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

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
16 May 2013 (16.05.2013)

WIPO | PCT

(10) International Publication Number
WO 2013/071208 A2

(51) International Patent Classification:
H04W 4/20 (2009.01)

(21) International Application Number:
PCT/US2012/064576

(22) International Filing Date:
10 November 2012 (10.11.2012)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
13/293,245 10 November 2011 (10.11.2011) US

(71) Applicant: **MICROSOFT CORPORATION** [US/US]; One Microsoft Way, Redmond, Washington 98052-6399 (US).

(72) Inventor: **KAUFMAN, Matthew;** c/o Skype, International Patents, 70 Sir John Rogerson's Quay, Dublin, 2 (IE).

(81) Designated States *(unless otherwise indicated, for every kind of national protection available):* AE, AG, AL, AM, AO, AT, AU, AZ, BA, BB, BG, BH, BN, BR, BW, BY, BZ, CA, CH, CL, CN, CO, CR, CU, CZ, DE, DK, DM, DO, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, GT, HN, HR, HU, ID, IL, IN, IS, JP, KE, KG, KM, 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, 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, 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(H))*

— *as to the applicant's entitlement to claim the priority of the earlier application (Rule 4.17(in))*

Published:

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

(54) Title: DEVICE ASSOCIATION VIA VIDEO HANDSHAKE

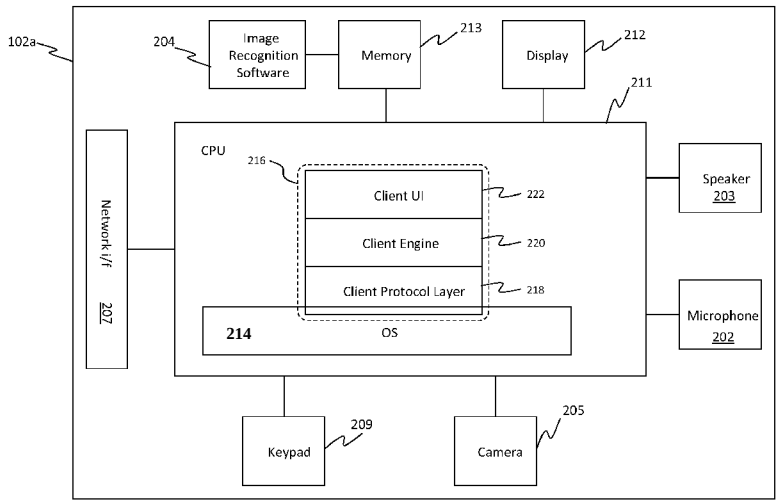

Figure 2

(57) Abstract: A method of pairing a first device with a second device is disclosed. Accordingly, an image that include encoded data is generated by the first device. The encoded data includes a unique identifier for identifying the first device and an arbitrary security code. The first device displays the image on a display. The second device captures the image using an image sensing device. The encoded data is decoded to generate a decoded data. The second device sends the decoded data to a server that is communicatively connected to the first device and the second device. Upon receiving the decoded data and using the unique identifier, the server communicates with the first device to verify the arbitrary security code.

WO 2013/071208 A2

DEVICE ASSOCIATION VIA VIDEO HANDSHAKE

BACKGROUND OF THE INVENTION

Field of the Invention

[0001] Embodiments of the present invention relate generally to establishing and management a communication event between first and second user terminals.

Description of the Related Art

[0002] Traditionally, electronic devices are paired using Bluetooth™ technology. The term "pairing" means that two devices exchange some data to agree to work together to provide a predefined function. For example, a Bluetooth™ enabled mobile phone may be paired with a Bluetooth™ headset and upon a successful pairing, the headset provides speakers and microphone to the mobile phone.

[0003] There are many issues with the above stated method of pairing devices. First, a special hardware is needed at both ends to effectuate such pairing. Second, such pairing can only be used for predetermined specific functions. Also, the Bluetooth™ signals have wider range, hence, without a proper security, unintended pairing may occur. Still further, the paired devices must stay within a particular range after the pairing.

SUMMARY OF THE INVENTION

[0004] In one embodiment, a method of pairing a first device with a second device is disclosed. An image that includes a unique identifier for identifying a first device and a security code is generated and displayed on the first device. A second device captures the image using an image sensing device. The unique identifier and the security code is then sent to a server that is communicatively connected to the first device and the second device. The server communicates with the first device, using the unique identifier, to verify the security code.

[0005] In another embodiment, a method of pairing a first device with a second device is disclosed. Accordingly, an image that include encoded data is generated by the first device. The encoded data includes a unique identifier for identifying the first device and an arbitrary security code. The first device displays the image on a display. The second device captures the image using an image sensing device. The encoded data is decoded to generate a decoded data. The

second device sends the decoded data to a server that is communicatively connected to the first device and the second device. Upon receiving the decoded data and using the unique identifier, the server communicates with the first device to verify the arbitrary security code.

[0006] In yet another embodiment, a system for pairing a first device with a second device is disclosed. The system includes a first device connected to a network. The first device is configured to generate an image that include encoded data. The encoded data includes a unique identifier for identifying the first device and an arbitrary security code, and to display the image on a display of the first device. The system also includes a second device connected to the network. The second device is configured to capture the image and to decode the encoded data to generate a decoded data, and to send the decoded data to a server that is communicatively connected to the first device and the second device. The server is connected to the first device and the second device through the network and the server is configured to communicate, using the unique identifier, with the first device to verify the arbitrary security code.

