



(51) International Patent Classification:

G06F 21/31 (2013.01) G06F 3/01 (2006.01)
G06F 1/16 (2006.01) H04L 9/32 (2006.01)

(21) International Application Number:

PCT/US2017/029394

(22) International Filing Date:

25 April 2017 (25.04.2017)

(25) Filing Language:

English

(26) Publication Language:

English

(30) Priority Data:

15/164,167 25 May 2016 (25.05.2016) US

(71) Applicant: INTEL CORPORATION [US/US]; 2200
Mission College Boulevard, Santa Clara, California 95054
(US).

(72) Inventor: JULIATO, Marcio; 15908 NW Linder Street,
Portland, Oregon 97229 (US).

(74) Agent: AUYEUNG, Al et al.; 1211 SW 5th Avenue, Suite
1500-1900, Portland, Oregon 97204 (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, 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, KH, 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.

(54) Title: WEARABLE COMPUTER APPARATUS WITH SAME HAND USER AUTHENTICATION

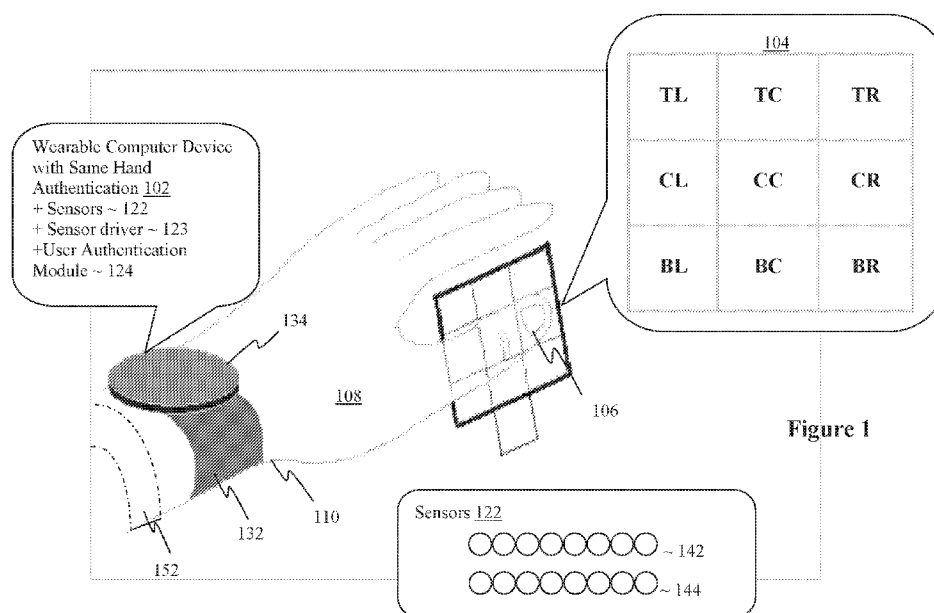


Figure 1

(57) Abstract: Apparatuses, methods and storage medium associated with same hand user authentication are disclosed herein. In embodiments, an apparatus, wearable on a user's wrist, may include a user authentication module to authenticate and grant access to the user. To authenticate the user, the user authentication module may be configured to receive sensor data indicative of movements of one or more fingers over a virtual grid, analyze the sensor data to determine the movements, and authenticate and grant the user access or deny the user access to the apparatus based at least in part on a result of the analysis. The one or more fingers are fingers of a hand of the user that adjoins the wrist on which the apparatus is worn. In embodiments, the sensor data may include sensor data collected by sensors configured to measure tendon/muscle positions of the wrist. Other embodiments may be disclosed or claimed.





(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, 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))*

Wearable Computer Apparatus with Same Hand User Authentication

Related Application

This application is claims priority to U.S. Application 15/164,167, entitled
5 “WEARABLE COMPUTER APPARATUS WITH SAME HAND USER
AUTHENTICATION,” filed May 25, 2016.

Technical Field

The present disclosure relates to the fields of computing. More
specifically, the present disclosure is related to same hand user authentication,
10 particularly suitable for wearable computer devices, such as smart watches,
smartphones, and so forth.

Background

The background description provided herein is for the purpose of generally
presenting the context of the disclosure. Unless otherwise indicated herein, the
15 materials described in this section are not prior art to the claims in this application
and are not admitted to be prior art by inclusion in this section.

With advances in integrated circuits and computing technology, wearable
computer devices, such as smart watches, are becoming increasingly popular. As
with all computer devices, especially with recent increase in interest in privacy and
20 data security, it is desirable or even necessary to authenticate a user before
allowing a user to access a wearable computer device.

Previously, most mobile computer devices, such as smart phones use
passwords, personal identification numbers (PIN) of 4 to 6 digits, or patterns traced
on a displayed 3x3 dot matrix. The disadvantage in porting and employing these
25 approaches on computer devices worn on the wrist, such as smart watches, is that
these approaches require a hand to touch the screen of the wearable computer
device to type in characters/numbers or form patterns. Necessarily, the hand
touching the screen has to be the other hand opposite to the wrist wearing the
computer device. Often times, the user's other hand may be busy, and thus require
30 extra effort of the user to authenticate himself/herself before the user is able to gain
access to the wearable computer device, and perform the desired function.

Brief Description of the Drawings

Embodiments will be readily understood by the following detailed

description in conjunction with the accompanying drawings. To facilitate this description, like reference numerals designate like structural elements. Embodiments are illustrated by way of example, and not by way of limitation, in the figures of the accompanying drawings.

5 Figure 1 illustrates a perspective view of a wearable computer device equipped with the same hand user authentication technology of the present disclosure, in accordance with various embodiments.

 Figures 2 and 3 illustrate two example sensor signal patterns for two example finger movements over a 3x3 virtual grid, in accordance with various
10 embodiments.

 Figure 4 illustrates possible finger movements across a 3x3 virtual grid, in accordance with alternate embodiments.

 Figure 5 illustrates example feedback by the wearable computer device, in accordance with various embodiments.

15 Figure 6 illustrates example architecture of the wearable computer device, in accordance with various embodiments.

 Figures 7 and 8 illustrate example operation flow/algorithmic architecture of the user authentication module, in accordance with various embodiments.

 Figures 9-11 illustrate an example 4x3 virtual grid suitable for pattern, PIN
20 or password authentication, in accordance with various embodiments.

Detailed Description

 Apparatuses, methods and storage medium associated with same hand user authentication are disclosed herein. In embodiments, an apparatus, wearable on a user's wrist, may include a processor with one or more processor cores, and a user
25 authentication module to be operated by the processor to authenticate and grant access to the user. To authenticate the user, the user authentication module may be configured to receive sensor data indicative of movements of one or more fingers over a virtual grid, analyze the sensor data to determine the movements, and authenticate and grant the user access or deny the user access to the apparatus
30 based at least in part on a result of the analysis. The one or more fingers are fingers of a hand of the user that adjoins the wrist on which the apparatus is worn, i.e. the same hand wearing the wearable computer device. In embodiments, the sensor data may include sensor data collected by sensors configured to measure

tendon/muscle positions of the wrist on which the apparatus is worn.

In the description to follow, reference is made to the accompanying drawings which form a part hereof wherein like numerals designate like parts throughout, and in which is shown by way of illustration embodiments that may be practiced. It is to be understood that other embodiments may be utilized and structural or logical changes may be made without departing from the scope of the present disclosure. Therefore, the following detailed description is not to be taken in a limiting sense, and the scope of embodiments is defined by the appended claims and their equivalents.

Operations of various methods may be described as multiple discrete actions or operations in turn, in a manner that is most helpful in understanding the claimed subject matter. However, the order of description should not be construed as to imply that these operations are necessarily order dependent. In particular, these operations may not be performed in the order of presentation. Operations described may be performed in a different order than the described embodiments. Various additional operations may be performed and/or described operations may be omitted, split or combined in additional embodiments.

For the purposes of the present disclosure, the phrase “A and/or B” means (A), (B), or (A and B). For the purposes of the present disclosure, the phrase “A, B, and/or C” means (A), (B), (C), (A and B), (A and C), (B and C), or (A, B and C).

