



- (51) **International Patent Classification:**
G06F 21/32 (2013.01) *G06K 9/00* (2006.01)
G06F 3/01 (2006.01)
- (21) **International Application Number:** PCT/IB2016/001623
- (22) **International Filing Date:** 21 October 2016 (21.10.2016)
- (25) **Filing Language:** English
- (26) **Publication Language:** English
- (30) **Priority Data:**
62/221,225 21 September 2015 (21.09.2015) US
15/286,877 6 October 2016 (06.10.2016) US
- (71) **Applicant:** FACEBOOK, INC. [US/US]; 1601 Willow Road, Menlo Park, CA 94025 (US).
- (72) **Inventors:** PRIESUM, Jonas; Islands Brygge 30B, 5.6, 2300 Copenhagen (DK). SAN AGUSTIN, Javier; Jagtvej 55. 2. th, 2200 Copenhagen (DK).

(74) **Agents:** MÜLLER-BORÉ & PARTNER et al.; Patentanwälte PartG mbB, Friedenheimer Brücke 21, 80639 München (DE).

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

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

[Continued on next page]

(54) **Title:** METHOD FOR USING EYE TRACKING AND EYE BIOMETRICS FOR AUTHENTICATION

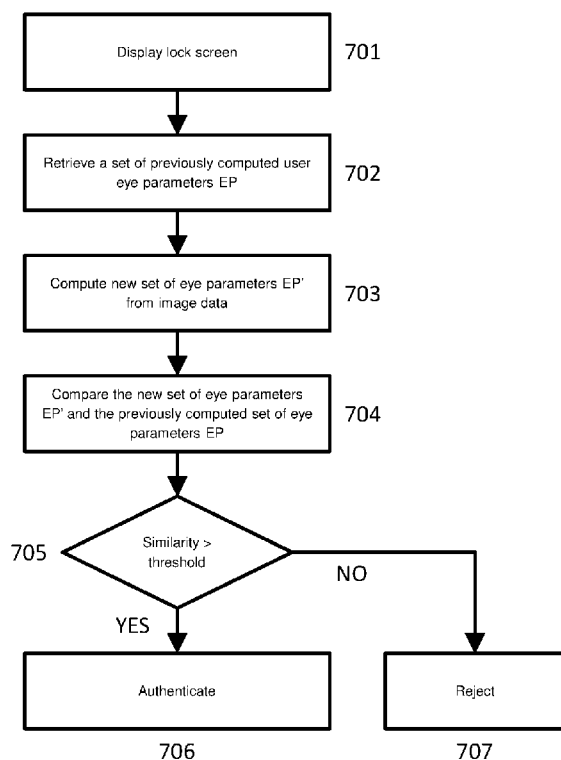


Fig. 7

(57) **Abstract:** The invention is a method for authenticating a system user based on eye tracking or eye parameters.



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))

— before the expiration of the time limit for amending the claims and to be republished in the event of receipt of amendments (Rule 48.2(h))

— with information concerning request for restoration of the right of priority in respect of one or more priority claims (Rules 26bis.3 and 48.2(b)(vii))

TITLE OF THE INVENTION

METHOD FOR USING EYE TRACKING AND EYE BIOMETRICS

FOR AUTHENTICATION

BACKGROUND

[0001] There is an indisputable trend where people are using handheld devices for communications, information access, financial transactions, and more. With tens of millions of smartphone systems in users' hands, these systems have become repositories for sensitive applications and data. As such, it is increasingly important the users feel secure that their systems will only operate under each user's control.

[0002] Many such systems now incorporate four-digit passcodes which allow operation only when someone enters the proper code. But, anyone can do so if the code is known. Fingerprint authentication subsystems and methods are also in limited use. With these, the user swipes a fingertip over a sensor and if the fingerprint matches a previously stored one, the user is authenticated and now able to operate the system.

SUMMARY

[0003] The invention disclosed and claimed is a method for using eye tracking or eye parameters as a way to authenticate a user's access to a system either alone or in combination with other authentication subsystems and methods.

[0004] With eye tracking, one would look at an image, and in particular, at a specific area the user has predefined as an unlocking area. When the gaze coordinates are found to coincide with the unlock area's coordinates, and the gaze is maintained for some interval of time, the system is unlocked.