[0007] In yet another embodiment, a computer readable storage medium containing a program which, when executed, performs an operation of pairing a first device with a second device, is disclosed. The operation comprises capturing an image using an image sensor. The image includes a unique identifier of another device and a security code. The operation further includes sending the unique identifier and the security code to a server via a network and instructing the server to communicate with the another device using the unique identifier to verify the security code with the another device.

[0008] Other embodiments include, without limitation, a non-transitory computer-readable storage medium that includes instructions that enable a processing unit to implement one or more aspects of the disclosed methods as well as a system configured to implement one or more aspects of the disclosed methods.

BRIEF DESCRIPTION OF THE DRAWINGS

[0009] So that the manner in which the above recited features of the present invention can be understood in detail, a more particular description of the invention, briefly summarized above, may be had by reference to embodiments,

some of which are illustrated in the appended drawings. It is to be noted, however, that the appended drawings illustrate only typical embodiments of this invention and are therefore not to be considered limiting of its scope, for the invention may admit to other equally effective embodiments.

[0010] Figure 1 illustrates a schematic depiction of a communication system based on the Internet, according to one embodiment of the present invention.

[0011] Figure 2 is a logical diagram of an end user terminal, according to one embodiment of the present invention.

[0012] Figure 3 illustrates an exemplary use case scenario of call management, according to one embodiment of the present invention.

[0013] Figure 4 illustrates a method of pairing two devices, according to one embodiment of the present invention.

DETAILED DESCRIPTION

[0014] In the following description, numerous specific details are set forth to provide a more thorough understanding of the present invention. However, it will be apparent to one of skill in the art that the present invention may be practiced without one or more of these specific details. In other instances, well-known features have not been described in order to avoid obscuring the present invention.

[0015] Reference throughout this disclosure to "one embodiment" or "an embodiment" means that a particular feature, structure, or characteristic described in connection with the embodiment is included in at least one embodiment of the present invention. Thus, the appearances of the phrases "in one embodiment" or "in an embodiment" in various places throughout this specification are not necessarily all referring to the same embodiment. Furthermore, the particular features, structures, or characteristics may be combined in any suitable manner in one or more embodiments.

[0016] Some communication systems allow the user of a device, such as a personal computer, to communicate across a packet-based computer network such as the Internet. Such communication systems include voice over internet protocol ("VoIP") communication systems. These systems are beneficial to the

user as they are often of significantly lower cost than conventional fixed line or mobile networks. This may particularly be the case for long-distance communication. To use a VoIP system, the user installs and executes client software on her/his device. The client software provides the VoIP connections as well as other functions such as registration and authentication. In addition to voice communication, the client may also provide further features such as video calling, instant messaging ("IM"), SMS messaging, file transfer and voicemail.

[0017] One type of communication system for packet-based communication uses a peer-to-peer ("P2P") topology. In one embodiment, to enable access to a peer-to-peer system, a user must execute client software provided by a communication system software provider (or a third party vendor) on their computer (which includes any supported computing device, including smart phones), and register with the P2P system. When the user registers with the P2P system, the client software is provided with a digital certificate from a server. Once the client software has been provided with the certificate, then calls or other communications can subsequently be set up and routed between users of the P2P system without the further use of a server in the set-up. Instead, the client looks up the required IP addresses from information distributed amongst the client software on other end users' computers within the P2P system. Once the IP address of a callee's terminal has thus been determined, the caller's client software then exchanges certificates with the callee's client software. The exchange of the digital certificates (or user identity certificates, "UIC") between users provides proof of the users' identities and that they are suitably authorized and authenticated in the P2P system. Therefore, the presentation of digital certificates provides trust in the identity of the users. It is therefore a characteristic of peer-to-peer communication that, once registered, the users can set up their own communication routes through the P2P system in a decentralized manner based on distributed address look-up and the exchange of one or more digital certificates, without using a server for those purposes. Further details on such a P2P system are disclosed in WO 2005/008524 and WO 2005/009019. VoIP or other packet-based communications can also be implemented using non-P2P systems that do use centralized call set-up.

[0018] Figure 1 is a schematic illustration of a communication system 100 comprising a packet-based network 101 such as the Internet, a mobile cellular network 103, and a circuit switched network1 12 such as the public switched telephone network (PSTN). The mobile cellular network 103 comprises a plurality of base stations 104 (sometimes referred to as node Bs in 3GPP terminology). Each base station 104 is arranged to serve a corresponding cell of the cellular network 103. Each base station 104 is connected to the circuit switched networkl 12 via a gateway 114. Further, the packet-switched network 101 comprises a plurality of wireless access points 106 such as Wi-Fi access points for accessing the Internet. These may be the access points of one or more wireless local area networks (WLANs). In one embodiment, the gateway 114 is also coupled to the Internet 101 to enable the routing of a call between the PSTN 112 and the Internet 101.

[0019] A plurality of user terminals 102 are arranged to communicate over one or more of the networks 101,103,112. For merely illustration purposes only, Figure 1 shows user terminal 102a as an Internet-enabled mobile device, user terminal 102b as a desktop or laptop PC, user terminal 102c as a cellular mobile phone 102c, and user terminal 102d as a landline telephone connected to the circuit switched networkl 12.

