionally, encrypt the wireless access information and transmit the encrypted data 450 to wireless camera 104. Wireless camera 104 receives the data 450 and, if encrypted, may decrypt the wireless access information. In some versions, wireless camera 104 may locally store the wireless access information for present and/or subsequent use. Wireless camera 104 may transmit and/or receive authentication data 460 to initiate wireless access authentication with device 106 identified in the wireless access information and, if provided, may transmit the corresponding access code. Once wireless access with the identified device 106 is established, wireless camera 104 may transmit and/or receive data 470 with device 106.

[0055] FIG. 5 depicts an example configuration webpage 500 that may be presented to a user at the user device when configuring wireless camera 104. In the present example, webpage 500 includes heading text with a wireless camera identifier 590, a plurality of entry fields 510, and a submission feature 520. Identifier 590 may correspond with the SSID of wireless camera 104 and/or may be any other identifier associated with wireless camera 104. In some versions, identifier 590 may be omitted entirely.

[0056] Entry fields 510 include a mode field 512, an ID field 514, and an access code field 516. Mode field 512 may be operable for a user to identify the operational mode of the wireless device for which the user is providing wireless access information. For example,

the mode may be indicated as Wireless G (IEEE 802.11g), Wireless B (IEEE 802.11b), Wireless A (IEEE 802.11a), Wireless N (IEEE 802.11n), IEEE 802.11ac, IEEE 802.11ad, Bluetooth®, etc. In some versions, mode field 512 may include a pre-populated dropdown menu, a plurality of a pre-populated radio buttons, a text entry field for manual entry, and/or otherwise. Mode field 512 may be optional and may be omitted in some embodiments.

[0057] ID field 514 may be operable for a user to provide an identifier associated with the wireless device for which wireless access information is being provided. In some versions ID field 514 may include a text entry field into which a user manually types the identifier. In other versions, ID field 514 may include a pre-populated dropdown menu and/or pre-populated radio buttons associated with identifiers (such as SSIDs) for wireless devices resulting from a scan by wireless camera 104. In some other versions, ID field 514 may be pre-populated by a scan of the user device's registry or other repository for wireless access information. Other configurations for ID field 514 may be implemented in varying embodiments.

[0058] Access code field 516 may be operable for a user to provide an access code for the wireless device for which wireless access information is being provided. In some versions access code field 516 may include a text entry field into which a user manually types the access code. In some versions, such as when a scan of the user device's registry or other repository for wireless access information is performed, access code field 514 may be omitted.

[0059] Submission feature 520 includes a selectable button that the user may click or otherwise interact with such that the information provided in fields 510 is transmitted, and optionally encrypted, to wireless camera 104.

[0060] Illustrated webpage 500 is merely an example. Webpage 500 may be formatted for mobile access and/or may be incorporated into an application for a mobile phone, tablet, laptop computer, or the like.

[0061] FIG. 6 depicts a configuration guide 600 having configuration instructions 610 that include a link 620. Link 620 may include a web address, such as <http://VRCamera/>, and/or may include an IPv4 or IPv6 address, e.g., 192.168.2.1 or 2001:db8:85a3:42::8a2e:370:7334. Thus, guide 600 may be presented to the user on a user device during configuration such that the user may select link 620 to access the

configuration webpage, such as webpage 500, without manually entering the web address and/or IP address for wireless camera 104. Guide 600 may be optional and may be omitted or modified according to varying embodiments.

[0062] It is important to note that the construction and arrangement of the elements of the systems and methods as shown in the exemplary embodiments are illustrative only.

Although only a few embodiments of the present disclosure have been described in detail, those skilled in the art who review this disclosure will readily appreciate that many modifications are possible (e.g., variations in sizes, dimensions, structures, shapes and proportions of the various elements, values of parameters, mounting arrangements, use of materials, colors, orientations, etc.) without materially departing from the novel teachings and advantages of the subject matter recited. For example, elements shown as integrally formed may be constructed of multiple parts or elements. It should be noted that the elements and/or assemblies of the enclosure may be constructed from any of a wide variety of materials that provide sufficient strength or durability, in any of a wide variety of colors, textures, and combinations. Additionally, in the subject description, the word “exemplary” is used to mean serving as an example, instance, or illustration. Any embodiment or design described herein as “exemplary” is not necessarily to be construed as preferred or advantageous over other embodiments or designs. Rather, use of the word “exemplary” is intended to present concepts in a concrete manner. Accordingly, all such modifications are intended to be included within the scope of the present inventions. The order or sequence of any process or method steps may be varied or re-sequenced according to alternative embodiments. Any means-plus-function clause is intended to cover the structures described herein as performing the recited function and not only structural equivalents but also equivalent structures. Other substitutions, modifications, changes, and omissions may be made in the design, operating conditions, and arrangement of the preferred and other exemplary embodiments without departing from scope of the present disclosure or from the spirit of the appended claims.

