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

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
19 November 2015 (19.11.2015)

WIPO | PCT

(10) International Publication Number
WO 2015/175634 A1

(51) International Patent Classification:
G06F 21/32 (2013.01) *H04L 29/06* (2006.01)

(21) International Application Number:
PCT/US2015/030527

(22) International Filing Date:
13 May 2015 (13.05.2015)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
14/276,107 13 May 2014 (13.05.2014) US

(71) Applicant: **GOOGLE TECHNOLOGY HOLDINGS LLC** [US/US]; 1600 Amphitheatre Parkway, Mountain View, CA 94043 (US).

(72) Inventors: **ALAMEH, Rachid, M.**; 4919 Daniel Drive, Crystal Lake, IL 60014 (US). **SLABY, Jiri**; 970 Indian Spring Lane, Buffalo Grove, IL 60089 (US).

(74) Agent: **LEE, Kwanwoo**; Faegre Baker Daniels LLP, 311 S. Wacker Drive, Suite 4400, Chicago, IL 60606 (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, LU, LY, MA, MD, ME, MG, MK, MN, MW, MX, MY, MZ, NA, NG, NI, NO, NZ, OM, PA, PE, PG, PH, PL, PT, QA, RO, RS, RU, RW, SA, SC, SD, SE, SG, SK, SL, SM, ST, SV, SY, TH, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, ZA, ZM, ZW.

(84) Designated States *(unless otherwise indicated, for every kind of regional protection available)*: ARIPO (BW, GH, GM, KE, LR, LS, MW, MZ, NA, RW, SD, SL, ST, SZ, TZ, UG, ZM, ZW), Eurasian (AM, AZ, BY, KG, KZ, RU, TJ, TM), European (AL, AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HR, HU, IE, IS, IT, LT, LU, LV, MC, MK, MT, NL, NO, PL, PT, RO, RS, SE, SI, SK,

[Continued on next page]

(54) Title: ELECTRONIC DEVICE AND METHOD FOR CONTROLLING ACCESS TO SAME

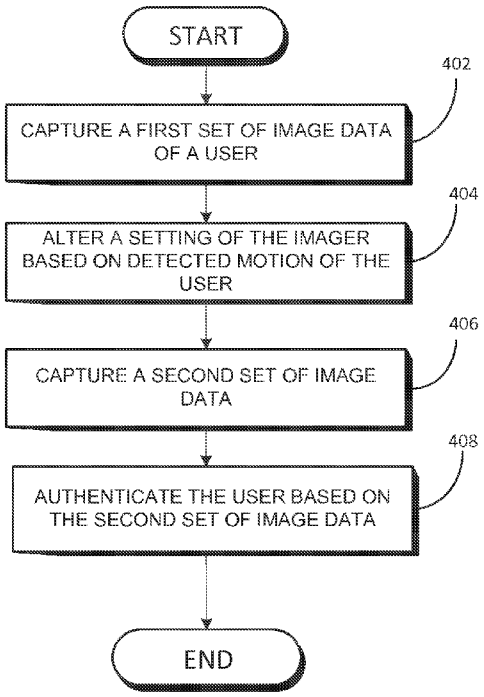

FIG. 4

(57) Abstract: An electronic device is able to alter one or more settings of its imager based on the motion of a user that the device is attempting to authenticate. The electronic device, in one implementation, captures a first set of image data of the user (e.g., a video or still photo of the user), detects motion of the user, alters a setting of the imager based on the motion, captures a second set of image data of the user, and authenticates the user based on the second set of image data. In some implementations, the electronic device has multiple imagers, and activates one or more additional imagers based on the detected motion of the user.

WO 2015/175634 A1

SM, TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, KM, ML, MR, NE, SN, TD, TG).

Published:

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

ELECTRONIC DEVICE AND METHOD FOR CONTROLLING ACCESS TO SAME

TECHNICAL FIELD

[0001] The present disclosure is related generally to user authentication techniques on electronic devices.

BACKGROUND

[0002] Although the potential advantages of using biometric authentication over traditional personal identification number ("PIN") authentication have long been understood, its use in consumer electronic devices has only recently become popular. With biometric authentication, a user does not need to enter a PIN and, under the right conditions, does not even need to touch the device in order to unlock it.

[0003] Most existing biometric authentication schemes use the same basic access logic that traditional PIN-based systems use. That is, a user is either authenticated or is not. The user either gains full access or no access. Furthermore, they generally do not adjust in real-time for dynamic conditions such as the movement and position of the user.

DRAWINGS

[0004] While the appended claims set forth the features of the present techniques with particularity, these techniques, together with their objects and advantages, may be best understood from the following detailed description taken in conjunction with the accompanying drawings of which:

[0005] FIG. 1A is a front view of an electronic device according to an embodiment;

[0006] FIG. 1B is a rear view of an electronic device according to an embodiment;

[0007] FIG. 2 is a block diagram of the electronic device according to an embodiment;

[0008] FIG. 3 is a diagrammatic view of a scenario in which the electronic device may be used;

[0009] FIG. 4 is a process flow diagram of a method that may be carried out in an embodiment;

[0010] FIG. 5 is a diagrammatic view of another scenario in which the electronic device may be used; and

[0011] FIG. 6 is a process flow diagram of a method that may be carried out in another embodiment.

DESCRIPTION

[0012] According to various embodiments of the disclosure, an electronic device (also referred to as "the device") is able to alter one or more settings of its imager (e.g., its camera) based on the motion of a user that the device is attempting to authenticate. In an embodiment, the device captures a first set of image data of the user (e.g., a moving video or still image of the user), alters a setting of the imager based on the motion, captures a second set of image data of the user, and authenticates the user based on the second set of image data.