The description may use the phrases “in an embodiment,” or “in embodiments,” which may each refer to one or more of the same or different embodiments. Furthermore, the terms “comprising,” “including,” “having,” and the like, as used with respect to embodiments of the present disclosure, are synonymous.

As used hereinafter, including the claims, the term “module” or “routine” may refer to, be part of, or include an Application Specific Integrated Circuit (ASIC), an electronic circuit, a processor (shared, dedicated, or group) and/or memory (shared, dedicated, or group) that execute one or more software or firmware programs, a combinational logic circuit, and/or other suitable components that provide the described functionality.

Referring now to Figure 1, wherein a perspective view of a wearable

computer device having the same hand user authentication technology of the present disclosure, in accordance with various embodiments, is illustrated. As shown, in the illustrated embodiments, a user wearing a computer device 102, such as a smart watch or a smartphone, equipped with the same hand user authentication technology of the present disclosure, may authenticate himself/herself and gain access to wearable computer device 102, by moving a finger 106 over a virtual grid 104 forming a pattern that corresponds to or matches an access control reference pattern. As depicted, finger 106 may be a finger of the same hand 108 adjoining wrist 110, on which computer device 102 is worn. And virtual grid 104 may be an imaginary grid in free space. Accordingly, the user may authenticate himself/herself and gain access to computer device 102 (to perform a function) in a single handed or same hand manner, without the need of using the other hand.

In embodiments, as depicted in the callout on the left side of Figure 1, wearable computer device 102 may include a number of sensors 122, sensor driver 123, and a user authentication module 124, configured to cooperate with each other to provide the single-handed or same hand user authentication capabilities. More specifically, sensors 122 may be configured to continuously sense the positions of tendons and muscles around wrist 110, wherein computer device 102 is worn, and continuously output signals representative of the positions sensed. Sensor driver 123 may be configured to process the signals, and continuously output sensor data indicative of successive positions sensed. User authentication module 124 may in turn receive these sensor data, and analyze the sensor data to determine movements of user finger 106 over virtual grid 104 and the pattern formed by the movements. Note that finger 106 is of the same hand adjoining wrist 110 where computer device 102 is worn. Further, user authentication module 124 may determine whether the pattern formed corresponds to or matches with an access control reference pattern, and authenticate and grant the user access to computer device 102, or deny access, based at least in part on the a result of the analysis against the access control reference pattern.

In embodiments, as illustrated by the insert at the lower center portion of Figure 1, sensors 122 may comprise of two strips or rows of pressure sensors 142 and 144. Sensors 142 may be configured to continuously sense positions of tendons/muscles at wrist 110 through the upper (or anterior) surface of wrist 110

and output corresponding signals, whereas sensors 144 may be configured to sense positions of tendons/muscles at wrist 110 through the under (or posterior) surface of wrist 110 and output corresponding signals. Sensor driver 123 processes and combines both sets of signals to output sensor data indicative of the positions of the tendons/muscles at wrist 110. User authentication module 124 in turn processes the sensor data to determine the position and movement of finger 106 over virtual grid 104. In embodiments, user authentication module 124 may be configured to determine the position and movement of finger 106 over virtual grid 104, using a set of reference sensor data patterns for various movements over virtual grid 104. The sensing of positions of tendons/muscles through the upper (or anterior) and the under (or posterior) surfaces, and usage of such sensed signals to determine finger and/or hand position are described further in U.S. Patent Application 15/087,385, filed March 31, 2016, entitled "Sensor Signal Processing to Determine Finger and/or Hand Position"; and in PCT Patent Application PCT/US2015/067534, filed Dec 22, 2015, entitled "System and Method to Collect Gesture Input Through Wrist Tendon and Muscle Sensing". The Specifications of USPA 15/087,385 and PCT/US2015/067534 are fully incorporated herein by reference.

In embodiments where computer device 102 is a smart watch having main body 134 housing the electronics, and band 132 coupled to main body 134 at two opposite sides/ends of main body 134, sensors 142 may be disposed at a bottom surface of main body 134 that touches the upper (or anterior) surface of wrist 110, and sensors 144 may be disposed at a portion of band 132 that touches the under (or posterior) surface of wrist 110. In alternate embodiments, where computer device 102 is a smart watch having main body 134 housing the electronics, and band 132 coupled to main body 134, passing through and covering (at least partially) the underside of main body 134, sensors 142 may be disposed at a portion of band 132 that touches the upper (or anterior) surface of wrist 110, and sensors 144 may be disposed at a portion of band 132 that touches the posterior (or under) surface of wrist 110. In still other embodiments, regardless whether computer device 102 is a smart watch or other wearable computer devices, sensors 142 may be disposed at the internal portion of external band 152 (that is not part of computer device 102) that touches the upper (or anterior) surface of wrist 110, and

sensors 144 may be disposed at the internal portion of external band 152 that touches the posterior (or under) surface of wrist 110.

In embodiments, as depicted by the callout in the upper right corner of Figure 1, virtual grid 104 may be a 3x3 virtual grid, which may comprise 9 cells organized into 3 rows and 3 columns. The 9 cells may be referred to as the top left (TL) cell, top center (TC) cell, top right (TR) cell, center left (CL) cell, center (CC) cell, center right (CR) cell, bottom left (BL) cell, bottom center (BC) cell, and bottom right (BR) cell. In alternate embodiments, other nomenclature may be used instead.

Referring now also to Figures 2 and 3, wherein two example sensor signal patterns for two example movement patterns over the 3x3 virtual grid, in accordance with various embodiments, are shown. More specifically, Figure 2 illustrates an example signal pattern 200 when thumb 106 is first placed at cell CL, traverse along the CL-CC-CR row to cell CC, then cell CR. Each line in Figure 2 depicts the signal level of a corresponding sensor as thumb 106 moves from cell CL, along the CL-CC-CR row to cell CC, then cell CR. Figure 3 illustrates an example signal pattern when thumb 106 is first placed at cell TC, traverse along the TC-CC-BC column to cell CC, then cell BC. Similarly, each line in Figure 3 depicts the signal level of a corresponding sensor as thumb 106 moves from cell TC, along the TC-CC-BC column to cell CC, then cell BC.

Figure 4 illustrates possible finger movements across the 3x3 virtual grid, in accordance with various embodiments. As illustrated in the left portion 402 of Figure 4, a user may also move finger 106 vertically, up and down any one of the columns of virtual grid 104, or horizontally, back and forth across any one of the rows of virtual grid 104. As illustrated in the center and right portions 404 and 406 of Figure 4, a user may move finger 106 diagonally in any one of a number of angular manners across the various cells of virtual grid 104. In embodiments, during traversal of the 3x3 virtual grid, a cell within the 3x3 virtual grid may be selected with a pre-determined finger movement, while the finger is positioned over the cell. For example, in embodiments where the 3x3 virtual grid is traversed using the thumb, selection of a cell may be indicated by moving the thumb towards the palm while the thumb is positioned over the cell.

Referring back to Figure 1, in embodiments, user authentication module

124 may be configured to support a configuration mode and an operation mode.

The configuration mode may have various configuration points or periods, where different aspects of the single handed/same hand authentication technology of the present disclosure may be configured/defined. In embodiments, these

5 configuration points or periods may include a point where finger 106 to be used to perform the pattern traversal may be selected/identified, and a first period where the free space occupied by virtual grid 102 (and its cells) may be defined. Further, these configuration points or periods may include a second period where the signal patterns for various movements of finger 106 over virtual grid 102 may be
10 recorded, and a third period where the reference pattern to be used to control access to computer device 102 may be defined.

In embodiments, at the finger selection/identification point in the configuration process, finger 106 to be used to perform the pattern traversal may be selected/identified through movement of one of the fingers. For example, a user
15 may move the finger he/she wants to use to traverse virtual grid 104, in response to a prompt from user authentication module 122. During the virtual grid definition period of the configuration process, the free space occupied by virtual grid 102 may be defined through movement of the selected/identified finger 106. For example, a user may use the selected/identified finger 106 to trace the perimeter of
20 virtual grid 102, in response to a prompt from user authentication module 122. Further, the number of cells within the virtual grid may be defined. For example, a user may enter (type in, via voice command, or select from pre-selected options) the configuration or the number of cells, or use the selected/identified finger 106 to partition virtual grid 102, in response to a prompt from user authentication module
25 122. And the free space occupied by the cells may be computed from the free space defined for virtual grid 104. For example, for a 3x3 virtual grid, the free space occupied by the cells may be computed by dividing the free space defined for virtual grid 104 into 9 equal portions in a 3x3 configuration.