[0063] The present disclosure contemplates methods, systems, and program products on any machine-readable media for accomplishing various operations. The embodiments of the present disclosure may be implemented using existing computer processors, or by a special purpose computer processor for an appropriate system, incorporated for this or

another purpose, or by a hardwired system. Embodiments within the scope of the present disclosure include program products comprising machine-readable media for carrying or having machine-executable instructions or data structures stored thereon. Such machine-readable media can be any available media that can be accessed by a general purpose or special purpose computer or other machine with a processor. By way of example, such machine-readable media can comprise RAM, ROM, EPROM, EEPROM, CD-ROM or other optical disk storage, magnetic disk storage or other magnetic storage devices, or any other medium which can be used to carry or store desired program code in the form of machine-executable instructions or data structures and which can be accessed by a general purpose or special purpose computer or other machine with a processor. Combinations of the above are also included within the scope of machine-readable media. Machine-executable instructions include, for example, instructions and data which cause a general purpose computer, special purpose computer, or special purpose processing machines to perform a certain function or group of functions.

[0064] Although the figures may show a specific order of method steps, the order of the steps may differ from what is depicted. Also two or more steps may be performed concurrently or with partial concurrence. Such variation will depend on the software and hardware systems chosen and on designer choice. All such variations are within the scope of the disclosure. Likewise, software implementations could be accomplished with standard programming techniques with rule based logic and other logic to accomplish the various connection steps, processing steps, comparison steps, and decision step.

WHAT IS CLAIMED IS:

1. A method for configuring a wireless camera to connect to a wireless access point, the method comprising:
 - wirelessly connecting to a client device;
 - transmitting an encryption key to the client device;
 - receiving encrypted data from the client device, wherein the encrypted data comprises an identifier and an access code;
 - decrypting, using a processing circuit of the wireless camera and the encryption key, the encrypted data; and
 - wirelessly connecting to the wireless access point using the decrypted data.
2. The method of Claim 1, wherein the client device is at least one of a desktop, laptop, and mobile phone.
3. The method of Claim 1, wherein the wireless access point is a WiFi router which forms a wireless LAN in an area and has a connection to the Internet.
4. The method of Claim 1, wherein the decrypted data includes an identifier associated with the wireless access point and a passcode for accessing the wireless access point.
5. The method of Claim 1, wherein the decrypted data comprises a passcode for accessing the wireless access point.
6. The method of claim 1, wherein the encryption key comprises a symmetric encryption key.
7. The method of claim 6, wherein the symmetric encryption key is generated, at least in part, based upon a serial number of the wireless camera or a MAC address of the wireless camera.

8. The method of claim 6, wherein the symmetric encryption key is randomly generated.
9. The method of claim 1, wherein the identifier comprises an SSID and the access code comprises at least one of a WEP code, a WPA code, a WPA2 code, and a passphrase.
10. The method of claim 1 further comprising:
broadcasting, from the wireless camera, an SSID associated with the wireless camera;
wherein wirelessly connecting to the client device comprises receiving a request from the client device to connect to the wireless camera, based, at least in part, on the SSID associated with the wireless camera.
11. The method of claim 1 further comprising:
transmitting display data to the client device, wherein the display data comprises a configuration webpage.
12. The method of claim 1, wherein the client device comprises at least one of a laptop computer, a mobile phone, a tablet, a desktop computer, a smart television, a PDA and a gaming system.
13. The method of claim 1 further comprising:
scanning, at the wireless camera, for one or more identifiers associated with one or more wireless access points; and
transmitting a list of the one or more identifiers associated with the one or more wireless access points to the client device.
14. The method of claim 1 further comprising:
providing a first feedback associated with the wireless connection to the wireless access point.