[0013] According to an embodiment of the disclosure, the device grants the user a first level of access to the device based on the first set of image data and grants the user second level of access to the device based on the second set of image data. The number of possible access levels is not limited, and the example of two levels discussed herein is only meant to be illustrative. Additionally, the electronic device may capture the two sets of image data with two different imagers, stitch the sets of image data together, and carry out authentication on the stitched sets of image data. The number of imagers that may be used is not limited to two, however.

[0014] Turning to FIG. 1A and FIG. 1B, an embodiment of the electronic device ("the device"), generally labeled 100, includes a housing 102 having a front side 104 and a rear side 106. Set along the perimeter of the housing are a first imager 110A, a second imager 110B, a third imager 110C, and a fourth imager 110D. Each of the first through fourth imagers has a field of view that extends outwardly from the perimeter of the device 100. Also set along the perimeter of the device 100 are a first motion sensor 116A, a second motion sensor 116B, a third motion sensor 116C, and a fourth motion sensor 116D. Each motion sensor is configured to sense motion external to device 100. Each motion sensor may be implemented as a passive infrared detector, such as a digital thermopile sensor, or as an active sensor that uses reflected light of a light source of the device 100.

[0015] Set within the front side 104 of the housing 102 is a display 108 (e.g., an organic light-emitting diode display) and a fifth imager 110E (e.g., a front facing camera). Set within the rear side 106 of the housing 102 is a sixth imager 110F (e.g., a rear facing camera). Although depicted in FIGS. 1A and 1B as a smartphone, the electronic device 100 may be implemented as other types of devices, including a tablet computer, portable gaming device, and a wearable device (e.g., a smart watch).

[0016] Turning to FIG. 2, an embodiment of the electronic device 100 includes a processor 202, network communication hardware 204 (e.g., WiFI chip or a cellular baseband chipset), an audio output 206 (e.g., a speaker), a memory 208 (which can be implemented as volatile memory or non-volatile memory), and a light source 212 (e.g., an infrared light-emitting diode). In various embodiments, the processor 202 retrieves instructions and data from the memory 208 and, using the instructions and data, carries out the methods described herein. Each of the elements of FIG. 2 (including the elements of FIGS. 1A and 1B that appear in FIG. 2) is communicatively linked to one or more other elements via one or more data pathways 226. Possible implementations of the data pathways 226 include wires, conductive pathways on a microchip, and wireless connections. Possible implementations of the processor 202 include a microprocessor and a controller.

[0017] Turning to FIG. 3 and to the flowchart of FIG. 4, a procedure that the device 100 carries out to authenticate a user in an embodiment will now be described. As shown in FIG. 3, the electronic device 100 is lying on a table in a room 304. A user 302 of the device enters the room 104 at position A and is moving. When the user is at position A, the first motion sensor 116A detects the user 302 and provides data regarding the user to the processor 202 (FIG. 2), including data regarding the user's position, motion (including the user's gait), speed, and context. In response to receiving the data, the processor 202 turns on the first imager 110A and controls the first imager 110A to capture a first set of image data (i.e., a still image, multiple still images, or multiple images organized as a moving image) of the user 302 (block 402) and provides the first set of image data to the processor 202. The processor 202 attempts to authenticate the user 302 using the first set of image data. For example, the processor 202 may attempt to authenticate the user 302 based on biometric data, such as the user's body geometry (e.g., the user's body shape, gender, height, girth, and gait). Thus, if the processor 202 knows that an authorized user is a tall male, and the image data indicates that the user 302 is a tall male, then the processor 202 will determine that it is possible that the

user 302 is the authorized user. Conversely, if the image data indicates that the user 302 is a short female, then the authentication will fail.

[0018] In this scenario, the processor 202 determines, with at least a 50% confidence level (based on its authentication attempt with the first set of image data) that the user 302 is an authorized user. Based on this determination, the processor 202 grants the user 302 a first level of access to the device 100. The first level of access may involve granting the user 302 access to telephone functions or lower security applications of the device 100. For example, the processor 202 may control the audio output 206 to inform that user 302 that "You missed two phone calls and have one voicemail." The processor 202 may also control the display 108 to display the user's access level (e.g., "You are now able to access the phone functions").

[0019] The processor 202 continues to receive data (position, motion, speed, and context) from the first motion sensor 116A. The processor 202 analyzes the data from the first motion sensor 116A. At block 404, the processor 202 alters a setting of the first imager 116A based on the detected motion. For example, the processor 202 may determine, based on the detected motion, that the user 302 is moving at or above a certain speed threshold (e.g., 3 feet per second), and, based on this fact, may increase the frame rate of the first imager 110A (e.g., from 20 frames per second ("fps") to 50 fps). This increase in frame rate allows the first imager 110A to obtain more detail about the user in order to compensate for the fact that the user 302 is now in motion or is now moving faster. Other ways that the processor 202 can alter a setting of the first imager 110A include controlling the first imager 110A to change one or more of its shutter speed, shutter timing, illumination setting, resolution, aperture, and zoom setting. In various embodiments, any or all of these changes may be triggered by the same motion sensor that prompted the processor 202 to turn on the first imager 202.

[0020] After the processor 202 alters the setting, the processor 202 controls the first imager 110A to capture a second set of image data of the user 302 (block 406) and provide the second set of image data to the processor 202. For example, the processor 202 may receive a second moving video of the user from the first imager 110A, this time at the higher frame rate.

[0021] In this example, it is assumed that the processor 202 is able to use the second set of image data (e.g., the second, higher-frame-rate moving video) to authenticate the user 302 (block 408). For example, the processor 202 may authenticate the user 302 with a high

enough confidence level to grant the user 302 a second level of access. The processor 214 grants the user 302 the second level of access to the device 100 based on the second set of image data. Granting the second level of access may involve the processor 202 granting the user 302 access to one or more of pictures, files, emails, or higher security applications on the device 100. The processor 202 may also control the display 108 to display the user's access level (e.g., "You are now able to access email").