Likewise, during the signal pattern recording period of the configuration
30 process, the signal patterns for various movements of finger 106 may be captured. For example, a user may use the selected/identified finger 106 to move vertically, horizontally or diagonally across virtual grid 104, in response to various prompts by user authentication module 124. During the reference pattern definition period

of the configuration process, the reference pattern to be used to control access to computer device 102 may be defined through movement of the selected/identified finger 106 over virtual grid 104. For example, a user may use the selected/identified finger 106 to traverse virtual grid 102, in response to a prompt
5 from user authentication module 122.

In embodiments, the different configuration point/periods to select/identify finger 106, define virtual grid 104, record the signal patterns, or define the reference pattern may be consecutive, with the selection/identification and recording/definitions being performed successive, or may be entered independently
10 to allow any of these selection/identification, recordings and definitions to be performed and/or repeated (e.g., periodic changing the access control reference pattern).

In embodiments, the identification of finger 106, the free space definition of virtual grid 104, the movement signal patterns recorded, and the access control reference pattern defined may be stored locally in wearable computer device 102.
15 Alternatively the identification of finger 106, the free space definition of virtual grid 104, the movement signal patterns recorded, and/or the access control reference pattern defined may be stored in a cloud server (not shown), accessible to wearable computer device 102, e.g., through wireless communication.

In alternate embodiments, other approaches may be employed to select/identify finger 106, define virtual grid 104, capture signal patterns for various finger movements, and/or define the access control reference pattern. The particular embodiments described should not be construed as limiting on the single
20 handed/same hand user authentication technology of the present disclosure.

Additionally, it should be noted that while a 3x3 virtual grid and usage of the thumb as the traversing figure are depicted in Figure 1, in alternate embodiments, virtual grid of other configurations, e.g., 4x3 virtual grid, and other fingers, such as the index finger, the middle finger, the ring finger, the baby finger, or usage of multiple fingers may be practiced instead. Further,
25 while a smart watch with two stripes/rows of sensors are depicted in Figure 1, in alternate embodiments, other wearable computer device and/or other configuration of sensor dispositions may be practiced instead. Still further, for smart watch embodiments, while a smart watch with a round main
30

body/housing is illustrated, in alternate embodiments, the main body/housing of smart watch may have other shapes, e.g. a rectangular shape. Again, these illustrative embodiments should not be construed as limiting on the single handed/same hand user authentication technology of the present disclosure.

5 In embodiments, user authentication module 124 may also be configured to provide feedback to the user, as the user endeavors to use finger 106 to traverse virtual grid 104 with movements to form a pattern that corresponds or matches an access control reference pattern, to authenticate himself/herself to gain access to wearable computer device 102. Figure 5 illustrates example feedback by a
10 wearable computer device, in accordance with various embodiments. As shown, in response to a particular predetermined movement of hand 108 or finger 106 that signal the user's desire to authenticate himself/herself to gain access, wearable computer device 102 may wake up from an idle or sleep state, enter the operation mode, and render display 500 that graphically or pictorially represents virtual grid
15 104. As the user moves finger 106 to form a pattern that corresponds or matches the access control reference pattern, the movement path 502, as interpreted/determined by user authentication module 124 may also be displayed for the user. Accordingly, the user may be aided in his/her endeavor to provide the corresponding/matching pattern to gain access. In embodiments, similar visual
20 feedbacks may be provided to the user during the configuration mode, for recording the signal patterns of various finger movements and/or for inputting the access control reference pattern.

Referring now to Figure 6, wherein example architecture of a wearable computer device having the single handed/same hand technology of the present disclosure,
25 according to various embodiments, is shown. As illustrated, in embodiments, wearable computer device 600 (which may be wearable computer device 102) may include hardware 602 and software 604. Software 604 may include operating system (OS) 634 and application 632. OS 634 may include user authentication module 644 and sensor driver 643, which may correspond to the earlier described user authentication module 144
30 and sensor driver 143. OS 634, except for user authentication module 644 and sensor driver 643, may be any one of a number of wearable computer device OS known in art. Alternatively to an OS, user authentication module 644 can conceived as a firmware or any other kind of embedded software dedicated to perform dedicated tasks. Applications

632 may likewise be any one of a number of known applications for wearable computer devices, e.g., personal health application, calendar or other personal information management (PIM) applications.

Hardware 602 may include processor(s) 612, memory 614, persistent storage 616, sensors 618, display 620, and communication interface 622. Processor(s) 612 may be any one of a number of processors known in the art, each having one or more processor cores. Memory 614 may be any known volatile or non-volatile memory in the art, suitable for storing instructions for execution and working data, in particular, instructions and data of applications 632 and OS 634, including user authentication module 644 and sensor driver 643. Memory 614 may include a hierarchy of cache memory and system memory. Both the cache and system memory may be respectively organized into segments and pages. Persistent storage 616 may be any known persistent mass storage suitable for providing persistent storage of instructions and data of applications 632 and OS 634, e.g., solid state storage, magnetic or optical disk drives. Sensors 618 may include the earlier described sensors 142 and 144 for sensing position of tendons/muscles. Display 620 may be any known display device, including e.g., touch sensitive screen. Communication interface 622 may include any number of wireless communication or networking interfaces known, such as WiFi, 3G/4G, Bluetooth®, Near Field Communication, LiFi, and so forth.

Referring now to Figures 7 and 8, wherein example operation flow/algorithmic structure of the user authentication module, according the various embodiments, is shown. As illustrated in Figure 7, in embodiments, user authentication module 144/642 may be configured with operating flow/algorithmic structure 700 for configuring various aspects of the single handed/same hand user authentication technology. Operating flow/algorithmic structure 700 may begin at/with block 702. At block 702, the finger to be used to traverse the virtual grid to provide the access control authentication may be selected/identified. As described earlier, a prompt may be made of the user to move the finger to be used to traverse the virtual grid to provide the access control pattern.

Next at block 704, the virtual grid may be defined. As described earlier, a prompt may be made of the user to move the finger to trace the free space to define the perimeter of the virtual grid. Further, a prompt may be made of the user to identify the configuration or cells of the virtual grid.

Next at block 706, on definition of the virtual grid, the sensor signal patterns of the various finger movement patterns over the virtual grid may be recorded. As described

earlier, a number of prompts may be made of the user to move the finger horizontally across various rows, vertically up and down various columns, and diagonally/angularly across various cells of the virtual grid.

Then, at block 708, the access control reference pattern may be defined. As
5 described earlier, a prompt may be made of the user to move the finger over the virtual grid to define the access control reference pattern.

As illustrated in Figure 8, in embodiments, user authentication module 144/642 may be configured with operating flow/algorithmic structure 800 for authenticating and granting access to the wearable computer device to a user or denying access to the
10 wearable computer device to the user. Operating flow/algorithmic structure 800 may begin at/with block 802. At block 802, on entry into an operational mode (from an idle/sleep state), a graphical representation of the virtual grid may be displayed.

Next at block 804, sensor data indicative of positions of tendons/muscles of the wrist on which the computer device is worn, may be received and analyzed to determine
15 the finger position over the virtual grid. At block 806, on determination of the current finger position over the virtual grid, visual feedback on the movement path may be provided.

At block 808, a determination may be made on whether the movement path provided thus far corresponds or matches the access control reference pattern. If a result
20 of the determination indicates that the movement path provided thus far corresponds or matches the access control reference pattern, operation/algorithm flow 800 may proceed to block 810. At block 810, the user may be authenticated, and access to the wearable computer device granted.

If a result of the determination indicates that the movement path provided thus far
25 does not correspond or match the access control reference pattern, and the number of cells touched is below the number of cells needed to provide the corresponding or matching access control pattern, operation/algorithm flow 800 may return to block 804 and continue there from for additional sensor data.