[0020] An example mobile device 102a is shown schematically in Figure 2. The mobile device 102a comprises a processing apparatus in the form of one or more processor units (CPUs) 211 coupled to a memory 213 storing a communication client application. The processor 211 is also coupled to: a microphone 202, a speaker 203, camera 205, a one or more RF transceivers 207, a keypad 209, and a display 212.

[0021] The one or more transceivers 207 enable the mobile device 102a to access the one or more networks 101,103,112. For example, mobile device 102a may comprise a cellular wireless transceiver for accessing the mobile cellular network 103 via the base stations 104, and/or a wired or wireless modem for accessing the Internet 101. In the case of a wireless modem, this typically comprises a short-range wireless transceiver (e.g. Wi-Fi) for accessing the Internet 101 via the wireless access points 106.

[0022] Access to the Internet 101 may also be achieved by other means such as GPRS (General Packet Radio Service) or HSPA (High Speed Packet Access). At a higher level of the cellular hierarchy, the cellular network 103 comprises a plurality of cellular controller stations 105 each coupled to a plurality of the base stations 104. The controller stations 105 are coupled to a traditional circuit-switched portion of the mobile cellular network 103 but also to the Internet 101. The controller stations 105 are thus arranged to allow access to packet-based communications via the base stations 104, including access to the Internet 101. The controller stations 105 may be referred to for example as Base Station Controllers (BSCs) in GSM/EDGE terminology or Radio Network Controllers (RNCs) in USTM or HSPA terminology.

[0023] The memory 213 may comprise a non-volatile memory such as an electronic erasable and programmable memory (EEPROM, or "flash" memory) coupled to the processor 211. The memory stores communications code arranged to be executed on the processor, and configured so as when executed to engage in communications over one or more networks 101,103,112. The communications code preferably comprises a communication client application 110a provided by a software provider associated with the communication system. The communication client application 110a may be executed for performing communications such as voice or video calls with other user terminals 102 over the Internet 101, via a short-range wireless transceiver 207 and wireless access points 106, and/or via a cellular wireless transceiver 207, base stations 104 and controller stations 105 of the cellular network 103 as discussed above. However, one or more of the user terminals 102 involved could alternatively communicate via a wired modem, e.g. in the case of a call between a mobile terminal and a desktop PC.

[0024] As shown in Figure 1 both user terminals 102a and 102d execute a communication client software110 in order for the user terminalsl 02a and 102d to transmit and receive data over the Internet 101.

[0025] The communication system 100 also includes a server 120. In one embodiment, the server 120 is a Peer-to-Peer (P2P) communication server. Further, in one embodiment, the server 120 provides one or more of the following functions: call setup, call management, routing calls among the user terminals

connected to the Internet 101 and routing calls among the user terminals connected to the Internet 101 and telephones connected to the PSTN network 112, etc. In one embodiment, the server 120 works cooperatively with the user stations with the help of a client software that runs on the user stations and/or the gateway 114.

[0026] Figure 2 illustrates a schematic diagram of a user terminal 102a. The user terminal includes operating system ("OS") 214 executed on the CPU 202. Running on top of the OS 214 is a software stack 216 for the client 108. The software stack shows a client protocol layer 218, a client engine layer 220 and a client user interface layer ("III") 222. Each layer is responsible for specific functions. Because each layer usually communicates with two other layers, they are regarded as being arranged in a stack as shown in Figure 2. The operating system 214 manages the hardware resources of the computer and handles data being transmitted to and from the link 106 via the network interface 110. The client protocol layer 218 of the client software communicates with the operating system 214 and manages the connections over the communication system. Processes requiring higher level processing are passed to the client engine layer 220. The client engine 220 also communicates with the client user interface layer 222. The client engine 220 may be arranged to control the client user interface layer 222 to present information to the user 102 via the user interface of the client and to receive information from the user 102 via the user interface.

[0027] Image recognition software 204 may be stored in memory 213 or in a separate memory not shown in Figure 2. Therefore when the camera 205 captures image data, the CPU 211 may execute the image recognition software 204 to decode any information encoded or obfuscated in the image data. In embodiments of the present invention described more fully below, the image recognition software 204 supplies decoded information from a barcode to the client engine 220. In one embodiment, the image recognition software 204 may be a part of the software stack 216. In other embodiments, the image recognition software 204 may be implemented in hardware. The image recognition software 204 may also be embedded in a driver for the camera 205.

[0028] Images and shapes may encapsulate data that can be encoded by a reader in conjunction with selected configurations. For example, a triangle shape

may be configured to convey a particular meaning between two entities. Other types of shapes may be used for conveying different types of information. Further, barcodes are commonly known in the art to comprise encoded data such that they may be optically read, and the encoded information decoded in order to read information about an item that the barcode is attached to.

[0029] There are two types of barcodes, linear barcodes and two dimensional (2D) barcodes, sometimes referred to as 'matrix' barcodes. One type of 2D barcode is the Quick Response (QR) barcode.

[0030] Figure 3 illustrates one example scenario of pairing two user terminals using a video handshake. In this example, a user terminal 102a is in a call session with a user terminal 102b-1 . The call may be voice call, chat or audio/video call. One of the user terminals 102a and 102b-1 may be connected to the PSTN network 112 and the call between the user terminal 102a and the user terminal 102b-1 may be established through the gateway 114. In another embodiment, both user terminals may be connected to the Internet 101 and are also in a cooperative communication with the server 120 via client software. Imagine now that the user of the user terminal 102a (which could be a handheld device) walks into a conference room, which includes a LCD TV (or any other type of display) 122 and a camera 107. The LCD TV 122 is coupled to a user terminal 102b-2 connected to the Internet 101. In one embodiment, the LCD TV 122 may include client software in its own memory. If so, then the LCD TV 122, standalone, would function as a user terminal without a need for any external hardware, such as a computer.