[0005] In another embodiment, eye parameters are measured and stored for a user, and each time the system is used subsequently, new eye parameters are measured and compared. If the similarity between the initial stored parameters and the current parameters meet or exceed a threshold value, then the user is authenticated and operation of the system is enabled.

[0006] Either or both embodiments may be used in conjunction with other authentication methods, such as fingerprint matching, to provide a higher level of security.

BRIEF DESCRIPTIONS OF THE DRAWINGS

[0007] Figure 1 depicts a person holding a smartphone system and gazing at an unlock area.

[0008] Figure 2 illustrates how a particular area of a screen image may be designated by the user as the unlock area, and when gazed at for some interval of time, will serve as an authentication

[0009] Figure 3 is a flow diagram of one embodiment of the method whereby eye tracking and gaze coordinates are used to determine if a user is gazing at an unlock area.

[00010] Figure 4 illustrates a sequence in which the user's system displays a locked screen image, followed by the user gazing at the unlock area, and the system then unlocks.

[00011] Figure 5 illustrates a combinatorial authentication scheme where by eye tracking and fingerprint detection is used to authenticate.

[00012] Figure 6 shows a variety of eye parameters that may be measured and stored based on light-source illumination and camera capture of various eye metrics.

[00013] Figure 7 is a flow diagram of another embodiment of the method whereby eye parameters are captured and compared, and if the similarity is above some predetermined threshold, then the user is authenticated.

[00014] Figure 8 illustrates a sequence in which the user's system displays a locked screen containing an unlock object, followed by the user gazing at the unlock object, and the system then unlocks.

DETAILED DESCRIPTION

[00015] With tens of millions of smartphones in use with many hosting sensitive applications and data, it is important for users to feel secure that their systems can only be operated under their control.

[00016] A common method for authentication is a four-digit passcode, such as 1 2 3 4, which the user predefines when setting up the system for the first time. Subsequent operation will require inputting that same passcode. However, anyone who knows that code can enter it and gain operational access.

[00017] Many laptop computers manufactured since 2005 are outfitted with fingerprint detection sensors and fingerprint matching authentication software. When initially setting up the computer, the user swipes his or her finger over the sensor and establishes the fingerprint data profile. Subsequent access and operation can be enabled by again swiping the same fingertip and having a match occur with the stored fingerprint profile.

[00018] Using eye tracking or eye parameter technologies, one can develop an alternative or combinatorial authentication method that can bolster the authentication security of any one method.

[00019] Eye tracking makes use of sensors to determine where someone is gazing. There are many eye tracking technologies available.

[00020] If a user makes use of eye tracking technology to first predefine an area of the screen as an unlock area; then subsequently using eye tracking technology, the system can determine if a user is gazing at the unlock area. In figure 1, the user by gazing at the area 101 can

designate that area as the unlock area, and subsequently if the user gazes at area 101 for some period of time, the eye tracking technology can substantiate it and authenticate the user.

[00021] Figure 2 illustrates a system with a display screen image where one area (e.g. the cloud) has been previously defined as the unlock area. When a user then gazes at the cloud for some minimal period of time, the eye tracking subsystem substantiates it and the system is then unlocked. Note that one can use gaze duration or a limit to the number of distinct gazes to mitigate attempts to establish authorization by someone other than the user

[00022] The flow diagram of Figure 3 shows one embodiment of the method disclosed and claimed. After a display lock screen has been displayed (301), a set of previously measured and computed user calibration parameters, CP, are retrieved (302). The current user gaze coordinates are measured and computed using the CP data (303). From the gaze coordinates and predetermined unlock area coordinates the distance between the two is computed (304). The distance is compared to a threshold distance (305), and if less than the threshold value, the user is authenticated (306). If greater than the threshold value (307) the authentication is rejected.

[00023] The set of calibration parameters CP may include coefficients of regression equations, projective transformations, affine transformations, mappings between coordinate systems, or any combination of these.

[00024] The set of calibration parameters may be computed when the user sets up the device for the first time, that is, via a calibration procedure. In some embodiments, one or more calibration parameters may be computed and updated while the user uses the device, so that a set of recent calibration parameters is available for authentication.

[00025] Figure 4 shows a typical sequence in which the system with locked screen display (401) is gazed at such that the unlock area (402) is determined to be the gaze area and the system is unlocked (403).