If a result of the determination indicates that the movement path provided thus far
30 does not correspond or match the access control reference pattern, and the number of cells touched has reached the number of cells needed to provide the corresponding or matching access control pattern, operation/algorithm flow 800 may proceed to block 812. At block 812, visual feedback, such as an error message and/or an alarm, may be provided to

convey authentication failure, and access to the wearable computer device denied.

As alluded to earlier, while for ease of understanding, the single handed/same hand user authentication technology has been described in the context of a 3x3 virtual grid thus far. In alternate embodiments, different grid configurations and/or personal identification number (PIN) or password (as
 5 opposed to patterns) may be practiced to authenticate and grant access to the user. Figures 9-11 illustrate an example 4x3 virtual grid suitable for PIN or password authentication, in accordance with various embodiments. As shown in Figure 9, 4x3 virtual grid 900 may comprise 4 rows and 3 columns. In embodiments, the
 10 cells of the top three rows may be similarly referred to as TL, TC, TR, CL, CC, CR, BL, BC and BR as before. The cells of the 4th row may be respectively referred to as cell AL, AC and AR.

In embodiments, user authentication module 144/644 may interpret the 12 cells as a 12-keys numeric keypad 1000 (Figure 10), with cells TL, TC and TR
 15 correspond to the numbers 1, 2 and 3; cells CL, CC and CR correspond to the numbers 4, 5, and 6; cells BL, BC and BR correspond to the numbers 7, 8 and 9, and cell AC corresponds to the number 0. Further, cells AL and AR may respectively correspond to special keys Backspace or asterisk (*), and Enter or #.

In embodiments, user authentication module 144/644 may support multi-
 20 tap allowing the 12 cells to be interpreted as 12-keys alphanumeric keypad 1100 (Figure 11). For example, a single tap of cell TC may correspond to the letter "A," two taps may correspond to the letter "B," three taps may correspond to the letter "C," and so forth. Accordingly, cells TC and TR may respectively correspond to letters "ABC" and "DEF," cells CL, CC and CR may respectively correspond to
 25 letters "GHI," "JKL," and "MNO," cells BL, BC and BR may respectively correspond to letters "PQR," "STU," and "WXYZ."

Thus, for these embodiments, during operation, similar to block 808 of Figure 8, a determination may be made on whether the movement path provided thus far corresponds or matches an access PIN or password. If a result of the
 30 determination indicates that the movement path provided thus far corresponds or matches the access PIN or password, the user may be authenticated, and access to the wearable computer device granted. On the other hand, if a result of the determination indicates that the movement path provided thus far does not

correspond or match the access PIN or password, and the number of cells touched is below the number of cells needed to provide the corresponding or matching PIN or password, additional sensor data may be collected. However, if a result of the determination indicates that the movement path provided thus far does not
5 correspond or match the access PIN or password, and the number of cells touched has reached the number of cells needed to provide the corresponding or matching access PIN or password, visual feedback, such as an error message and/or an alarm, may be provided to convey authentication failure, and access to the wearable computer device denied.

10 Further, similar to the access pattern embodiments, user authentication module 144/644 may provide visual feedback similar to the graphical representation illustrated in Figure 5, as the various keys are touched or tapped to provide the access control PIN or password.

Referring back to Figure 6, in one embodiment, at least one of processors
15 612 may be packaged together with a computer-readable storage medium having sensor driver 643 and/or user authentication module 644 (in lieu of storage in memory 614 and/or storage 616). For one embodiment, at least one of processors 612 may be packaged together with a computer-readable storage medium having sensor driver 643 and/or user authentication module 644 to form a System in
20 Package (SiP). For one embodiment, at least one of processors 612 may be integrated on the same die with a computer-readable storage medium having sensor driver 643 and/or user authentication module 644. For one embodiment, at least one of processors 612 may be packaged together with a computer-readable storage medium having sensor driver 643 and/or user authentication module 644 to form a
25 System on Chip (SoC).

Thus, example embodiments described may include:

Example 1 may be an apparatus for computing, comprising: a processor having one or more processor cores; and a user authentication module to be operated by the processor to authenticate and grant access to a user of the apparatus. The apparatus may be wearable
30 on a user's wrist. To authenticate the user, the user authentication module may be configured to receive sensor data indicative of movements of one or more fingers over a virtual grid, analyze the sensor data to determine the movements, and authenticate and grant the user access or deny the user access to the apparatus based at least in part on a

result of the analysis. The one or more fingers are fingers of a hand of the user that adjoins the wrist on which the apparatus is worn.

Example 2 may be example 1, wherein the virtual grid may comprise a 3x3 virtual grid, and the user authentication module may be configured to authenticate and grant
5 access to the user in response to a determination of the movements over the virtual grid matching a reference pattern.

Example 3 may be example 1, wherein the virtual grid may comprise a 4x3 virtual keypad, and the user authentication module may be configured to authenticate and grant
10 access to the user in response to a determination of the movements over the virtual grid matching a reference pattern, a personal information number (PIN) or a password.

Example 4 may be example 1, wherein the one or more fingers may comprise a thumb of the hand of the user that adjoins the wrist on which the apparatus is worn.

Example 5 may be example 1, further comprising a sensor driver to be operated by the processor to receive sensor signals representative of tendon or muscle positions of the
15 wrist, and process the sensor signals to output the sensor data for the user authentication module.

Example 6 may be example 5, wherein the apparatus may further comprise a plurality of sensors coupled to the processor to sense and output the sensor signals representative of the tendon or muscle positions of the wrist.

20 Example 7 may be example 6, wherein the apparatus may be a smart watch having a watch band, and the plurality of sensors may be disposed on the watch band.

Example 8 may be example 5, wherein the apparatus may further comprise a communication interface to receive sensor signals from an external wrist band having a plurality of sensors to sense and output the sensor signals representative of the tendon or
25 muscle positions of the wrist, and process the sensor signals into the sensor data; wherein the external wrist band is not part of the apparatus.

Example 9 may be any one of examples 1-8, wherein the user authentication module may be configured to further provide visual feedbacks to the user to assist the user in traversing the virtual grid.

30 Example 10 may be example 9, wherein to provide visual feedbacks may comprise to display a graphical representation of the virtual grid, including indicators indicating portions of the virtual grid traversed.

Example 11 may be a method for computing, comprising: receiving, by a wearable computer device, sensor data indicative of movements of one or more fingers of a user of the wearable computer device over a virtual grid; analyzing, by the wearable computer device, the sensor data to determine the movements; and authenticating and granting the user access or denying the user access to the wearable computer device, based at least in part on a result of the analysis. The one or more fingers are fingers of a hand of the user that adjoins the wrist on which the wearable computer device is worn.

Example 12 may be example 11, wherein the virtual grid may comprise a 3x3 virtual grid, and authenticating and granting access may comprise authenticating and granting access to the user in response to a determination of the movements over the virtual grid matching a reference pattern.

Example 13 may be example 11, wherein the virtual grid may comprise a 4x3 virtual keypad, authenticating and granting access may comprise authenticating and granting access to the user in response to a determination of the movements over the virtual grid matching a reference pattern, a personal information number (PIN) or a password.

Example 14 may be example 11, wherein the one or more fingers may comprise a thumb of the hand of the user that adjoins the wrist on which the apparatus is worn.

Example 15 may be example 11, wherein receiving may comprise receiving sensor signals representative of tendon or muscle positions of the wrist, and processing the sensor signals to output the sensor data.

Example 16 may be example 15, further comprising sensing and outputting the sensor signals representative of the tendon or muscle positions of the wrist.

Example 17 may be example 16, wherein the wearable computer device may be a smart watch having a watch band, and the plurality of sensors may be disposed on the watch band.

Example 18 may be example 15, wherein receiving may comprise receiving sensor signals from an external wrist band having a plurality of sensors to sense and output the sensor signals representative of the tendon or muscle positions of the wrist, and processing the sensor signals into the sensor data; wherein the external wrist band is not part of the apparatus.

Example 19 may be any one of examples 11-18, further comprising providing, by the wearable computer device, visual feedbacks to the user to assist the user in traversing the virtual grid.

Example 20 may be example 19, wherein providing visual feedbacks may
5 comprise displaying a graphical representation of the virtual grid, including indicators indicating portions of the virtual grid traversed.