[0031] Suppose the user of the user terminal 102a wants to pair the LCD TV 122 with the user terminal 102a in order to use the LCD TV 122 for Audio/Video. Alternatively, the user may want to transfer the communication session between the user terminal 102a and the user terminal 102b-1 from the user terminal 102a to the LCD TV 122 without interrupting the ongoing call session and transparently to the user of the user terminal 102b-1 .

[0032] In one embodiment, the user of the user terminal 102a would invoke a user interface (e.g., the UI 222 in Figure 2) in the user terminal 102a. The user interface would have various configurable options. For example, the user

interface may have one or more of the following options: transfer session, transfer audio, transfer video, transfer chat, and various combinations thereof.

[0033] It should be noted that the examples in this disclosure are provided merely to impart a better understanding of the invention. A person skilled in the art would realize that the systems and methods disclosed herein are directed to pairing of devices. Once paired, the devices may participate in many other activities, such as data transfer, one device controlling the other, etc. Unlike traditional pairing of devices using other technologies, such as Bluetooth™, the two devices, once paired, communicate via a server. Therefore, there is no location restriction on the paired devices. However, in another embodiment, the pairing include both server supported pairing, as described herein, and a device-to-device pairing, so that devices may exchange information directly as well as via the server. Among other, one advantage of the pairing methods described herein is that no special "pairing specific" hardware is required to effectuate the pairing of the two devices. Therefore, existing devices without any pairing specific hardware (e.g., Bluetooth™ hardware) may be configured to be paired using the methods described herein.

[0034] The LCD TV 122 is connected to the Internet 122 and can be located by the server 120 using a distinct identification. In one example, suppose the user selects (via the user interface) to transfer the video stream of the communication session from the user terminal 102a to the LCD TV 122. Upon the selection of an option, the user interface activates the camera 107 and the image recognition software 204 of the user terminal 102a. A second user interface is invoked on the LCD TV 122 either via the client software in the LCD TV 122 (or in the user terminal 102b-2) or via a separate software, hardware, or combination thereof. The user interface on the LCD TV 122 displays a coded pattern 124. In another embodiment, a number is displays on the LCD TV 122 instead of a graphical pattern. The coded pattern may be a QR code or a barcode. The coded pattern, in one example, includes the IP address of the LCD TV 122 (or the user terminal 102b-2). Additionally, the coded pattern may also include another number or code. Alternatively, the coded pattern may include just one number. In another example, the LCD TV 122 may simply display one or more words.

[0035] If the coded pattern is configured to include the IP address and a security code, the camera 107 of the user terminal 102a, when brought close to the displayed coded pattern, deciphers the coded pattern and extracts the IP address and the security code. In an alternative embodiment, the user terminal 102a send the encoded pattern to either the server 120 or another external device that is connected to the Internet 101 for deciphering the encoded pattern. The client software of the user terminal 102a sends the IP address and the security code to the server 120 with the instructions that the video portion of the ongoing communication session be transferred to the LCD TV 122. Upon receiving said instructions, the server asks the LCD TV for the security code. In one embodiment, other data related to the devices and/or the user may also be sent to the server 120. However, in yet another embodiment, only the IP address and the security code are sent to the server 120. The handshake is complete when the security code provided to the server 120 by the user terminal 102a matches with the security code received directly from the LCD TV 122. In one embodiment, the security code included in the coded pattern may be transient and may be valid only for a selected period of time. In another embodiment, the security check may be optional and the coded pattern may include only the IP address.

[0036] In another embodiment, any other identification of the LCD TV 122 may be included instead of the IP address so long as the server 120 can locate the LCD TV 122 on the Internet 101 by that identification.

[0037] In another example, instead of a coded pattern, the LCD TV 122 may simply display the IP address and/or any other type of temporary or permanent identification code (such as the MAC number, machine network name, etc.) in plain text and the image recognition software 204 may be configured to recognize plain text characters.

[0038] In one example, the server 120 is configured to maintain separate data streams for audio, video and chat. Hence, if the user terminal 102a requests the server 120 to transfer the video to the LCD TV 122, the server 120 redirects the video stream to the LCD TV 122. In a partial transfer of the communication session, the part that is transferred to LCD TV 122 runs concurrently and synchronously with the remaining part of the communication session on the user

terminal 102a. Similarly, if the complete session transfer was desired, the server 120 redirects all data streams to the IP address of the LCD TV 122.

[0039] In one embodiment, if the P2P communication system requires P2P users to log in using unique user identifications, the server 120 is configured to automatically send a login certificate (corresponding to the user of the user terminal 102a) to the LCD TV 122 (or the user terminal 102b-2) so that the user of the user terminal 102a is automatically logged into the LCD TV 122 (or the user terminal 102b-2).