[00026] Figure 5 shows a similar sequence to Figure 4 with the addition of fingerprint detection with eye tracking detection as the authentication method. Here the locked screen

display is shown (501) followed by a gaze at the unlock area (502) followed by the swipe of a fingertip (503). The gaze and fingerprint detection may occur simultaneously, too. In that case, the system may compare gaze data to the unlock area only during the time while the fingertip is placed on the scanner. This could prevent a malicious user from just looking around the screen until it unlocks. If the fingerprint matches the fingerprint data profile and the gaze area is determined to be the unlock area, then the system is unlocked (504).

[00027] Figure 6 illustrates some eye parameters that can be determined using one or more light sources and one or more cameras. The set of eye parameters could include the horizontal and vertical displacements between the optical axis and visual axis, which are designated as alpha and beta; it can also include the corneal radius, designated rc ; it can also include the distance between cornea center and pupil center, designated h . The eye parameter data, like fingerprint data, is essentially unique to each individual. A system outfitted with light source, camera, and pertinent computational algorithms could measure, calculate, and store one or plurality of such eye parameters.

[00028] Figure 7 shows another embodiment of the method whereby eye parameter data is used for authentication. First, a locked system display screen is displayed (701). A previously computed set of eye parameter data is retrieved (702). The current eye parameter data of a user is measured and computed (703). The current user eye parameter data is compared to the previously stored data (704). One way of comparing one set of eye parameters to another, for example, would be to use the Mahalanobis distance. The comparison value is compared to a predetermined similarity threshold value (705). If the similarity value exceeds the threshold value, the user is authenticated (706). If the similarity value is less than the threshold value, the authentication is rejected (707).

[00029] Figure 8 shows a typical sequence in which the system with locked screen display (801) is gazed at. In particular, the unlock area (802), e.g. the lock icon, is gazed at. The system

computes a set of current eye parameters, which are matched against the precomputed set of eye parameters, and the system is unlocked (803).

[00030] The set of eye parameters may be computed when the user sets up the device for the first time, that is, via a calibration procedure. In some embodiments, one or more eye parameters may be computed and updated while the user uses the device, so that an optimal set of eye parameters for the user is available for authentication.

[00031] In some embodiments, the set of eye parameters may include eye movement information, for example, saccade information (saccade latency, velocity and acceleration profile, saccade duration, or any combination of these). Saccade information may be computed by having the user look at two consecutive unlock areas, and tracking the eye movement and velocity during the saccadic movement taking place between those locations.

[00032] Similarly, the set of eye parameters may include information about smooth pursuit movement. The system may compute the smooth pursuit movement information by having the unlock object move smoothly with predetermined movement parameters such as acceleration, velocity and direction. When the user tracks the movement of the unlock object, a smooth pursuit eye movement takes place.

CLAIMS

What is claimed is:

1. A method comprising:

retrieving a set of one or more pre-computed stored eye tracking calibration parameters;

using said calibration parameters to determine a gaze area;

calculating a distance between said gaze area and the unlock area of a display screen;

comparing said distance to a predetermined threshold value.

2. A method as in claim 1, further comprising:

authenticating and unlocking a system if said distance is less than said threshold value,
and rejecting access otherwise.

3. A method as in claim 2 further comprising:

determining whether a second authentication criterion has been met;

keeping said system locked if said second authentication criterion has not been met.

4. A method as in claim 1 further comprising:

computing one or more said eye tracking calibration parameters during a calibration
procedure.

5. A method as in claim 1 further comprising:

computing one or more said eye tracking calibration parameters during system use.

6. A method as in claim 1 further comprising:

updating one or more said eye tracking calibration parameters after a successful authentication.

7. A method comprising:

retrieving a set of one or more pre-computed stored user eye parameters;

measuring current user eye parameters;

comparing said stored eye parameters to said current user eye parameters;

determining if said current user eye parameters match said stored eye parameters within a predetermined similarity threshold value.

8. A method as in claim 7 further comprising:

authenticating and unlocking said system if said current user eye parameters equal or exceed said predetermined similarity threshold value, and rejecting access otherwise.

9. A method as in claim 8 further comprising:

determining whether a second authentication criterion has been met;

keeping said system locked if said second authentication criterion has not been met.