Example 21 may be one or more computer-readable media comprising instructions that cause a computer device, in response to execution of the instructions by one or more processor cores of the computer device, to provide a user authentication module to
10 authenticate and grant access to a user of the apparatus; wherein the apparatus is wearable on a user's wrist; wherein to authenticate the user, the user authentication module may be configured to receive sensor data indicative of movements of one or more fingers over a virtual grid, analyze the sensor data to determine the movements, and authenticate and grant the user access or deny the user access to the computer device based at least in part
15 on a result of the analysis; and wherein the one or more fingers are fingers of a hand of the user that adjoins the wrist on which the apparatus is worn.

Example 22 may be example 21, wherein the virtual grid may comprise a 3x3 virtual grid, and the user authentication module may be configured to authenticate and grant access to the user in response to a determination of the movements over the virtual
20 grid matching a reference pattern.

Example 23 may be example 21, wherein the virtual grid may comprise a 4x3 virtual keypad, and the user authentication module may be configured to authenticate and grant access to the user in response to a determination of the movements over the virtual grid matching a reference pattern, a personal information number (PIN) or a password.
25

Example 24 may be example 21, wherein the one or more fingers may comprise a thumb of the hand of the user that adjoins the wrist on which the apparatus is worn.

Example 25 may be example 21, further comprising a sensor driver to be operated by the processor to receive sensor signals representative of tendon or muscle positions of the wrist, and process the sensor signals to output the sensor data for the user
30 authentication module.

Example 26 may be example 25, wherein the computer device may further comprise a plurality of sensors coupled to the processor cores to sense and output the sensor signals representative of the tendon or muscle positions of the wrist.

Example 27 may be example 26, wherein the computer device is a smart watch having a watch band, and the plurality of sensors may be disposed on the watch band.

Example 28 may be example 25, wherein the computer device may further comprise a communication interface to receive sensor signals from an external wrist band
5 having a plurality of sensors to sense and output the sensor signals representative of the tendon or muscle positions of the wrist, and process the sensor signals into the sensor data; wherein the external wrist band is not part of the apparatus.

Example 29 may be any one of examples 21-28, wherein the user authentication module may be configured to further provide visual feedbacks to the user to assist the user
10 in traversing the virtual grid.

Example 30 may be example 29, wherein to provide visual feedbacks may comprise to display a graphical representation of the virtual grid, including indicators indicating portions of the virtual grid traversed.

Example 31 may be a wearable apparatus for computing, comprising: means for
15 receiving sensor data indicative of movements of one or more fingers of a user of the wearable apparatus over a virtual grid; means for analyzing the sensor data to determine the movements; and means for authenticating and granting the user access or denying the user access to the wearable apparatus, based at least in part on a result of the analysis; and wherein the one or more fingers are fingers of a hand of the user that adjoins the wrist on
20 which the wearable computer device is worn.

Example 32 may be example 31, wherein the virtual grid may comprise a 3x3 virtual grid, and means for authenticating and granting access may comprise means for authenticating and granting access to the user in response to a determination of the movements over the virtual grid matching a reference pattern.

Example 33 may be example 31, wherein the virtual grid may comprise a 4x3
25 virtual keypad, and means for authenticating and granting access may comprise means for authenticating and granting access to the user in response to a determination of the movements over the virtual grid matching a reference pattern, a personal information number (PIN) or a password.

Example 34 may be example 31, wherein the one or more fingers comprise a
30 thumb of the hand of the user that adjoins the wrist on which the wearable apparatus is worn.

Example 35 may be example 31, wherein means for receiving may comprise means for receiving sensor signals representative of tendon or muscle positions of the wrist, and means for processing the sensor signals to output the sensor data.

Example 36 may be example 35, may further comprise means for sensing and
5 outputting the sensor signals representative of the tendon or muscle positions of the wrist.

Example 37 may be example 36, wherein the wearable computer device may be a smart watch having a watch band, and the means for sensing may comprise a plurality of sensors disposed on the watch band.

Example 38 may be example 35, wherein means for receiving sensor signals may
10 comprise means for receiving sensor signals from an external wrist band having a plurality of sensors to sense and output the sensor signals representative of the tendon or muscle positions of the wrist, and processing the sensor signals into the sensor data; wherein the external wrist band is not part of the wearable apparatus.

Example 39 may be any one of examples 31-38, further comprising means for
15 providing visual feedbacks to the user to assist the user in traversing the virtual grid.

Example 40 may be example 39, wherein means for providing visual feedbacks may comprise means for displaying a graphical representation of the virtual grid, including indicators indicating portions of the virtual grid traversed.

Although certain embodiments have been illustrated and described herein
20 for purposes of description, a wide variety of alternate and/or equivalent embodiments or implementations calculated to achieve the same purposes may be substituted for the embodiments shown and described without departing from the scope of the present disclosure. This application is intended to cover any adaptations or variations of the embodiments discussed herein. Therefore, it is
25 manifestly intended that embodiments described herein be limited only by the claims.

Where the disclosure recites “a” or “a first” element or the equivalent thereof, such disclosure includes one or more such elements, neither requiring nor excluding two or more such elements. Further, ordinal indicators (e.g., first, second
30 or third) for identified elements are used to distinguish between the elements, and do not indicate or imply a required or limited number of such elements, nor do they indicate a particular position or order of such elements unless otherwise specifically stated.

Claims

What is claimed is:

1. An apparatus for computing, comprising:
a processor having one or more processor cores; and
5 a user authentication module to be operated by the processor to authenticate and grant access to a user of the apparatus;
wherein the apparatus is wearable on a user's wrist;
wherein to authenticate the user, the user authentication module is to receive sensor data indicative of movements of one or more fingers over a virtual
10 grid, analyze the sensor data to determine the movements, and authenticate and grant the user access or deny the user access to the apparatus based at least in part on a result of the analysis; and
wherein the one or more fingers are fingers of a hand of the user that adjoins the wrist on which the apparatus is worn.
- 15 2. The apparatus of claim 1, wherein the virtual grid comprises a 3x3 virtual grid, and the user authentication module is to authenticate and grant access to the user in response to a determination of the movements over the virtual grid matching a reference pattern.
- 20 3. The apparatus of claim 1, wherein the virtual grid comprises a 4x3 virtual keypad, and the user authentication module is to authenticate and grant access to the user in response to a determination of the movements over the virtual grid matching a reference pattern, a personal information number (PIN) or a password.
4. The apparatus of claim 1, wherein the one or more fingers comprise a thumb of the hand of the user that adjoins the wrist on which the apparatus is worn.
- 25 5. The apparatus of claim 1, further comprising a sensor driver to be operated by the processor to receive sensor signals representative of tendon or muscle positions of the wrist, and process the sensor signals to output the sensor data for the user authentication module.

6. The apparatus of claim 5, wherein the apparatus further comprises a plurality of sensors coupled to the processor to sense and output the sensor signals representative of the tendon or muscle positions of the wrist.

7. The apparatus of claim 6, wherein the apparatus is a smart watch having a watch band, and the plurality of sensors are disposed on the watch band.

8. The apparatus of claim 5, wherein the apparatus further comprises a communication interface to receive sensor signals from an external wrist band having a plurality of sensors to sense and output the sensor signals representative of the tendon or muscle positions of the wrist, and process the sensor signals into the sensor data; wherein the external wrist band is not part of the apparatus.

9. The apparatus of any one of claims 1-8, wherein the user authentication module is to further provide visual feedbacks to the user to assist the user in traversing the virtual grid.

10. The apparatus of claim 9, wherein to provide visual feedbacks comprises to display a graphical representation of the virtual grid, including indicators indicating portions of the virtual grid traversed.

11. A method for computing, comprising:
receiving, by a wearable computer device, sensor data indicative of movements of one or more fingers of a user of the wearable computer device over a virtual grid;
analyzing, by the wearable computer device, the sensor data to determine the movements; and
authenticating and granting the user access or denying the user access to the wearable computer device, based at least in part on a result of the analysis; and
wherein the one or more fingers are fingers of a hand of the user that adjoins the wrist on which the wearable computer device is worn.

12. The method of claim 11, wherein the virtual grid comprises a 3x3 virtual grid, and authenticating and granting access comprises authenticating and granting access to the user in response to a determination of the movements over the virtual grid matching a reference pattern.