[0040] It should be noted that the code pattern itself may also include the operation to be performed by the other user terminal after a successful pairing, thus diminishing a need for displaying multiple options on the user interface of the user terminal 102a. Instead, the user interface on the LCD TV 122 may generated different codes for different operations. Further, it should also be noted that in the above example, a session may be transferred from the LCD TV 122 to the user terminal 102a using the same method as described above. Similarly, a particular user station may be paired with a plurality of other user stations or devices, each performing either a distinct or duplicate function of a selected session, as for example, two devices may be setup to display the video part of the communication session. However, as stated above, the above examples are being provided for the easy understanding of the invention. The above embodiments may also be used for performing other operations that require a pairing of two or more devices.

[0041] The method of establishing a communication relationship between mobile device 102a and user device 102b will now be discussed with reference to Figure 4. When the user 108a of the mobile device 102a decides to establish a communication relationship between the mobile device 102a and the user device 102b, a coded pattern is displayed on the display of the user device 102b. As described above, in one embodiment, the coded pattern may contain the IP address or any other unique identification of the user device 102b. Optionally, the coded pattern may also include a security code.

[0042] When the communication client 110a is executed on user device 102a the client 110a presents an option to the user 108a to enter a pattern recognition

mode. At step 302, the user 108a may enter this recognition mode by making an appropriate input selection for example pressing a button on mobile device 102a, touching the appropriate section of display 212 or making a voice command or the like.

[0043] At step 304, the user 108a points the camera 205 of the mobile device 102a at the coded pattern. The user 108a then makes an appropriate selection on mobile device 102a to capture image data of the coded pattern at step 306. It will be appreciated that the captured image data comprises encoded information including IP address of the user terminal 102 (or any other identification to enable the server 120 to locate the user terminal 102b in the Internet 101) and also optionally a security code and/or encoded data defining a communication event related to the entity that generated the coded pattern.

[0044] As a result of the communication client 110a being in the pattern recognition mode, at step 308 the CPU 211 executes the image recognition software 204 to decode the image data and supplies decoded information to the communication client application 110a, the decoded information including decoded contact information and decoded data defining a communication event related to the entity that generated the barcode.

[0045] It will be appreciated that when the client 110a is not in the barcode recognition mode, and the user 108a uses camera 205 to capture image data the captured image data is stored in memory (whether internal or external) and no further action is taken.

[0046] At step 310, in response to receiving the decoded contact information, the communication client 110a establishes a communication relationship using the decoded information. That is the communication client establishes a communication relationship, for example transferring an ongoing communication session or a part thereof, from the mobile device 102a to the user device 102b. As described above, the server 120 takes part in the process of establishing the communication relationship between the mobile device 102a and the user device 102b.

[0047] While the forgoing is directed to embodiments of the present invention, other and further embodiments of the invention may be devised without departing

from the basic scope thereof. For example, aspects of the present invention may be implemented in hardware or software or in a combination of hardware and software. One embodiment of the invention may be implemented as a program product for use with a computer system. The program(s) of the program product define functions of the embodiments (including the methods described herein) and can be contained on a variety of computer-readable storage media. Illustrative computer-readable storage media include, but are not limited to: (i) non-writable storage media (e.g., read-only memory devices within a computer such as CD-ROM disks readable by a CD-ROM drive, flash memory, ROM chips or any type of solid-state non-volatile semiconductor memory) on which information is permanently stored; and (ii) writable storage media (e.g., floppy disks within a diskette drive or hard-disk drive or any type of solid-state random-access semiconductor memory) on which alterable information is stored. Such computer-readable storage media, when carrying computer-readable instructions that direct the functions of the present invention, are embodiments of the present invention.

CLAIMS:

1. A method of pairing a first device with a second device, the method comprising:

generating, by the first device, an image that includes a unique identifier for identifying the first device and a security code;

displaying the image on a display of the first device;

capturing the image by the second device using an image sensing device; and

sending the unique identifier and the security code to a server that is communicatively connected to the first device and the second device, and requesting the server to communicate with the first device, using the unique identifier, to verify the security code.

2. A system for pairing a first device with a second device, comprising:

a first device connected to a network, the first device is configured to generate an image that includes a unique identifier for identifying the first device and a security code, and to display the image on a display of the first device; and

a second device connected to the network, the second device is configured to capture the image and to retrieve the unique identifier and the security code , and to send the unique identifier and the security code to a server that is communicatively connected to the first device and the second device, wherein the server is connected to the first device and the second device through the network and the server is configured to communicate, using the unique identifier, with the first device to verify the security code.

3. The method of claim 1 or system of claim 2, wherein the first device is further configured to obfuscate the unique identifier and the security code in the image, the second device or the server is further configured to decode the unique identifier and the security code from the obfuscated form.

4. The method or system of claim 3, further comprising a third device connected to the network and in an active communication with the second.

5. The method or system of claim 4, wherein, the active communication session includes an audio visual communication.

6. The method or system of claim 5, wherein, the server is configured to transfer at least a part of the active communication session from the second device to the first device, upon verifying the security code and according to a preference of a user of the second device.

7. The method or system of claim 6, wherein, the server is configured such that if only a part of the active communication session is transferred to the first device, the remaining communication session runs concurrently and synchronously on the second device.

8. The method or system of claim 6, wherein, the server is configured to generate an authentication certificate corresponding to a user of the second device and to send the authentication certificate to the first device, prior to the transfer.

9. The method or system of claim 4, wherein, the transfer of the at least a part of the active communication session includes setting up a session between the first device and the third device.

10. A computer readable storage medium containing a program which, when executed, performs an operation of pairing devices, according to the steps of any of claim 1 and claims 3 to 9.