[0022] In another embodiment, the device 100 uses multiple imagers to gradually authenticate a user. Referring to FIGS. 5 and 6, a procedure for doing so will now be described.

[0023] As shown in FIG. 5, the electronic device 100 is lying on a table in a room 504. A user 502 of the device enters the room 504 at position A and is moving. When the user is at position A, the first motion sensor 116A detects the user 502 and provides data regarding the user, such as the user's position, motion (including the user's gait), speed, and context, to the processor 202 (FIG. 2). In response to receiving the data, the processor 202 turns on the first imager 110A and controls the first imager 110A to capture a first set of image data of the user 302 (block 602) and provides the first set of image data to the processor 202. The processor 202 attempts to authenticate the user 502 using the first set of image data. In this scenario, the processor 202 determines, with at least a 50% confidence level based on its authentication attempt with the image data that the user 502 is an authorized user. Based on this determination, the processor 202 grants the user 502 a first level of access to the device 100 (block 604).

[0024] The processor 202 then receives data regarding the user, including the user's position, motion (including the user's gait), speed, and context, from the second motion sensor 116B. The processor 202 analyzes the data from the second motion sensor 116B and, based on this motion data (and possibly based on further data from the first motion sensor 116A) determines that the user 502 has moved within viewing range of the second imager 110B. The processor 202 reacts by turning on the second imager 110B and controlling the second imager 110B to capture a second set of image data of the user 502 (block 606). The controller 202 then stitches the first set of image data and the second set of image data together (block 608). This stitching process allows the processor 202 to get a more comprehensive view of the user 502 and attempt to authenticate the user 502 on that basis. At block 610, the processor 202 grants the user 502 a second level of access to the electronic device 100 based

on the stitched first and second sets of image data. In doing so, the processor 202 may also use the stitched images to assess the environment surrounding the device 100—such as the walls, ceiling, room settings, and table—and grant a level access to the user if the processor 202 determines that the environment is specific to the user (the user's house, office, car, etc.) The processor 202 can also use the surrounding environment to reinforce the biometric data (i.e., the user's gait, etc.) collected regarding the user. In this scenario, the combination of the environmental authentication and the biometric authentication is enough for the processor 202 to raise the level of access from a first level to a second level at block 610.

[0025] The process described in conjunction with FIG. 6 is not limited to two imagers. For example, if the user 502 continued to walk around the device 100, the third and fourth motion sensors 116C and 116D could detect the motion and signal the processor 202. The processor 202 could react by activating the third imager 110C and the fourth imager 110D, respectively, control the imagers to capture third and fourth sets of video data, and perform stitching (and possibly environmental analysis) in order to grant the second level of access, or even to grant further levels of access.

[0026] Furthermore, the process described in conjunction with FIG. 6 may also be carried out with sensors of the device 100, such as the motion sensors 116A-116D. For example, as the user walks around the device 100, the processor 202 may stitch the data from the first motion sensor 116A and the second motion sensor 116B together. The stitched data can be used, for example, to map the XY position of the user, and may be part of the basis upon which the processor 202 grants the first or second level of access.

[0027] It should be understood that the embodiments described herein should be considered in a descriptive sense only and not for purposes of limitation. Descriptions of features or aspects within each embodiment should typically be considered as available for other similar features or aspects in other embodiments.

[0028] While one or more embodiments of the have been described with reference to the figures, it will be understood by those of ordinary skill in the art that various changes in form and details may be made therein without departing from their spirit and scope of as defined by the following claims. For example, the steps of the flow diagrams of FIGS. 4 and 6 can be reordered in way that will be apparent to those of skill in the art. Steps may also be added to the flow diagrams of FIGS. 4 and 6 without departing from the spirit of the disclosure.

CLAIMS

We claim:

1. A method for controlling access to an electronic device, the method comprising:

capturing a first set of image data of a user with an imager of the electronic device;

altering a setting of the imager based on detected motion of the user;

capturing a second set of image data of the user with the imager after altering the setting; and

authenticating the user a second level of access to the electronic device based on the second set of image data.

2. The method of claim 1, further comprising:

granting the user a first level of access to the electronic device based on the first set of image data; and

granting the user a second level of access to the electronic device based on the second set of image data.

3. The method of claim 2, wherein

granting the first level of access comprises granting the user access to telephone functions or lower security applications of the electronic device,

granting the second level of access comprises granting the user access to one or more of pictures, files, emails, and higher security applications on the electronic device.

4. The method of claim 1, further comprising

carrying out a first authentication procedure on the user based on the user's body geometry with the first set of image data;

carrying out a second authentication procedure on the user based on the user's body geometry with the second set of image data.

5. The method of claim 4, wherein the user's body geometry is one or more of the user's body shape, body size, and gait.

6. The method of claim 1, wherein the setting is one or more of the imager's frame rate, shutter speed, shutter timing, illumination, resolution, aperture, and zoom.

7. The method of claim 1, further comprising changing the illumination intensity of a light source on the electronic device based on the detected motion of the user.

8. A method for controlling access to an electronic device, the method comprising:

capturing a first set of image data of a user with a first imager of the electronic device;

granting the user a first level of access to the electronic device based on the first set of image data;

based on detected motion of the user, capturing a second set of image data of the user with a second imager of the electronic device;

stitching the first and second sets of image data together; and

granting the user a second level of access to the electronic device based on the stitched first and second sets of image data.

9. The method of claim 8, further comprising:

using the stitched first and second sets of image data to assess the environment surrounding the electronic device; and

granting the second level access based on the assessment.

10. The method of claim 9, further comprising:

using one or more of the first and second sets of image data to make a biometric assessment of the user; and

granting the second level access based on the combination of the environmental assessment and the biometric assessment.