13. The method of claim 11, wherein the virtual grid comprises a 4x3 virtual keypad, authenticating and granting access comprises authenticating and granting access to the user in response to a determination of the movements over the virtual grid matching a reference pattern, a personal information number (PIN) or a password.

5 14. The method of claim 11, wherein the one or more fingers comprise a thumb of the hand of the user that adjoins the wrist on which the apparatus is worn.

15. The method of claim 11, wherein receiving comprises receiving sensor signals representative of tendon or muscle positions of the wrist, and processing the sensor signals to output the sensor data.

10 16. The method of claim 11, further comprising providing, by the wearable computer device, visual feedbacks to the user to assist the user in traversing the virtual grid; wherein providing visual feedbacks comprises displaying a graphical representation of the virtual grid, including indicators indicating portions of the virtual grid traversed.

15 17. One or more computer-readable media comprising instructions that cause a computer device, in response to execution of the instructions by one or more processor cores of the computer device, to provide a user authentication module to practice any one of the methods of claims 11-16.

18. A wearable apparatus for computing, comprising:
means for receiving sensor data indicative of movements of one or more
20 fingers of a user of the wearable apparatus over a virtual grid;
means for analyzing the sensor data to determine the movements; and
means for authenticating and granting the user access or denying the user access to the wearable apparatus, based at least in part on a result of the analysis;
and

25 wherein the one or more fingers are fingers of a hand of the user that adjoins the wrist on which the wearable computer device is worn.

19. The wearable apparatus of claim 18, wherein the virtual grid comprises a 3x3 virtual grid, and means for authenticating and granting access comprises means for authenticating and granting access to the user in response to a determination of the
30 movements over the virtual grid matching a reference pattern.

20. The wearable apparatus of claim 18, wherein the virtual grid comprises a 4x3 virtual keypad, and means for authenticating and granting access comprises means for authenticating and granting access to the user in response to a determination of the movements over the virtual grid matching a reference pattern, a personal information
5 number (PIN) or a password.

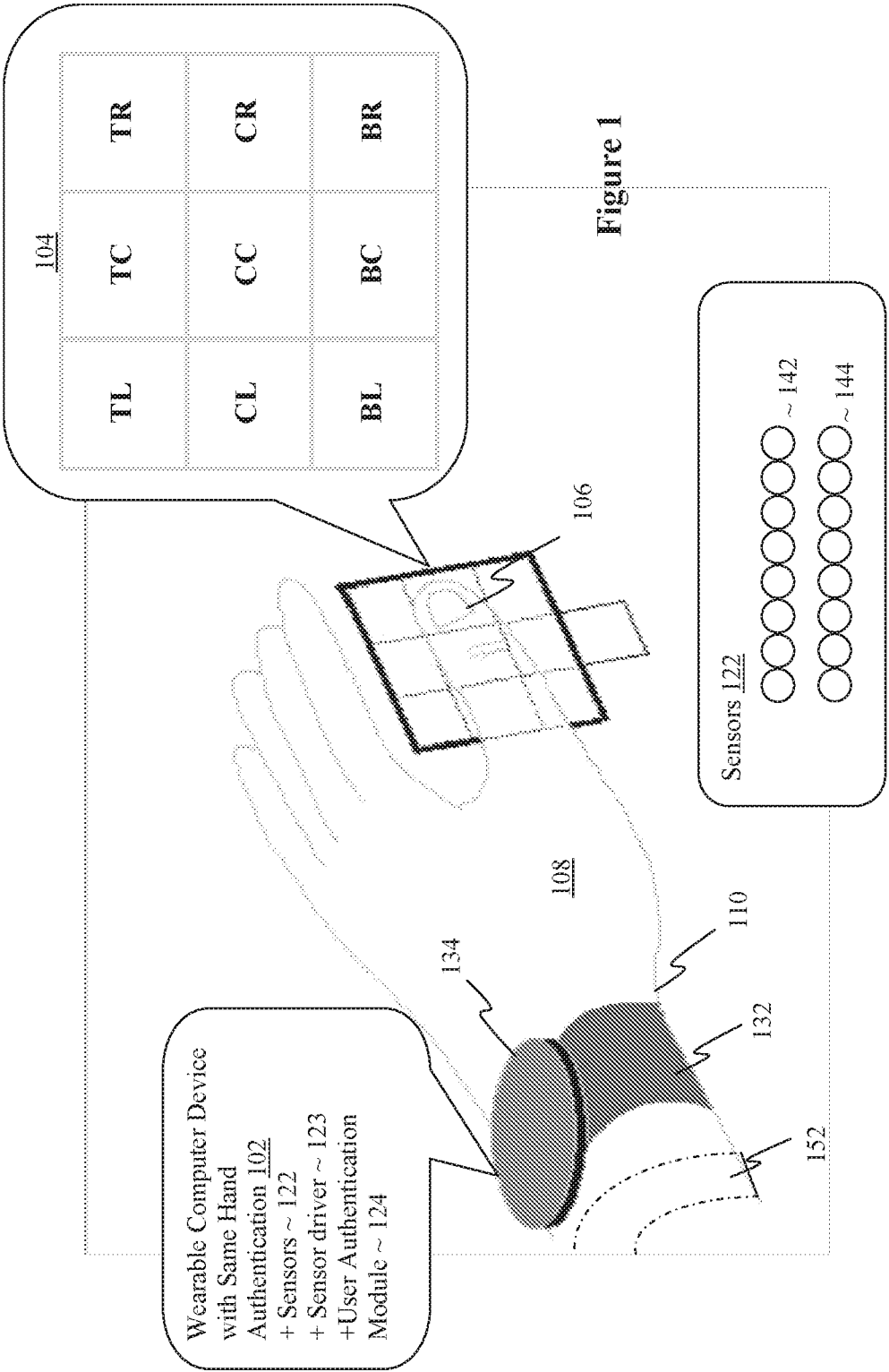
21. The wearable apparatus of claim 18, wherein the one or more fingers comprise a thumb of the hand of the user that adjoins the wrist on which the wearable apparatus is worn.

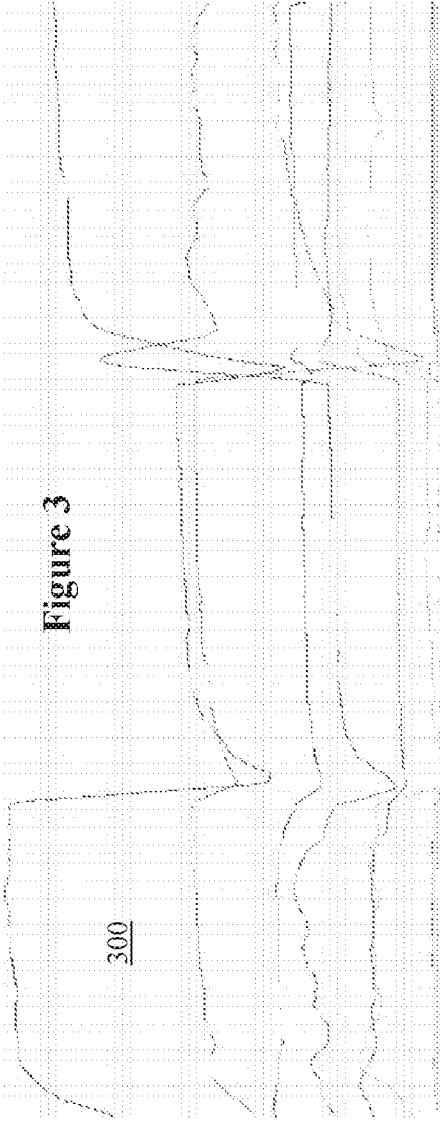
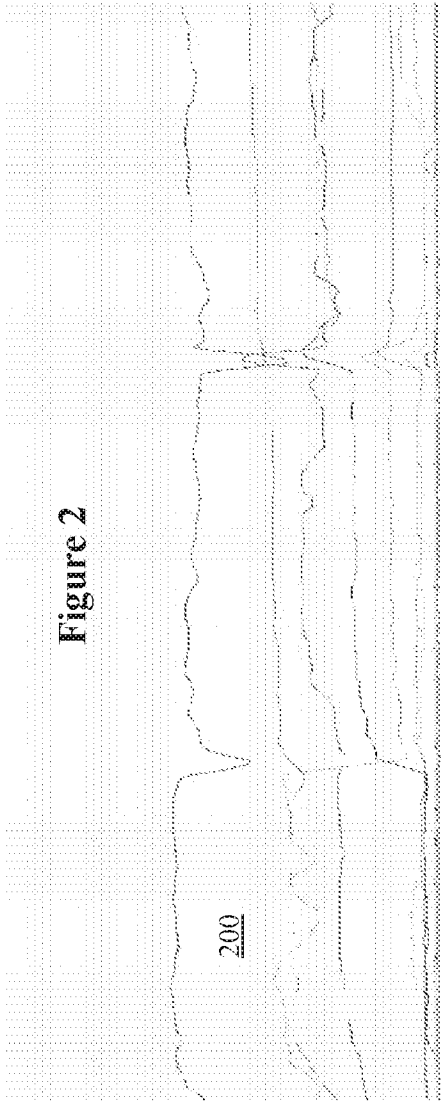
22. The wearable apparatus of claim 18, wherein means for receiving
10 comprises means for receiving sensor signals representative of tendon or muscle positions of the wrist, and means for processing the sensor signals to output the sensor data.