15. The method of claim 14 further comprising:
providing a second feedback associated with an activation of an access point mode of the wireless camera.
16. The method of claim 15, wherein the first feedback and the second feedback comprise an audible voice.
17. The method of claim 15, wherein the first feedback and the second feedback comprise a visual indicator.
18. The method of claim 1, wherein the wireless access point comprises at least one of a wireless access point, a laptop computer, a desktop computer, a game system, a tablet, a smart television, and a mobile phone.
19. The method of claim 1 further comprising:
storing the decrypted identifier and access code on a storage device of the wireless camera.
20. A method connecting a wireless camera to a wireless access point, comprising:
activating the wireless camera to serve as a temporary wireless access point;
wirelessly connecting to the wireless camera as the temporary wireless access point via a client device;
transmitting, at the client device, an encryption key from the wireless camera;
encrypting, at the client device, one or more identifiers and one or more access codes, wherein the one or more identifiers and the one or more access codes are associated with one or more wireless access points; and
transmitting the encrypted one or more identifiers and one or more access codes to the wireless camera.

21. The method of Claim 20, wherein the wireless camera does not include a user interface control for entering information regarding the wireless access point directly to the wireless camera.
22. The method of claim 20 further comprising:
receiving display data from the wireless camera, wherein the display data is configured to display a configuration webpage.
23. The method of claim 20, wherein the client device comprises at least one of a laptop computer, a mobile phone, a tablet, a desktop computer, a smart television, a PDA and a gaming system.
24. The method of claim 20 further comprising:
retrieving one or more identifiers and one or more access codes, wherein the one or more identifiers and the one or more access codes are stored on the client device.
25. The method of claim 20, wherein the steps of wirelessly connecting to the wireless camera, receiving an encryption key, encrypting the one or more identifiers and the one or more access codes, and transmitting the encrypted one or more identifiers and one or more access codes to the wireless camera are automatically performed by an application on the client device.
26. A computer-implemented method for configuring a wireless camera to connect to a wireless access point comprising:
activating an access point mode of the wireless camera;
providing speech audio via a speaker of the wireless camera indicating that the access point mode is activated;
broadcasting an SSID associated with the wireless camera;
receiving a request from a client device to connect to the wireless camera;
wirelessly connecting to the client device;
transmitting an encryption key to the client device, wherein the encryption key is

uniquely associated with the wireless camera;

receiving encrypted data from the client device, wherein the encrypted data is encrypted using the encryption key and wherein the encrypted data comprises an identifier and an access code;

decrypting, using a processing circuit of the wireless camera, the encrypted data;

identifying a wireless device based, at least in part, on the identifier; and

wirelessly connecting to the wireless device using the identifier and access code.