11. An electronic device comprising:

an imager configured to capture a first set of image data of a user; and

a processor configured to

grant the user a first level of access to the electronic device based on the first set of image data;

alter a setting of the imager based on detected motion of the user,

wherein the imager is further configured to capture a second set of image data of the user based on the altered setting, and

wherein the processor is further configured to grant the user a second level of access to the electronic device based on the second set of image data.

12. The electronic device of claim 11, wherein the processor is further configured to

carry out a first authentication procedure on the user based on the user's body geometry with the first set of image data; and

carry out a second authentication procedure on the user based on the user's body geometry with the second set of image data.

13. The electronic device of claim 11, wherein

the processor is further configured to grant the first level of access by granting the user access to telephone functions or lower security applications of the electronic device,

the processor is further configured to grant the second level of access by granting the user access to one or more of pictures, files, emails, and higher security applications on the electronic device.

14. A method for controlling access to an electronic device, the method comprising:

capturing a first set of image data of a user with a first imager of the electronic device;

granting the user a first level of access to the electronic device based on the first set of image data;

based on detected motion of the user, capturing a second set of image data with a second imager of the electronic device;

stitching the first and second sets of data together; and

granting the user a second level of access to the electronic device based on the stitched first and second sets of image data.

15. The method of claim 14, further comprising activating the second imager based on the detected motion.

16. The method of claim 14, further comprising:

receiving data regarding the user from a first motion sensor and a second motion sensor;

stitching the data from the first motion sensor and the second motion sensor together,

wherein granting the user the second level of access comprises granting the user a second level of access based, at least in part, on the stitched data from the first motion sensor and the second motion sensor.

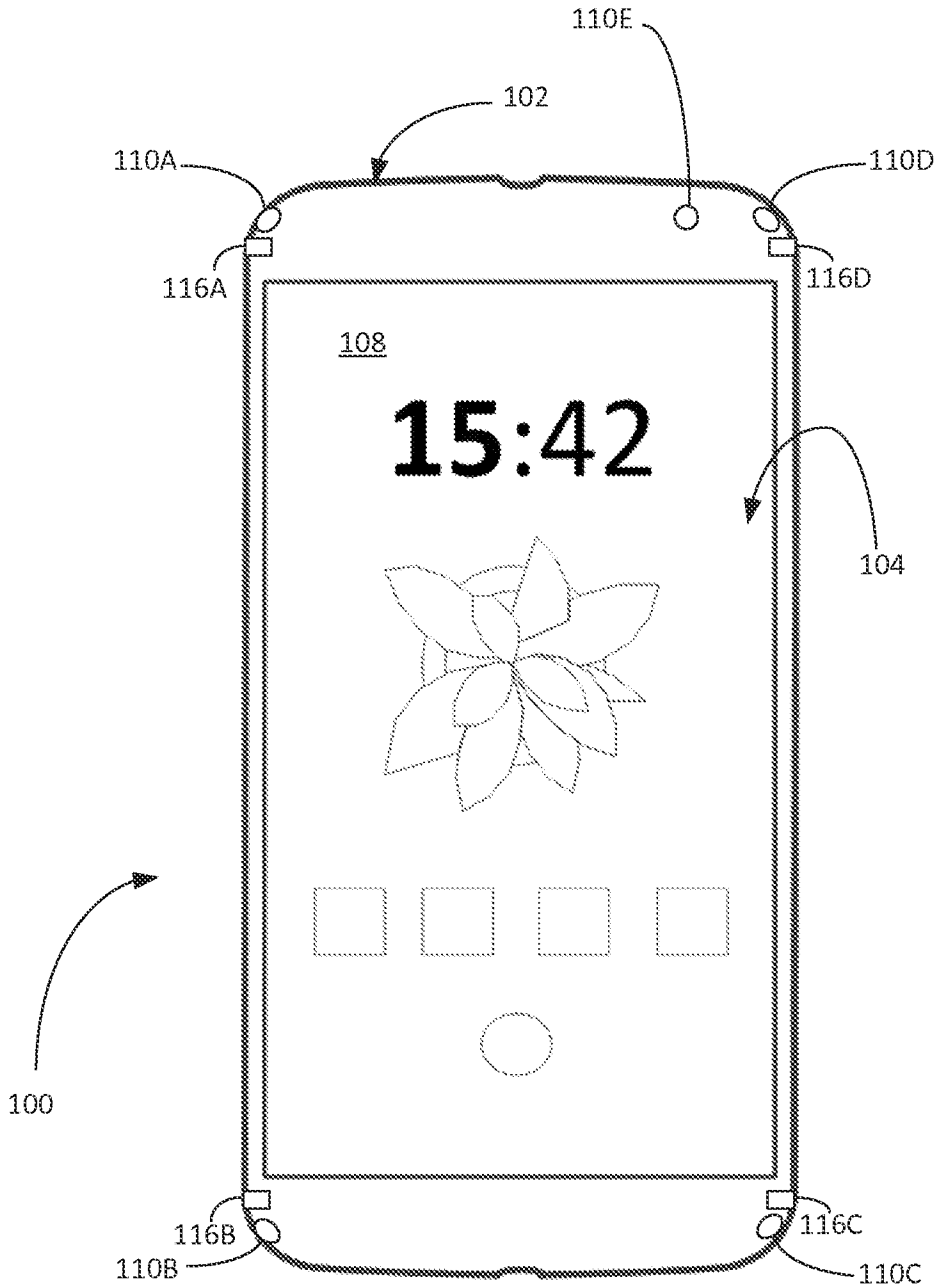
110E
102
110A
110D
116A
116D
108
15:42
104
100
116B
116C
110B
110C