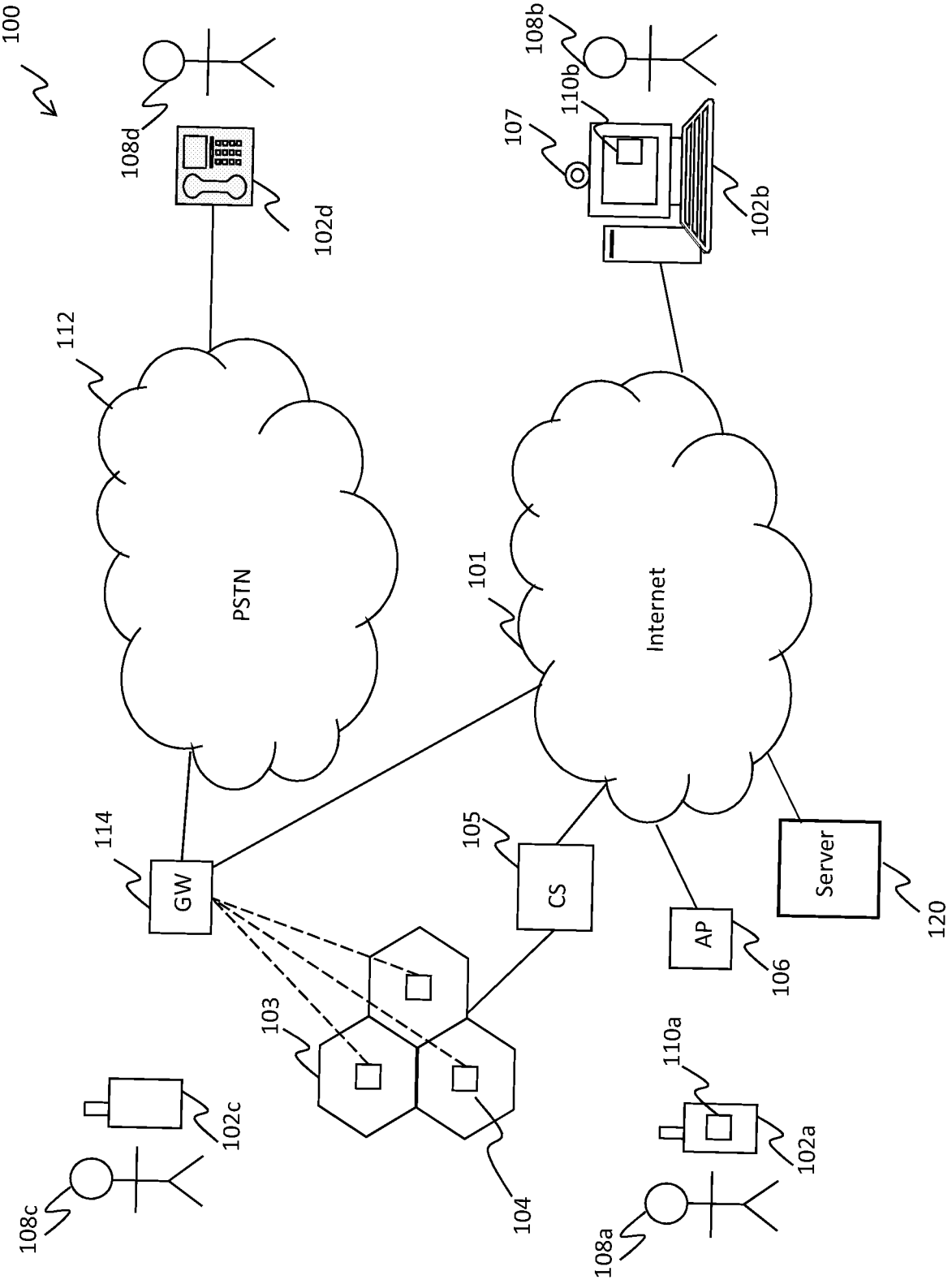
100
108d
102d
112
PSTN
108b
110b
107
102b
101
Internet
114
GW
105
CS
Server
120
AP
106
103
110a
102a
102c
108c
104
108a