1/5

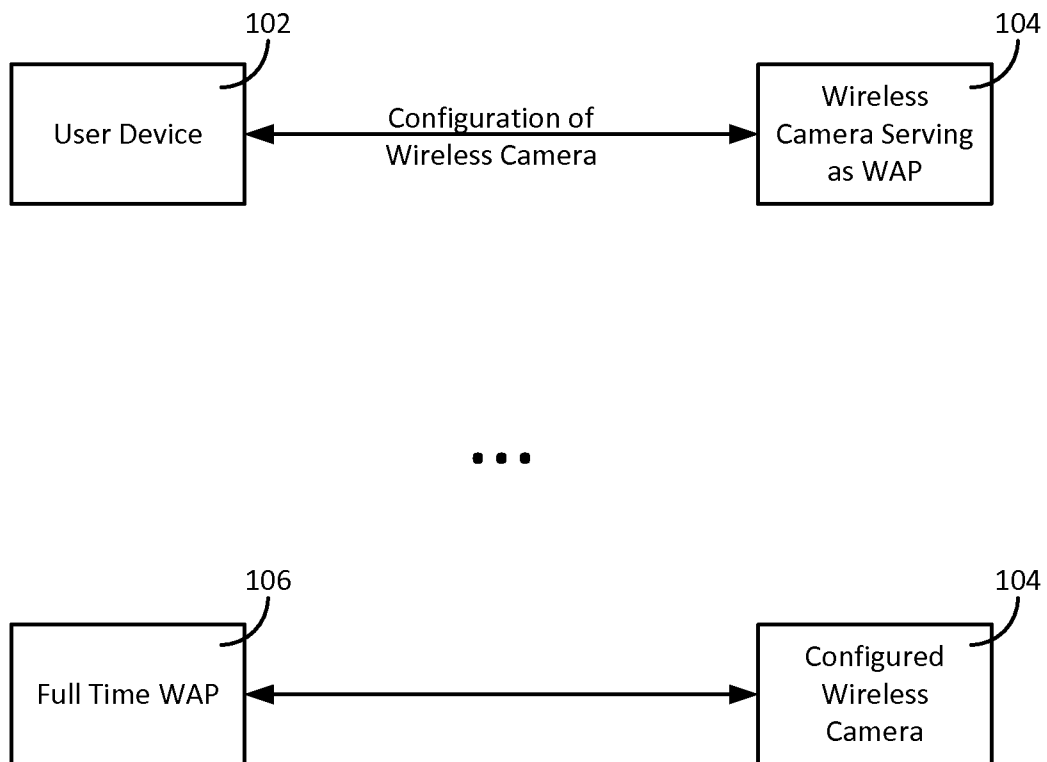


FIG. 1

2/5