FIG. 1A

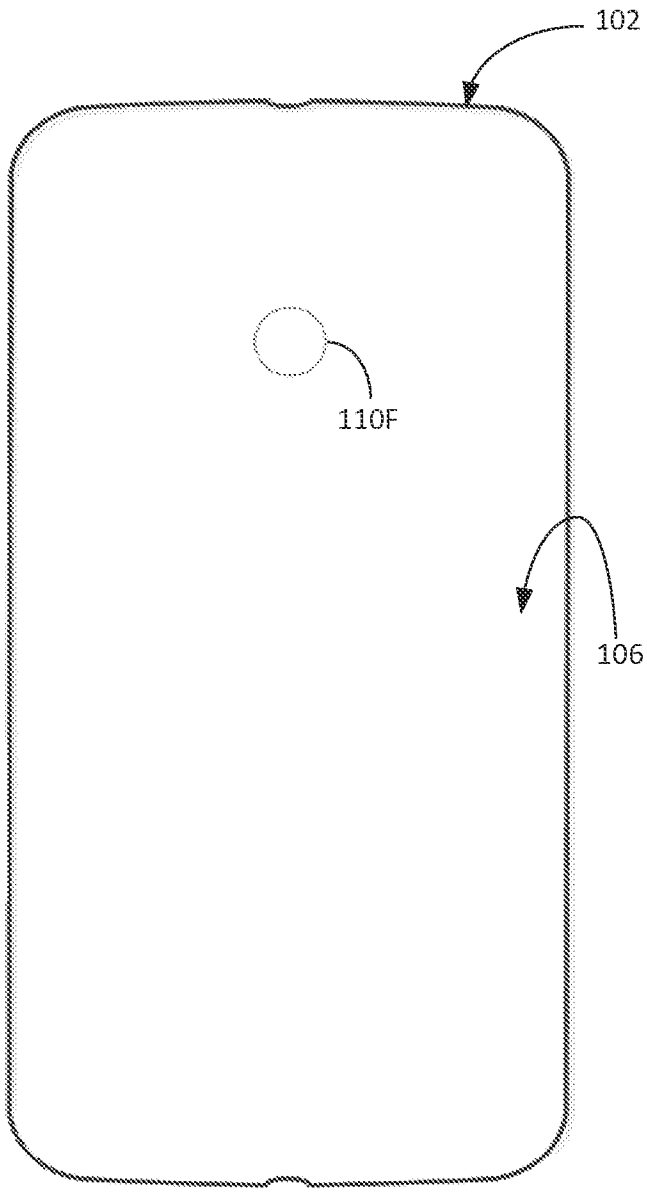

FIG. 1B

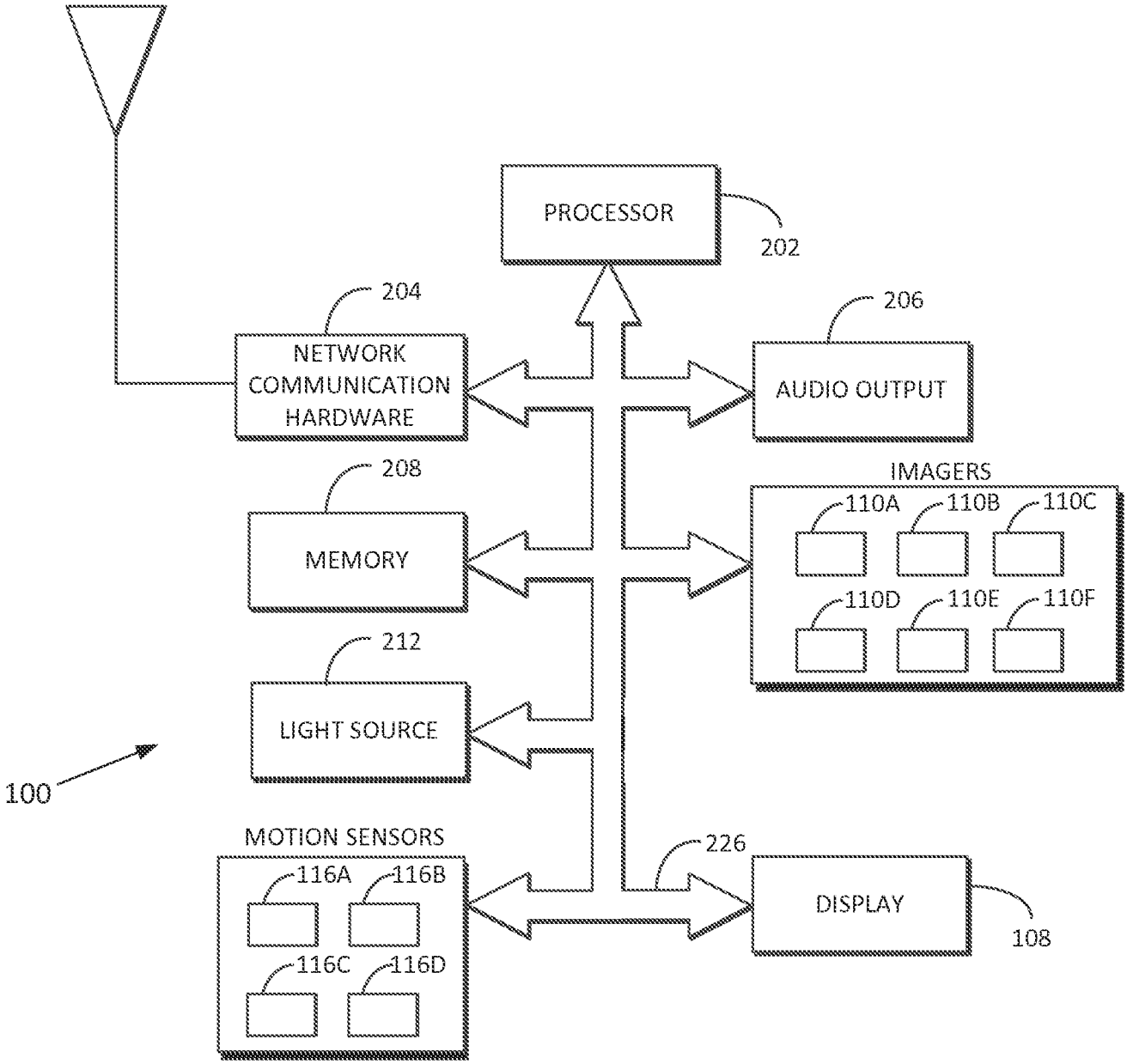
PROCESSOR
202
204
NETWORK COMMUNICATION HARDWARE
206
AUDIO OUTPUT
208
MEMORY
IMAGERS
110A
110B
110C
110D
110E
110F
212
LIGHT SOURCE
100
MOTION SENSORS
116A
116B
116C
116D
226
DISPLAY
108