23. The wearable apparatus of claim 22, further comprises means for sensing and outputting the sensor signals representative of the tendon or muscle positions of the wrist; wherein the wearable computer device is a smart watch having a watch band, and
15 the means for sensing comprises a plurality of sensors disposed on the watch band.

24. The wearable apparatus of claim 22, wherein means for receiving sensor signals comprises means for receiving sensor signals from an external wrist band having a plurality of sensors to sense and output the sensor signals representative of the tendon or muscle positions of the wrist, and processing the sensor signals into the sensor data;
20 wherein the external wrist band is not part of the wearable apparatus.

25. The wearable apparatus of any one of claims 18-24, further comprising means for providing visual feedbacks to the user to assist the user in traversing the virtual grid; wherein means for providing visual feedbacks comprises means for displaying a graphical representation of the virtual grid, including indicators indicating portions of the
25 virtual grid traversed.





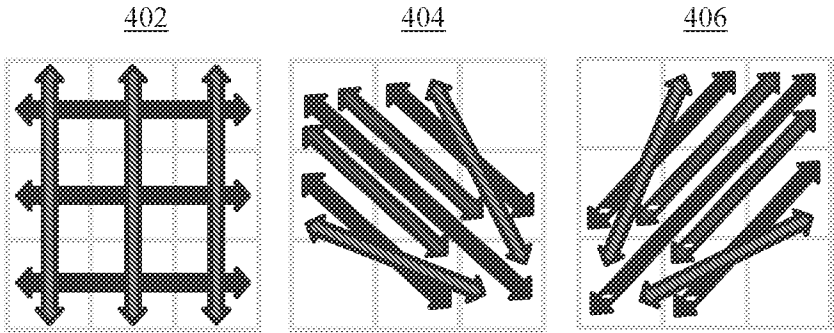


Figure 4

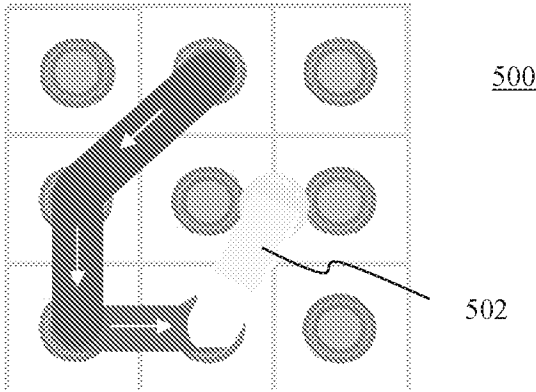


Figure 5

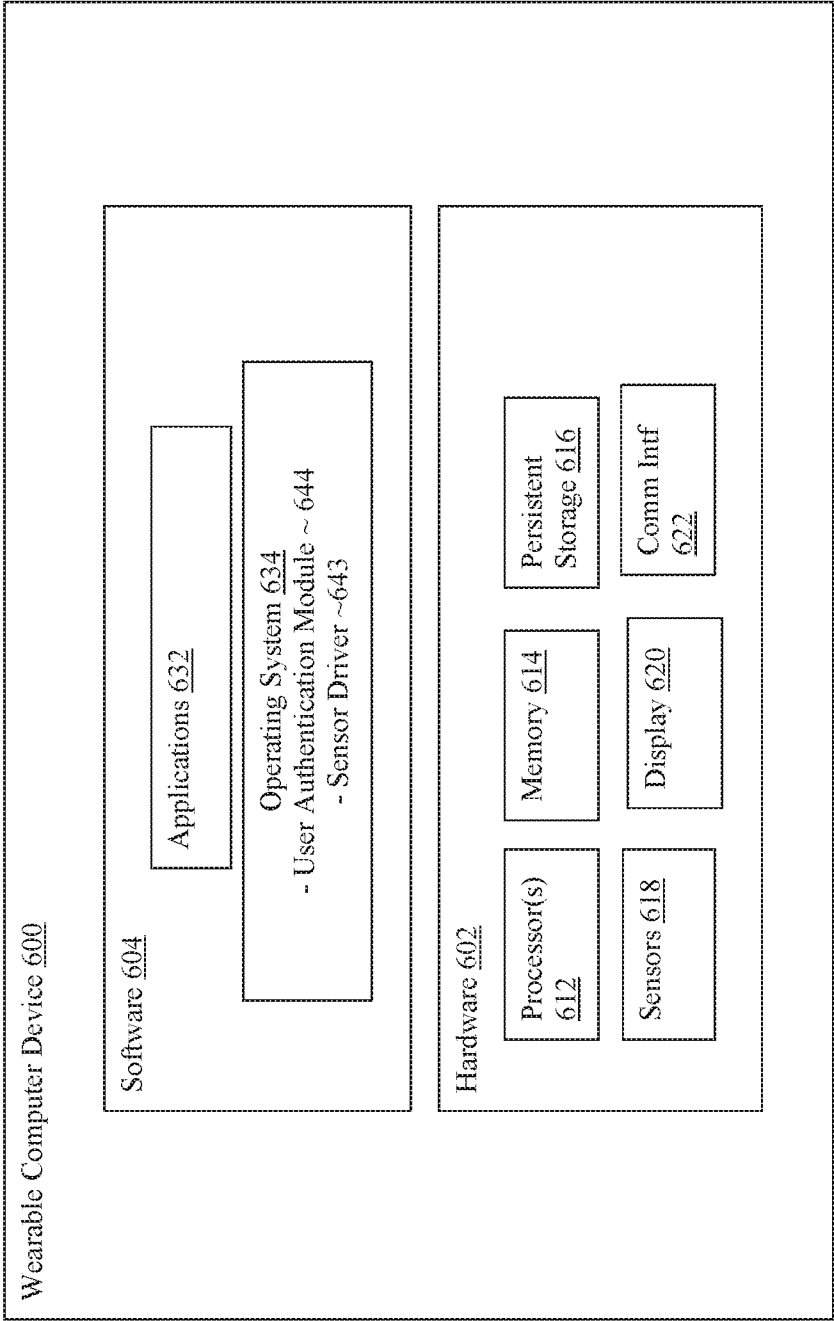


Figure 6

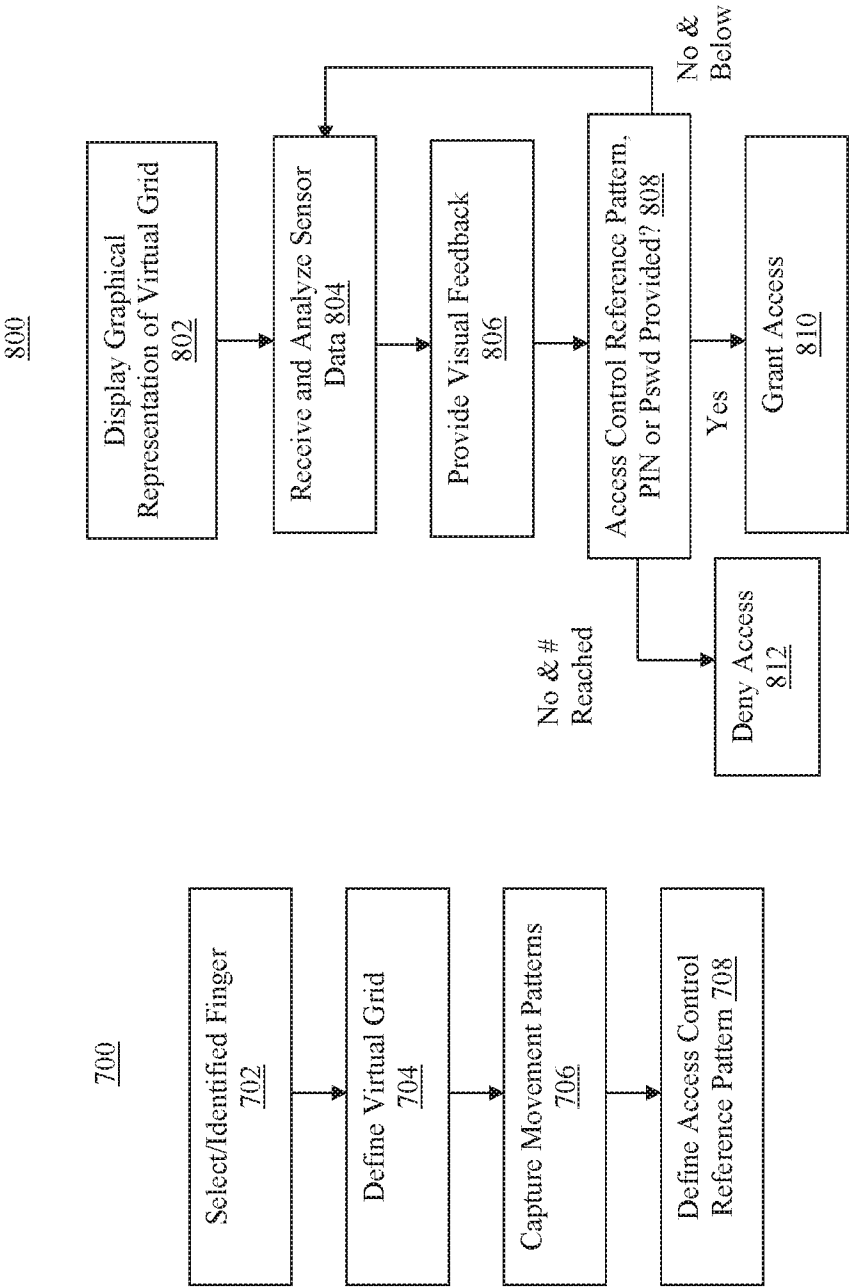


Figure 7

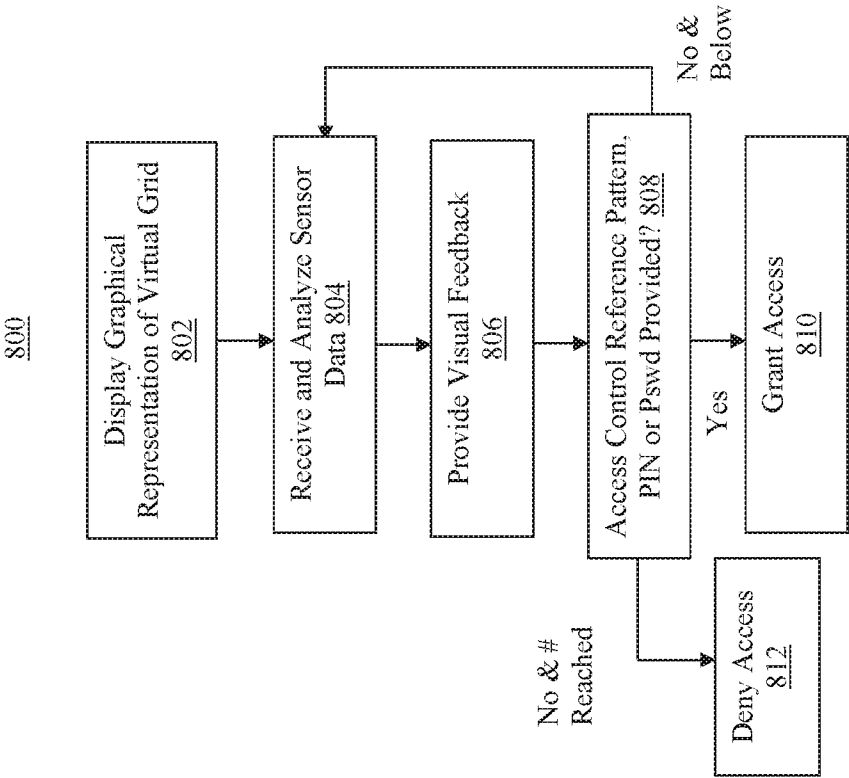


Figure 8

1000

1	2	3
4	5	6
7	8	9
Bksp	0	Enter

Figure 10

900

TL	TC	TR
CL	CC	CR
BL	BC	BR
AL	AC	AR

Figure 9

1100

1	2 ABC	3 DEF
4 GHI	5 JKL	6 MNO
7 PQR	8 STU	9 WXYZ
Bksp/ *	0	Enter/ #

Figure 11

INTERNATIONAL SEARCH REPORT

International application No.
PCT/US2017/029394**A. CLASSIFICATION OF SUBJECT MATTER****G06F 21/31(2013.01)i, G06F 1/16(2006.01)i, G06F 3/01(2006.01)i, H04L 9/32(2006.01)i**

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 21/31; G06N 5/04; H04L 29/06; G06F 3/01; G06T 19/00; G01C 21/00; G06F 1/16; H04L 9/32

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