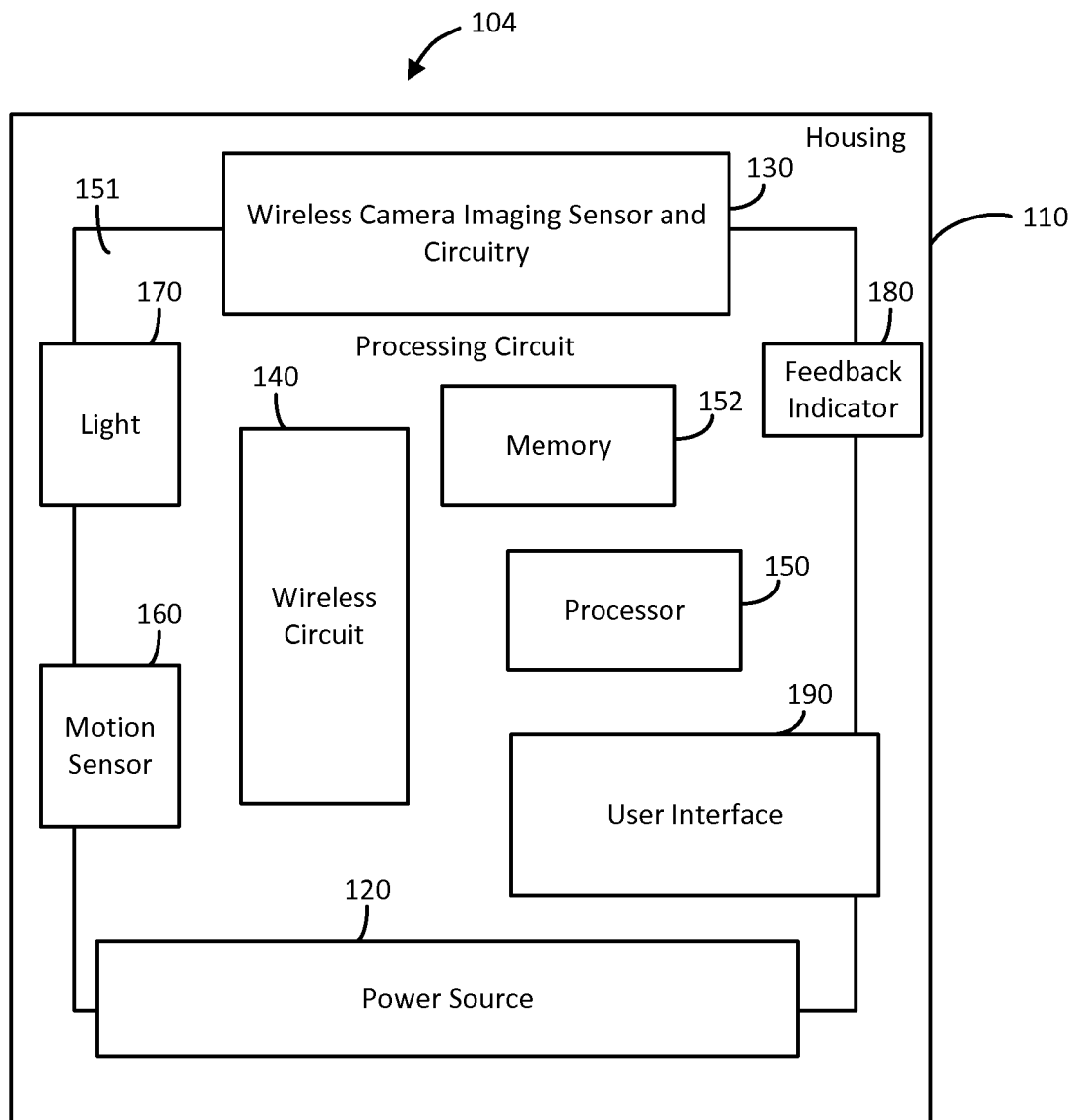
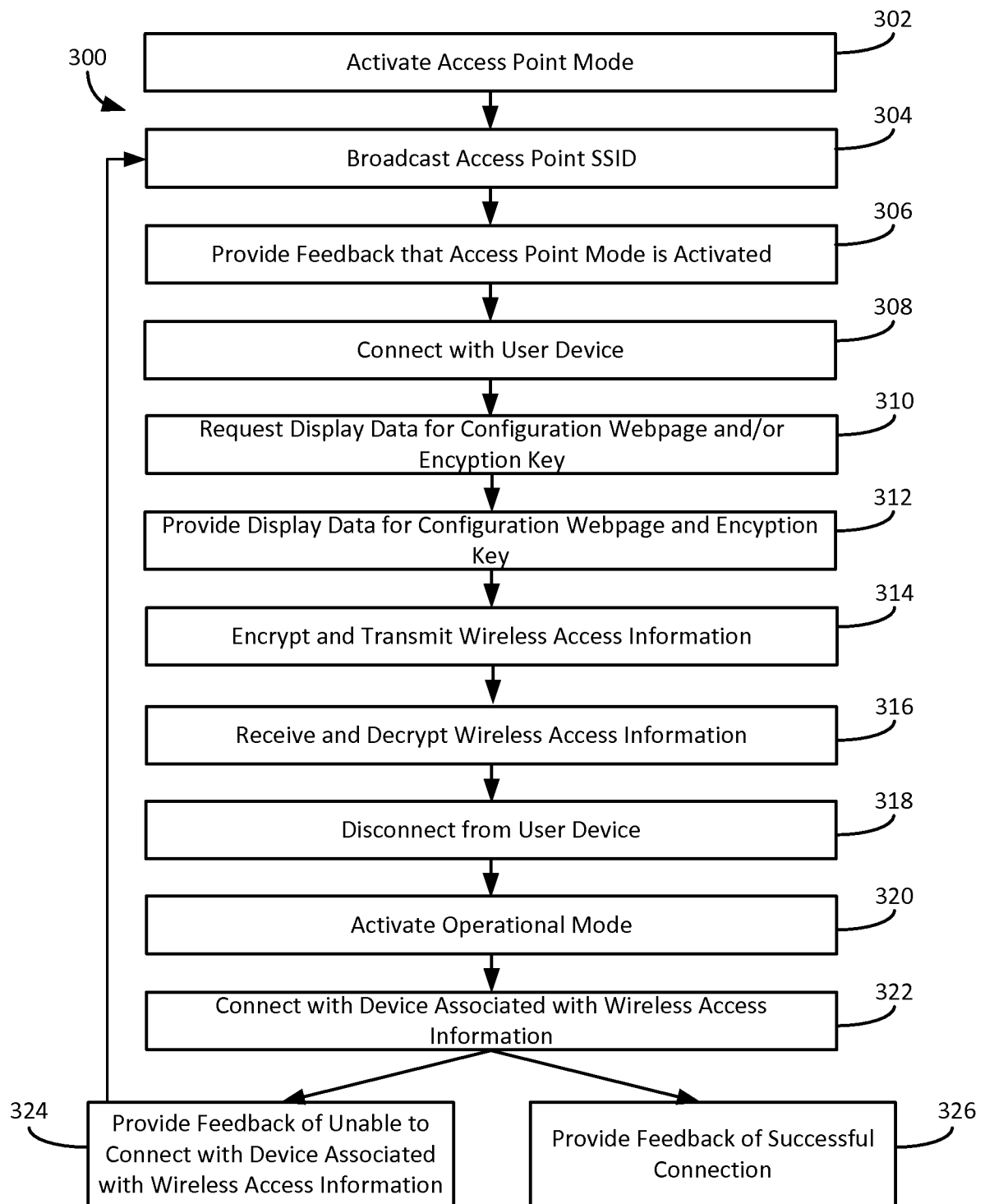