FIG. 2

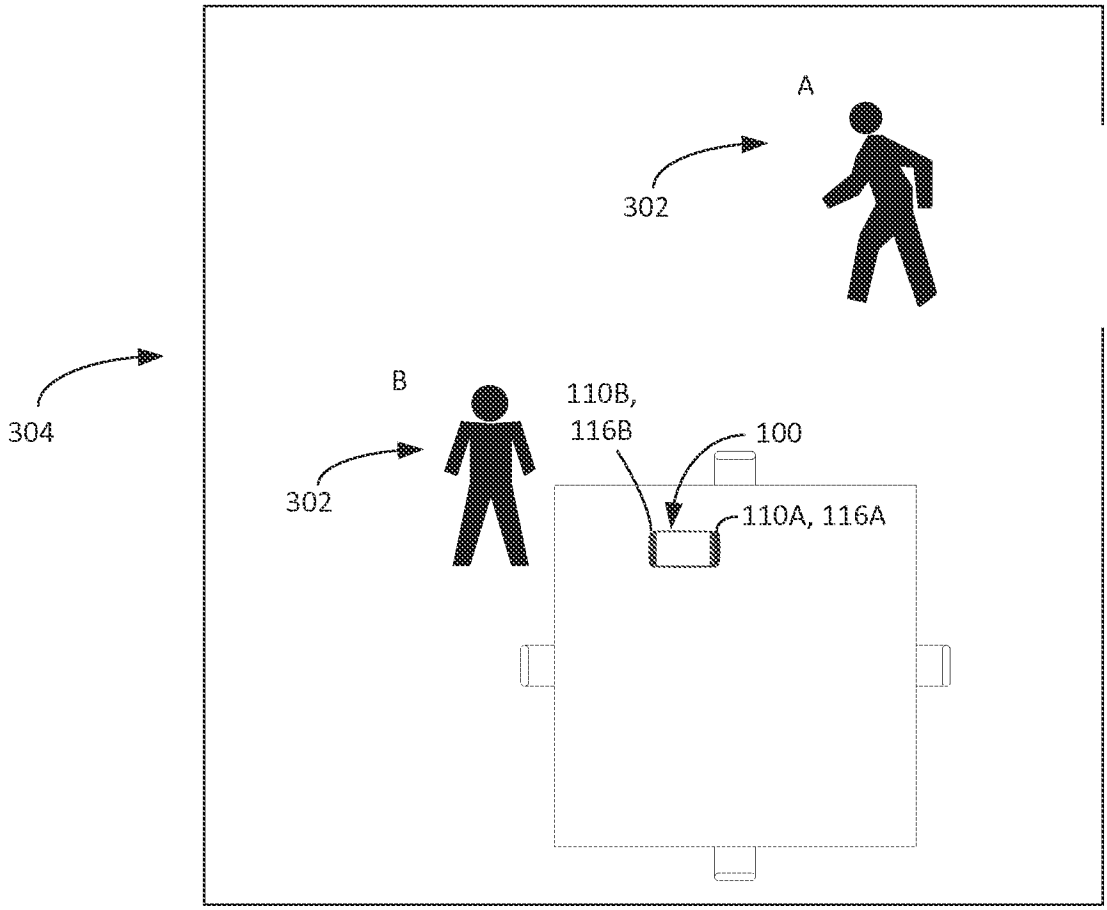

FIG. 3

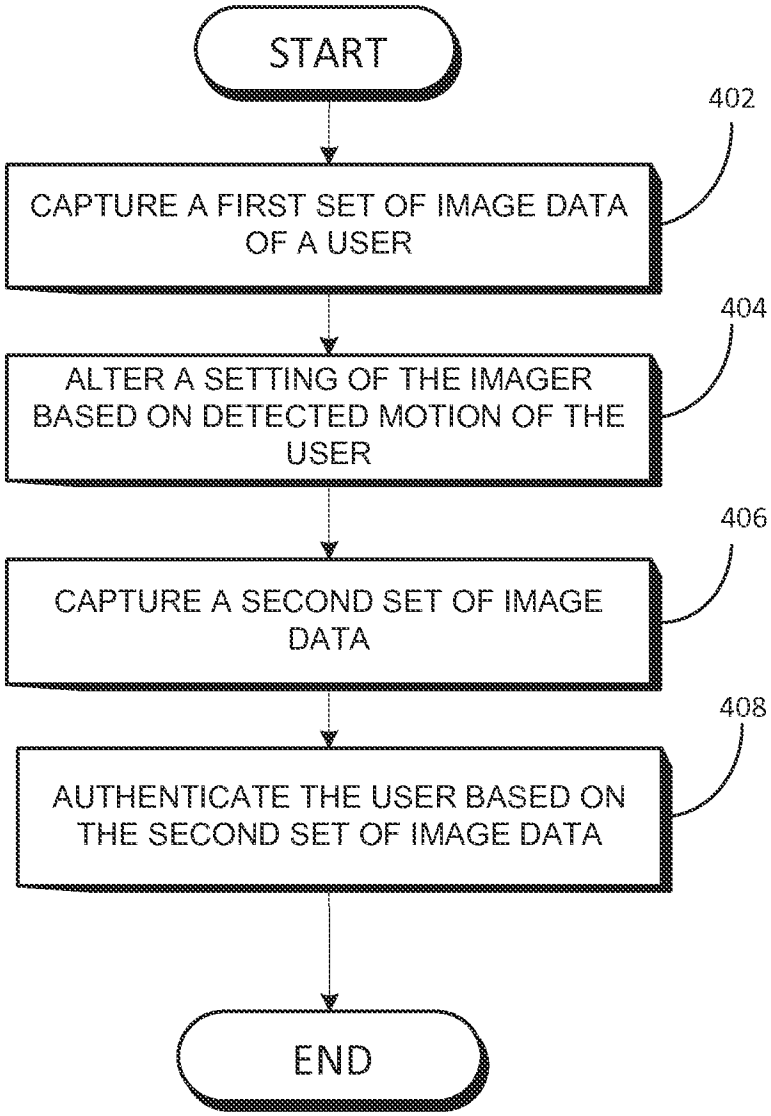
START
402
CAPTURE A FIRST SET OF IMAGE DATA OF A USER
404
ALTER A SETTING OF THE IMAGER BASED ON DETECTED MOTION OF THE USER
406
CAPTURE A SECOND SET OF IMAGE DATA
408
AUTHENTICATE THE USER BASED ON THE SECOND SET OF IMAGE DATA
END