10. A method as in claim 7 further comprising:

computing one or more said eye parameters during a calibration process.

11. A method as in claim 7 further comprising:

computing one or more said eye parameters while the system is being used.

12. A method as in claim 7 further comprising:

updating one or more said eye parameters are updated after a successful authentication of the user.

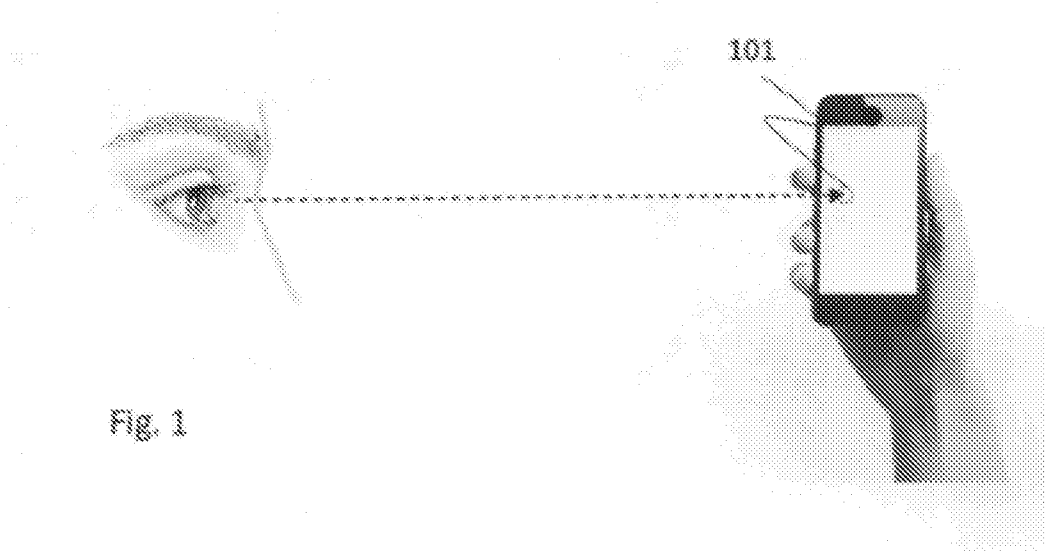


Fig. 1

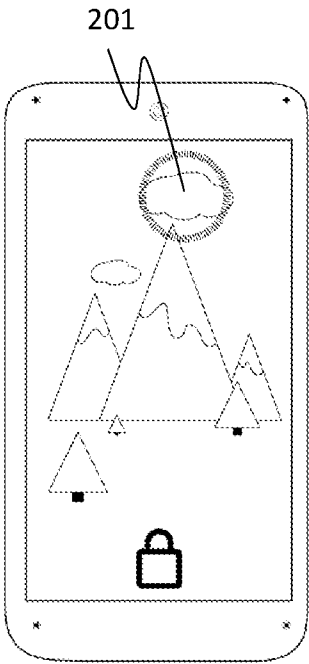


Fig. 2

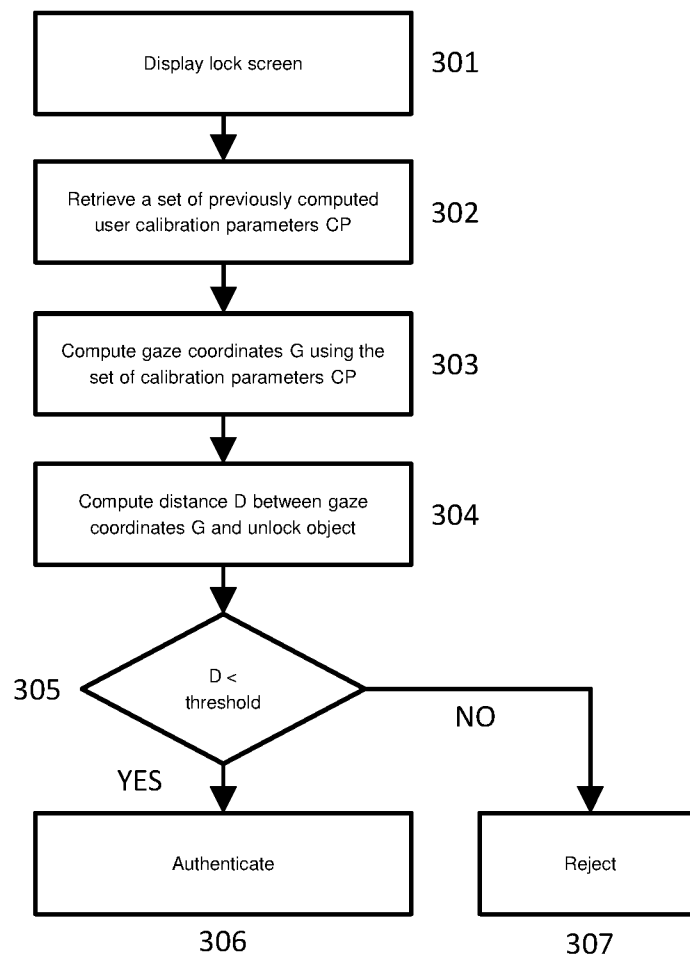


Fig. 3

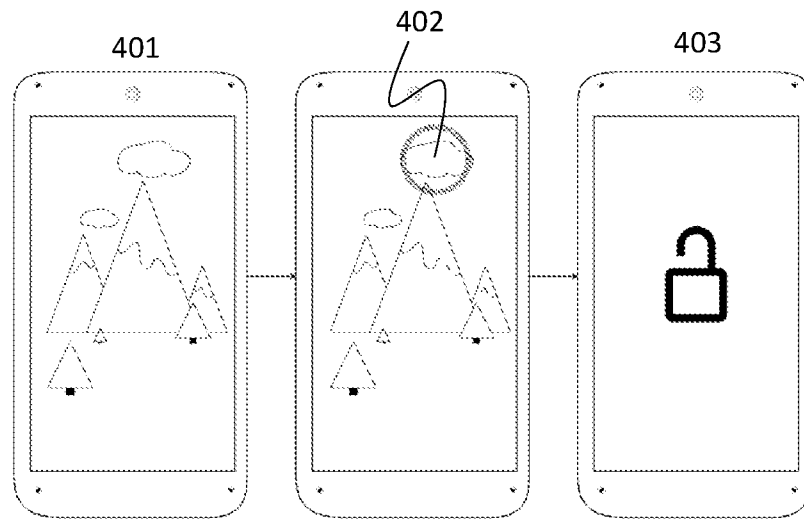


Fig. 4

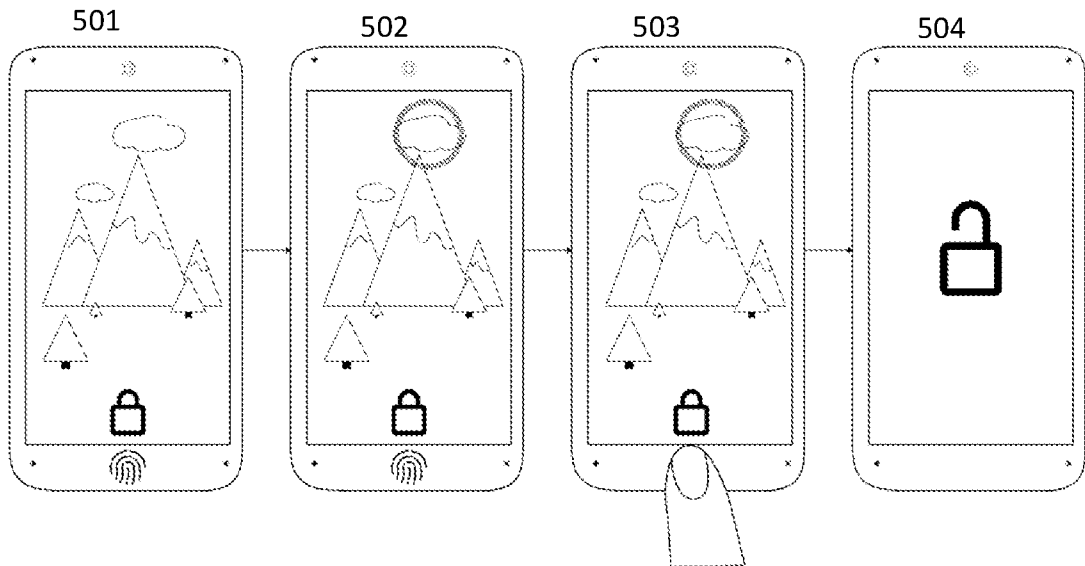


Fig. 5

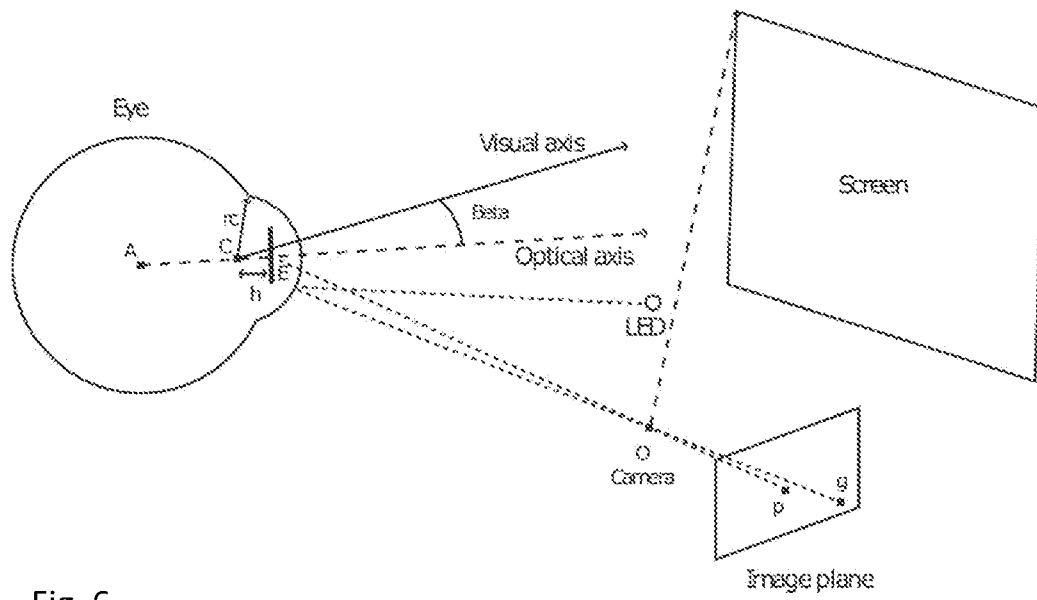


Fig. 6

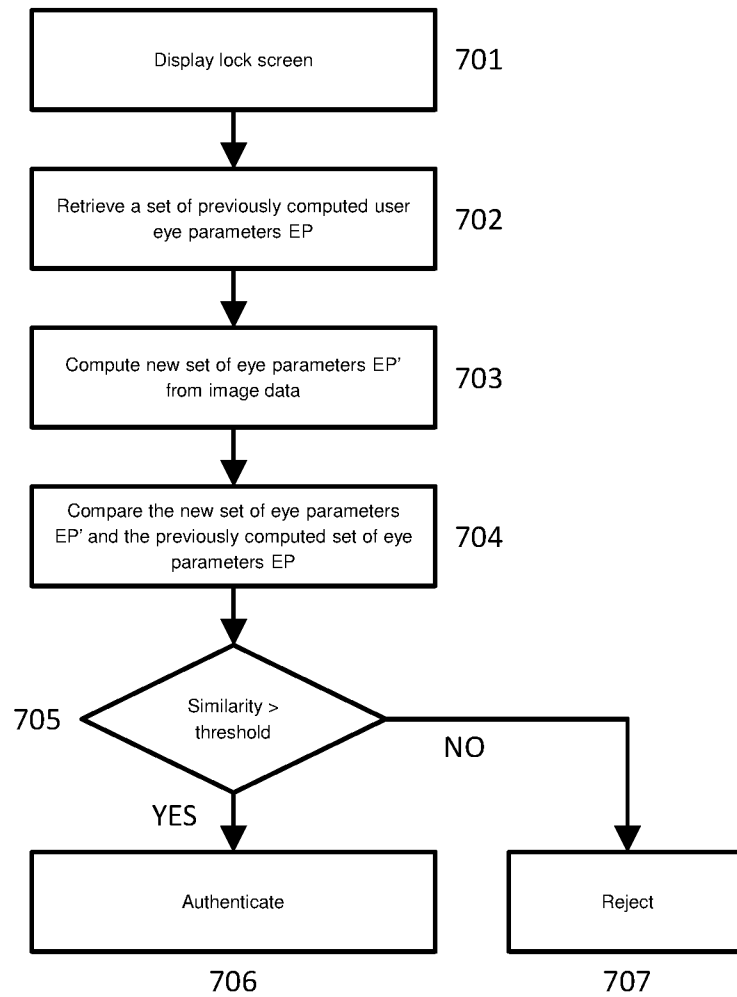


Fig. 7

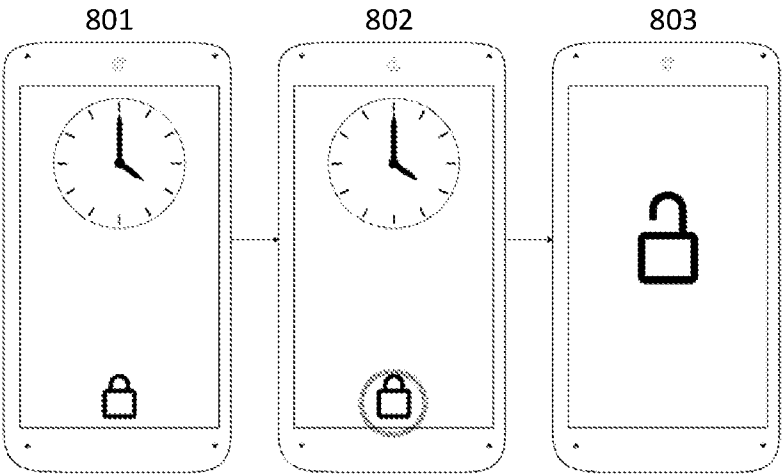


Fig. 8

INTERNATIONAL SEARCH REPORT

International application No