FIG. 2

3/5**FIG. 3**

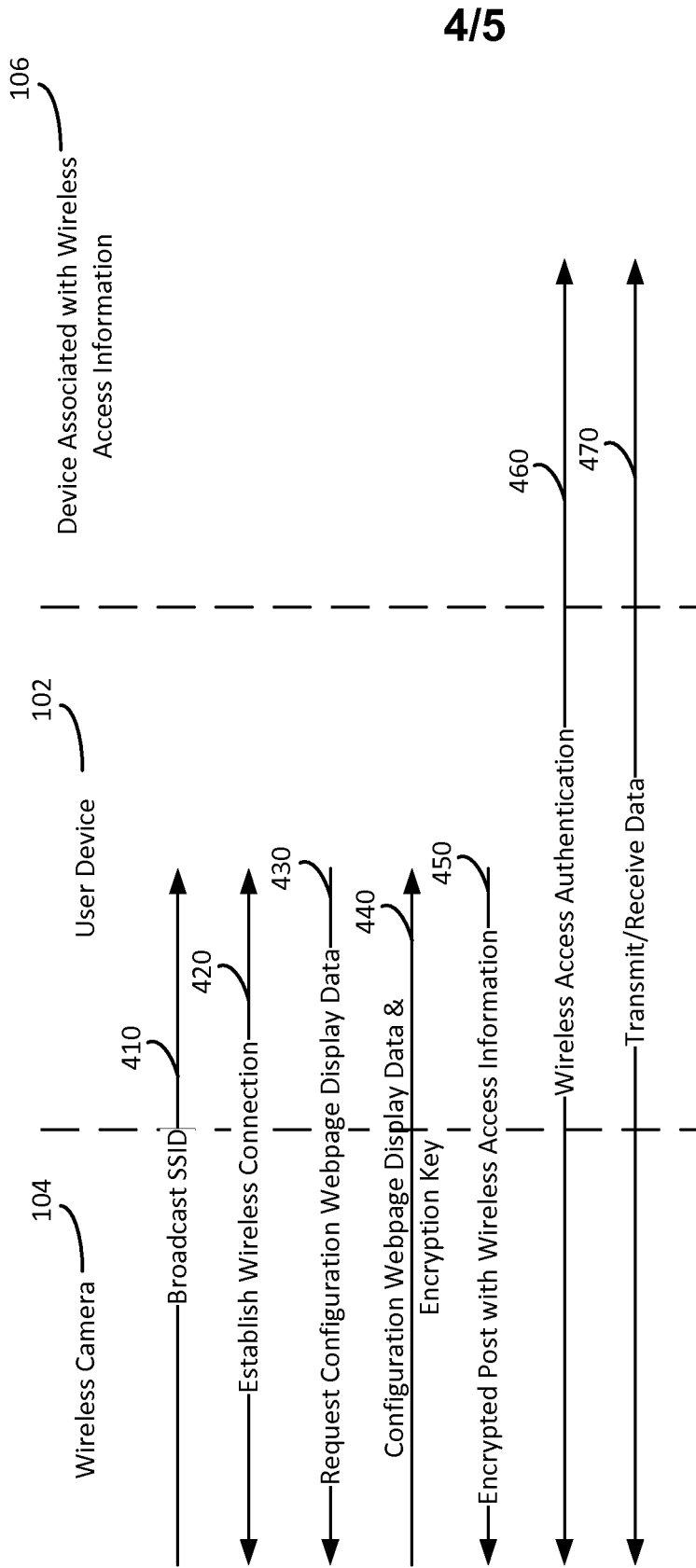
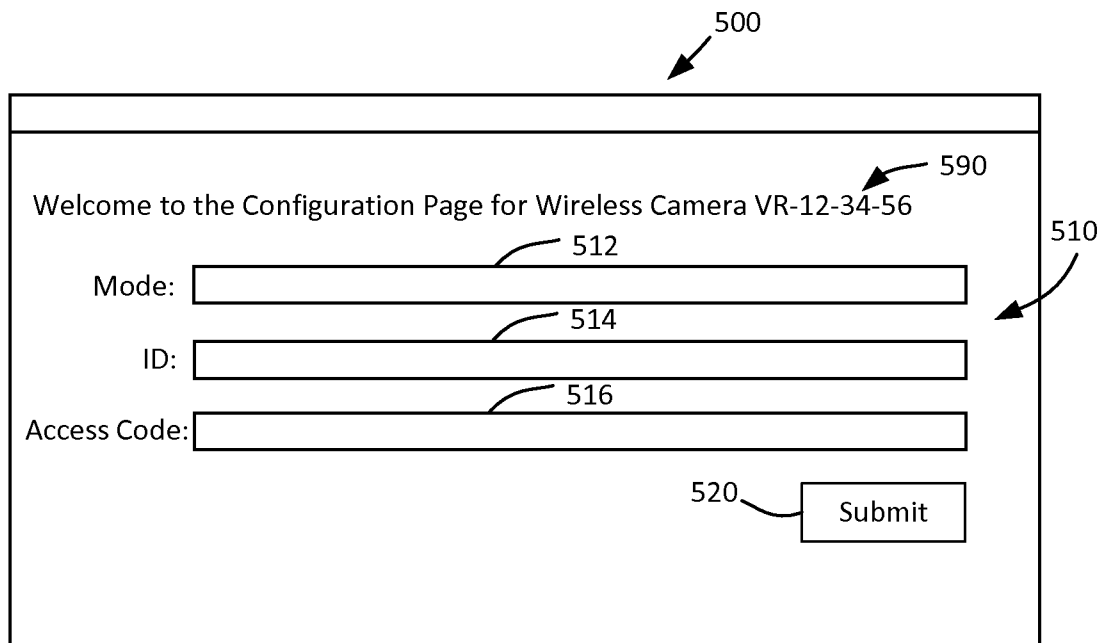