FIG. 4

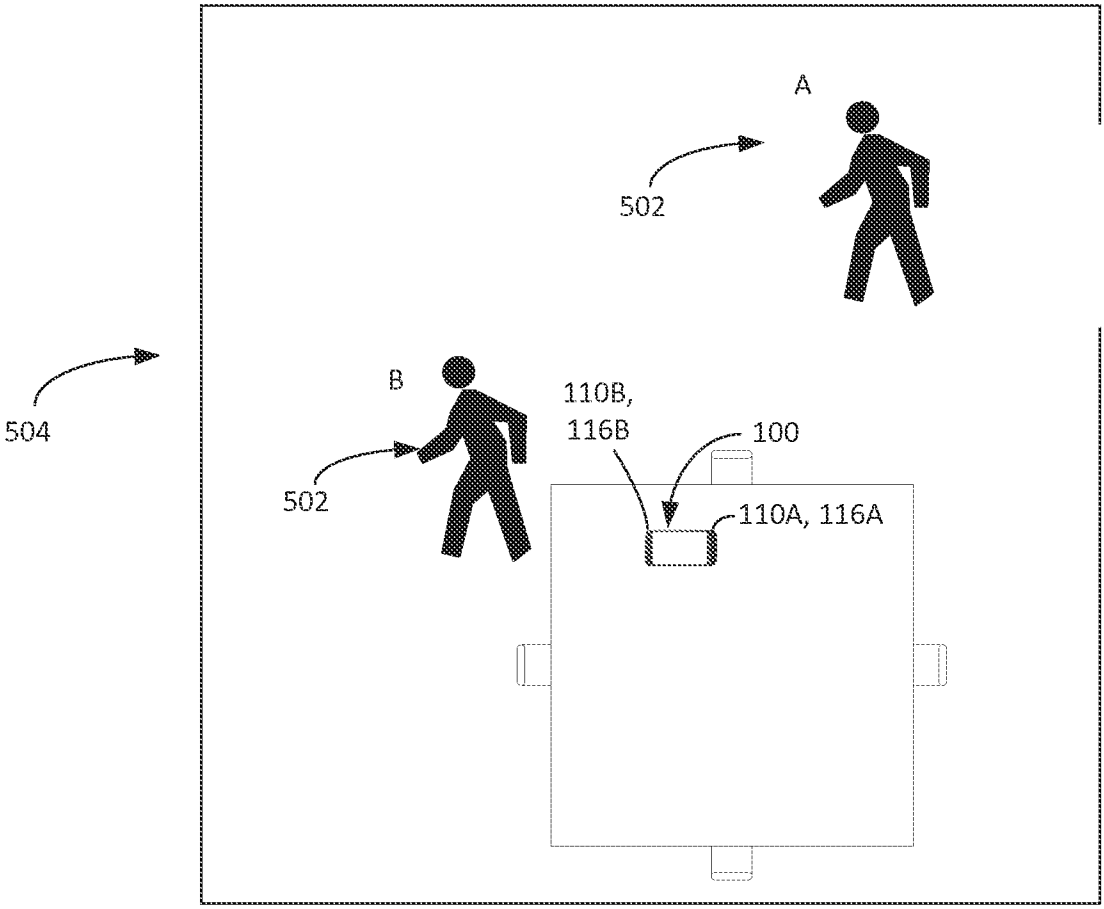

FIG. 5

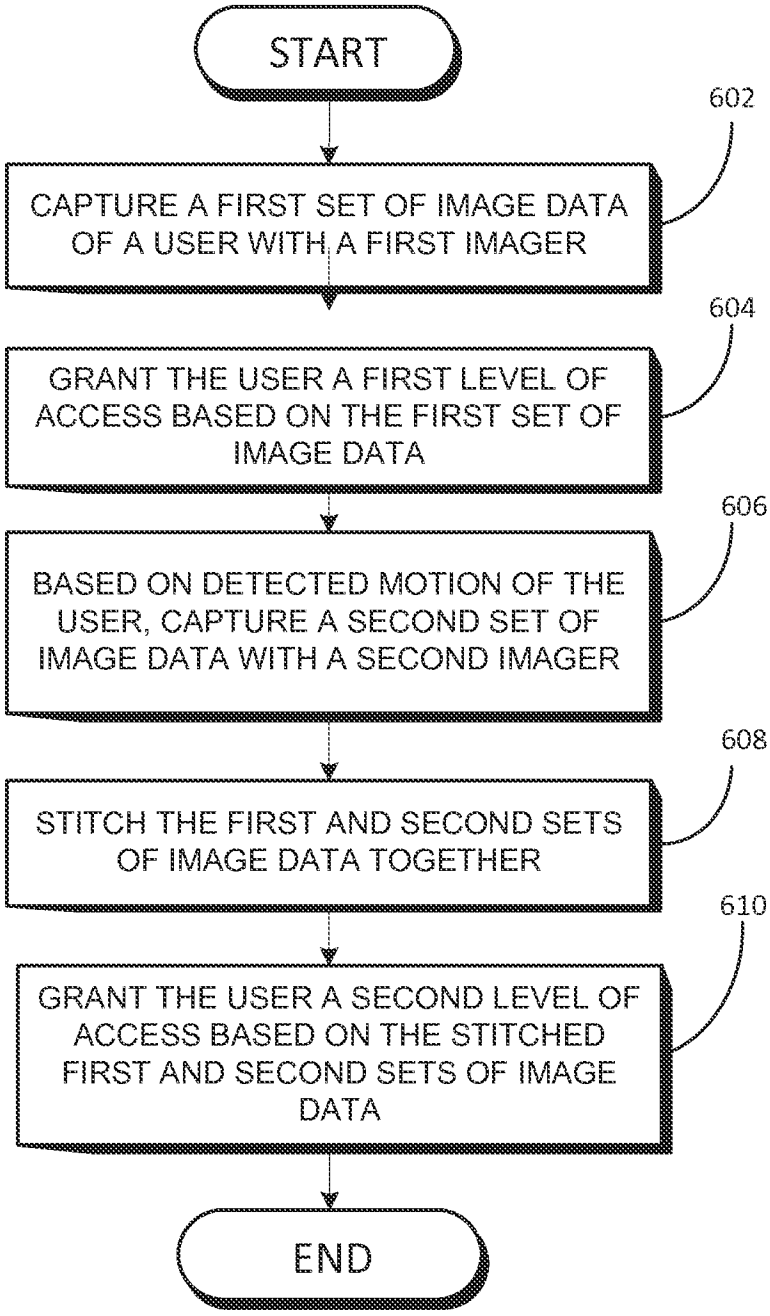
START
602
CAPTURE A FIRST SET OF IMAGE DATA OF A USER WITH A FIRST IMAGER
604
GRANT THE USER A FIRST LEVEL OF ACCESS BASED ON THE FIRST SET OF IMAGE DATA
606
BASED ON DETECTED MOTION OF THE USER, CAPTURE A SECOND SET OF IMAGE DATA WITH A SECOND IMAGER
608
STITCH THE FIRST AND SECOND SETS OF IMAGE DATA TOGETHER
610
GRANT THE USER A SECOND LEVEL OF ACCESS BASED ON THE STITCHED FIRST AND SECOND SETS OF IMAGE DATA
END

FIG. 6

INTERNATIONAL SEARCH REPORT

International application No
PCT/US2015/030527

A. CLASSIFICATION OF SUBJECT MATTER
INV. G06F21/32 H04L29/06
ADD.

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
G06F H04L H04W

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)
EPO-Internal, WPI Data, COMPENDEX, INSPEC

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
Y	EP 1 990 769 A1 (OKI ELECTRIC IND CO LTD [JP]) 12 November 2008 (2008-11-12) abstract; figures 1-5 paragraphs [0001] - [0011], [0020] - [0025], [0028] - [0031], [0038], [0040] - [0044], [0055] - [0070]	1-16
Y	GB 2 474 536 A (POINTGRAB LTD [IL]) 20 April 2011 (2011-04-20) abstract paragraphs [0001] - [0005], [0074] - [0077]	1-16

-/--

[X] Further documents are listed in the continuation of Box C.

[X] See patent family annex.

* Special categories of cited documents :

"A" document defining the general state of the art which is not considered to be of particular relevance