Figure 1

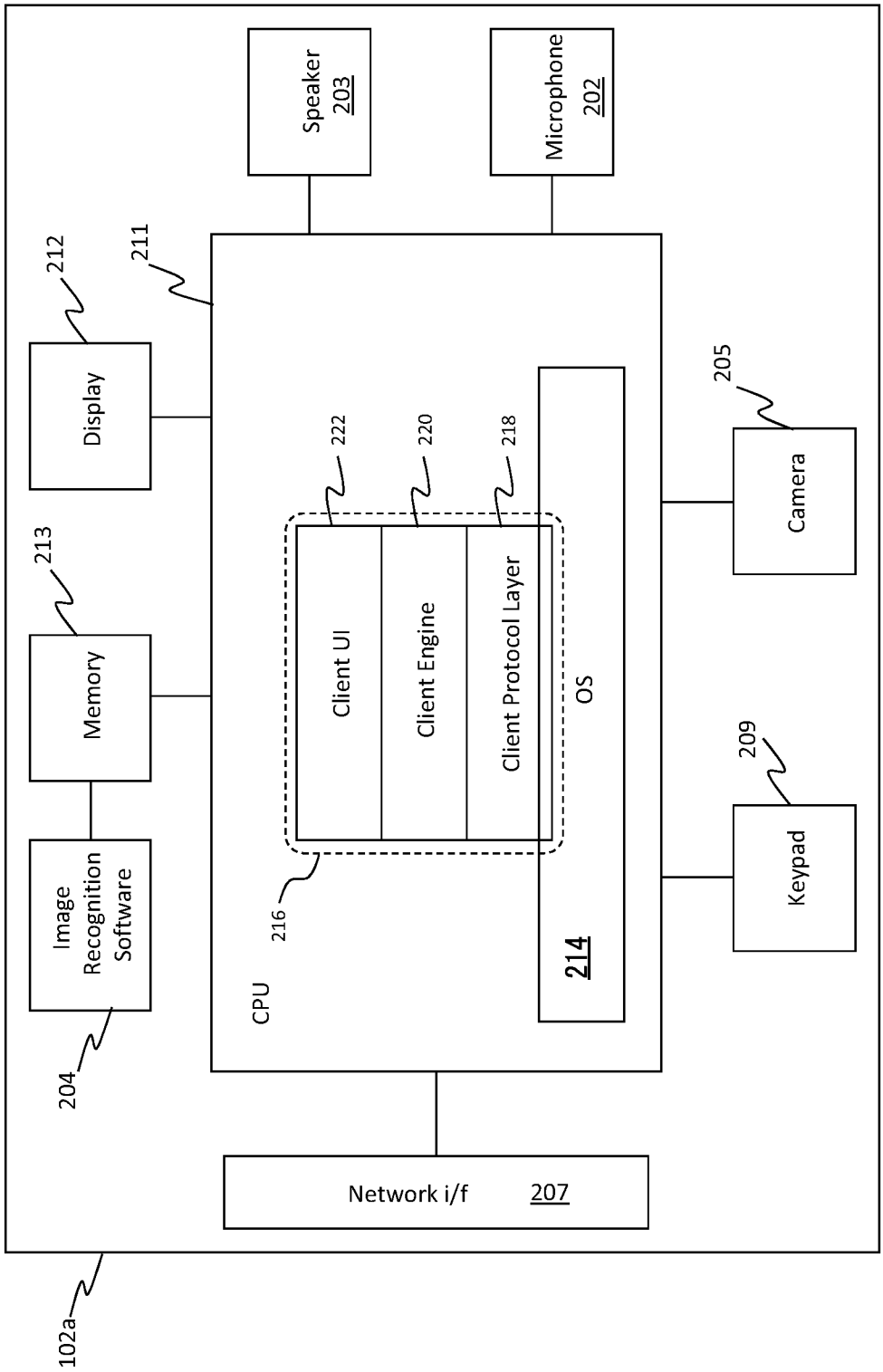
Speaker 203
Microphone 202
211
212
Display
205
Camera
222
220
218
213
Memory
Client UI
Client Engine
Client Protocol Layer
OS
209
Keypad
Image Recognition Software
216
CPU
214
204
Network i/f 207
102a

Figure 2

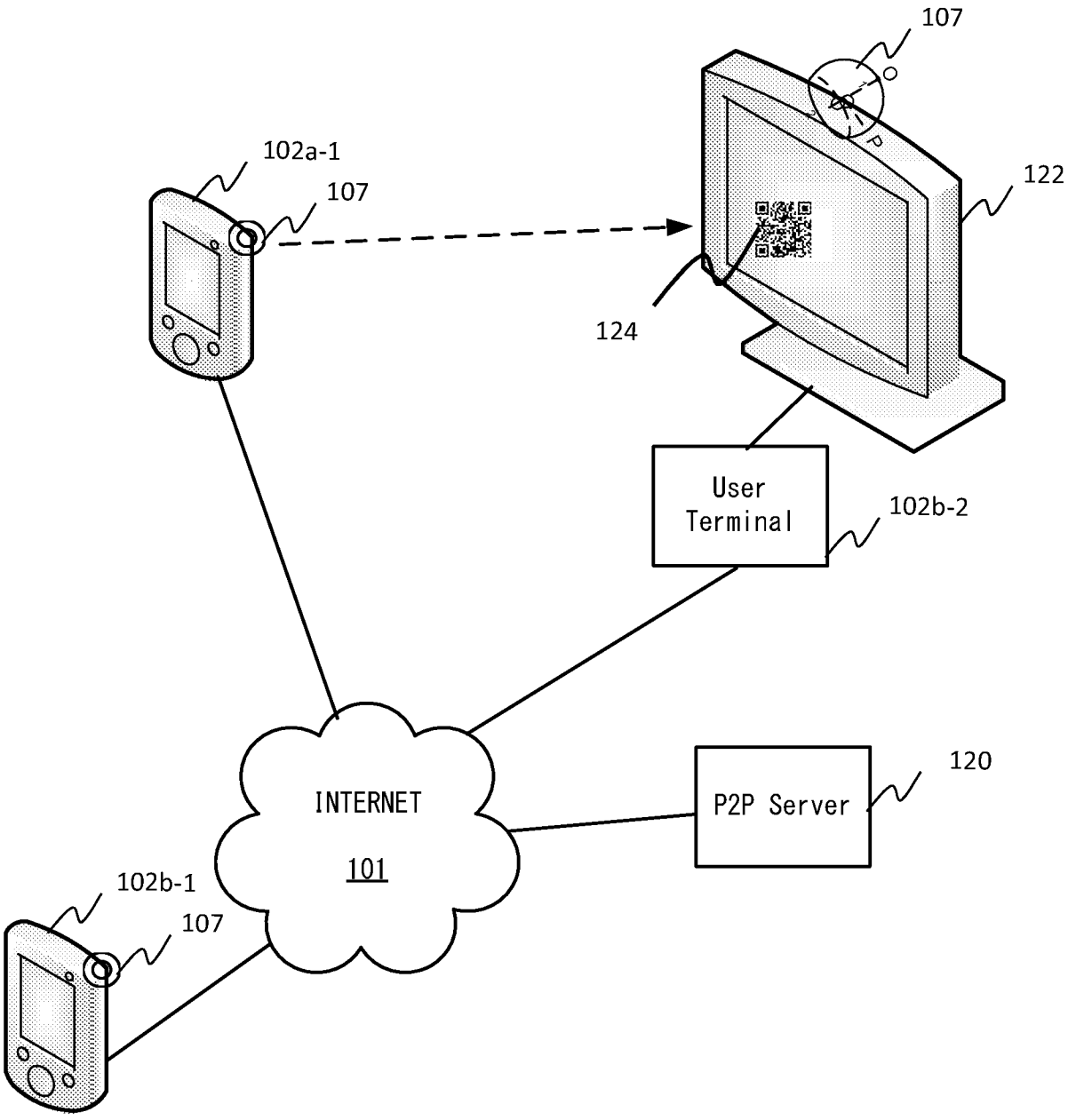
107
102a-1
107
122
124
User
Terminal
102b-2
INTERNET
101
120
P2P Server
102b-1
107