FIG. 4

5/5



500

Welcome to the Configuration Page for Wireless Camera VR-12-34-56 590

Mode: 512

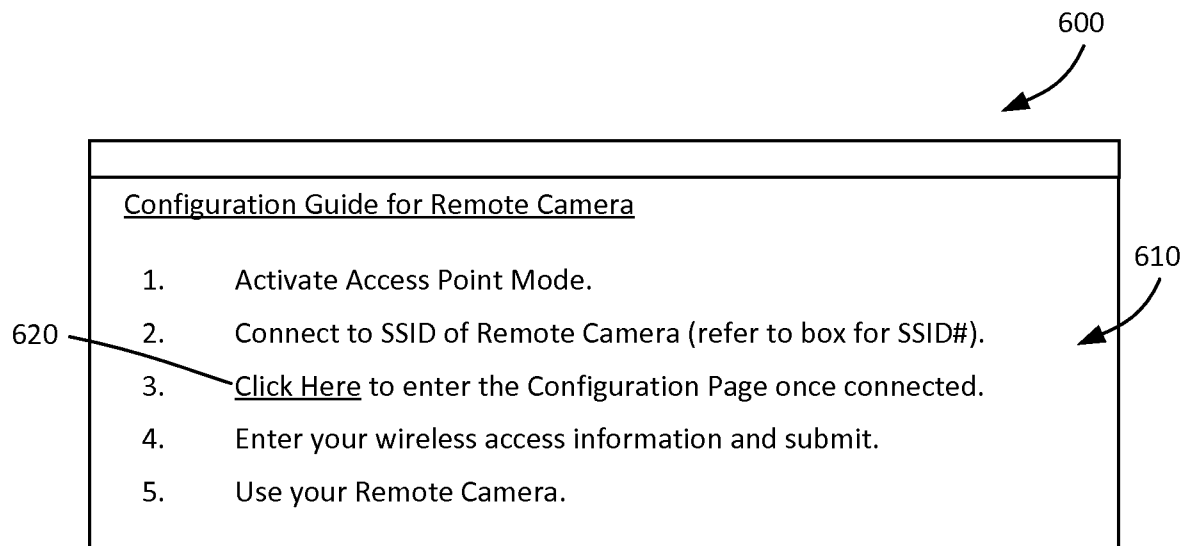
ID: 514

Access Code: 516

520

510

FIG. 5



600

Configuration Guide for Remote Camera

1. Activate Access Point Mode.
2. Connect to SSID of Remote Camera (refer to box for SSID#).
3. Click Here to enter the Configuration Page once connected. 620
4. Enter your wireless access information and submit.
5. Use your Remote Camera.

610

FIG. 6