"E" earlier application or patent but published on or after the international filing date

"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)

"O" document referring to an oral disclosure, use, exhibition or other means

"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art

"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
26 August 2015	02/09/2015

Name and mailing address of the ISA/	Authorized officer
European Patent Office, P.B. 5818 Patentlaan 2 NL - 2280 HV Rijswijk Tel. (+31-70) 340-2040, Fax: (+31-70) 340-3016	López Monclús, I

1

Form PCT/ISA/210 (second sheet) (April 2005)

INTERNATIONAL SEARCH REPORT

International application No
PCT/US2015/030527

C(Continuation). DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	US 2012/038796 A1 (POSA JOHN G [US] ET AL) 16 February 2012 (2012-02-16) abstract figures 1,3,4 paragraphs [0002] - [0004], [0006], [0013], [0014], [0019] - [0021], [0024] - [0026]	1-16

1

INTERNATIONAL SEARCH REPORT

Information on patent family members

International application No
PCT/US2015/030527

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
EP 1990769 A1	12-11-2008	EP 1990769 A1	12-11-2008
		JP 4367424 B2	18-11-2009
		JP 2007226327 A	06-09-2007
		KR 20080106426 A	05-12-2008
		US 2009060293 A1	05-03-2009
		WO 2007097144 A1	30-08-2007
GB 2474536 A	20-04-2011	GB 2474536 A	20-04-2011
		GB 2483168 A	29-02-2012
		TW 201129918 A	01-09-2011
		US 2012200494 A1	09-08-2012
		US 2014043234 A1	13-02-2014
		US 2014145941 A1	29-05-2014
		WO 2011045789 A1	21-04-2011
US 2012038796 A1	16-02-2012	NONE	