PCT/IB2016/001623

A. CLASSIFICATION OF SUBJECT MATTER
INV. G06F21/32
ADD. G06F3/01 G06K9/00

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 G06K

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

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	US 7 986 816 B1 (HOANCA BOGDAN [US] ET AL) 26 July 2011 (2011-07-26)	1-4,7-10
Y	column 7, line 20 - line 55 column 7, line 56 - column 10, line 35 column 14, line 55 - column 15, line 40; figures 1,2,5	5,6,11, 12
Y	----- US 8 594 374 B1 (BOZARTH BRADLEY J [US]) 26 November 2013 (2013-11-26)	5,6,11, 12
A	column 2, line 6 - column 5, line 61 column 7, line 31 - column 9, line 14 figures 1,2,3,7 ----- -/--	1-4,7-10

☒ Further documents are listed in the continuation of Box C.

☒ See patent family annex.

* Special categories of cited documents :

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

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

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

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

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

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

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

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

"&" document member of the same patent family

Date of the actual completion of the international search

3 February 2017

Date of mailing of the international search report

13/02/2017

Name and mailing address of the ISA/

European Patent Office, P.B. 5818 Patentlaan 2
NL - 2280 HV Rijswijk
Tel. (+31-70) 340-2040,
Fax: (+31-70) 340-3016

Authorized officer

Dingel, Janis

INTERNATIONAL SEARCH REPORT

International application No
PCT/IB2016/001623

C(Continuation). DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	US 2014/055591 A1 (KATZ SAGI [IL]) 27 February 2014 (2014-02-27)	1-4,7-10
A	paragraph [0017] - paragraph [0020] paragraph [0027] paragraph [0035] figures 1,2	5,6,11, 12
A	----- US 2012/016798 A1 (CARPER TODD ALAN [US]) 19 January 2012 (2012-01-19) paragraph [0054] - paragraph [0056] paragraph [0083] -----	1-12

INTERNATIONAL SEARCH REPORT

Information on patent family members

International application No

PCT/IB2016/001623

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
US 7986816	B1	26-07-2011	NONE
US 8594374	B1	26-11-2013	US 8594374 B1 26-11-2013 US 9280652 B1 08-03-2016
US 2014055591	A1	27-02-2014	US 2014055591 A1 27-02-2014 WO 2014030017 A1 27-02-2014
US 2012016798	A1	19-01-2012	US 2012016798 A1 19-01-2012 US 2014232526 A1 21-08-2014