Figure 3

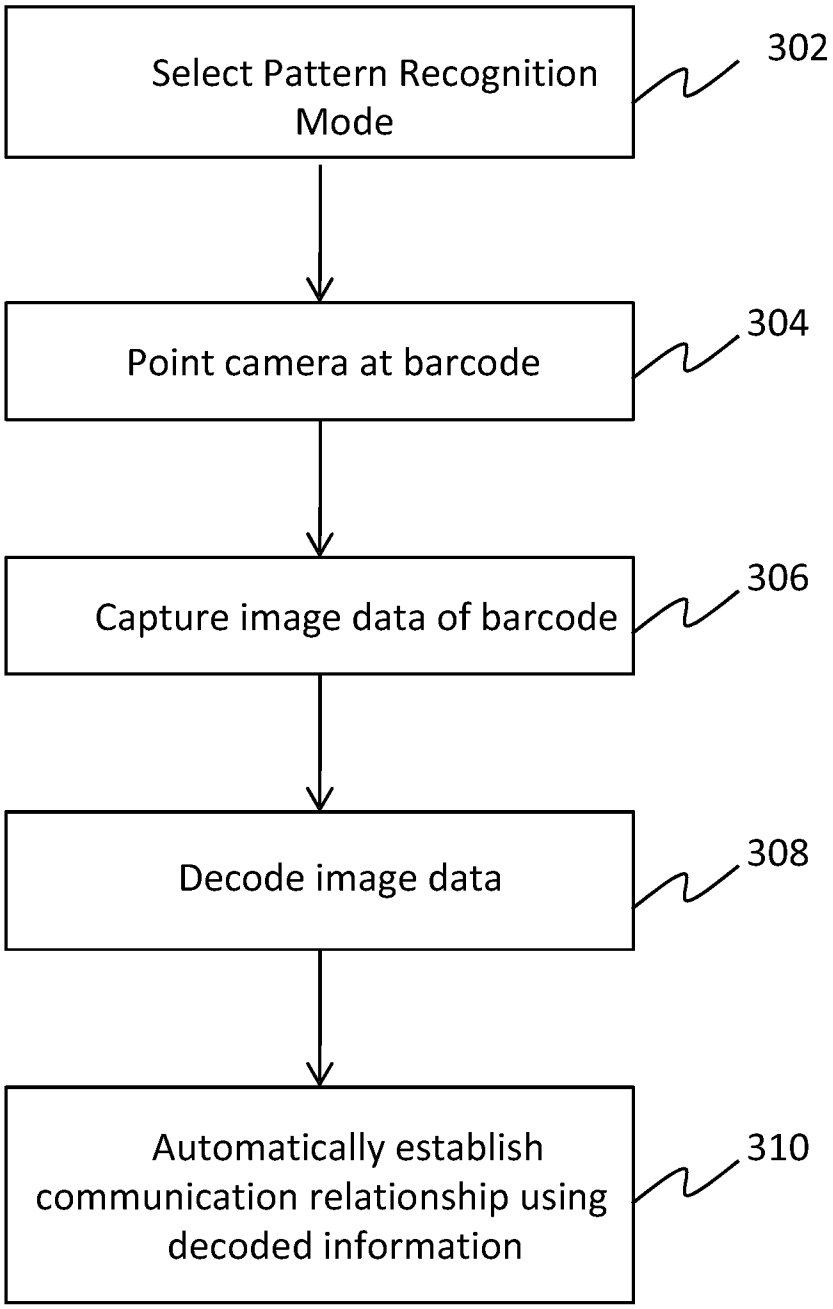
Select Pattern Recognition Mode
302
Point camera at barcode
304
Capture image data of barcode
306
Decode image data
308
Automatically establish communication relationship using decoded information
310

Figure 4