Korean utility models and applications for utility models

Japanese utility models and applications for utility models

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)

eKOMPASS(KIPO internal) & keywords: user authentication module, wearable, movements, fingers

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
Y	US 2015-0362999 A1 (LG ELECTRONICS INC.) 17 December 2015 See paragraphs [0053]-[0123], [0151]-[0169], [0258]-[0261]; and figures 1A, 2-3c, 23(a)-23(c).	1-25
Y	US 2013-0346168 A1 (DYLAN T X ZHOU et al.) 26 December 2013 See paragraph [0042]; claims 1-62; and figure 3.	1-25
Y	KR 10-1497829 B1 (HYUNDAI MNSOFT, INC.) 04 March 2015 See paragraphs [0050]-[0053]; claims 1-5; and figure 8.	8, 24
A	US 2014-0317028 A1 (BIOCATCH LTD.) 23 October 2014 See paragraphs [0080]-[0082]; claims 1-35; and figure 8.	1-25
A	US 2015-0301606 A1 (VALENTIN ANDREI) 22 October 2015 See paragraphs [0054]-[0064]; and figures 5-8.	1-25



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

25 July 2017 (25.07.2017)

Date of mailing of the international search report

01 August 2017 (01.08.2017)

Name and mailing address of the ISA/KR

International Application Division

Korean Intellectual Property Office

189 Cheongsa-ro, Seo-gu, Daejeon, 35208, Republic of Korea

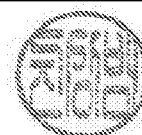


Facsimile No. +82-42-481-8578

Authorized officer

CHIN, Sang Bum

Telephone No. +82-42-481-8398



INTERNATIONAL SEARCH REPORT

Information on patent family members

International application No.

PCT/US2017/029394

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
US 2015-0362999 A1	17/12/2015	CN 105282316 A	27/01/2016
		EP 2957986 A1	23/12/2015
		FR 3022367 A1	18/12/2015
		KR 10-2015-0144668 A	28/12/2015
US 2013-0346168 A1	26/12/2013	CN 104781841 A	15/07/2015
		CN 104995545 A	21/10/2015
		CN 105164707 A	16/12/2015
		EP 2896001 A1	22/07/2015
		EP 2896011 A1	22/07/2015
		EP 2898464 A1	29/07/2015
		EP 2904557 A1	12/08/2015
		EP 2912620 A1	02/09/2015
		US 2011-0276636 A1	10/11/2011
		US 2012-0006891 A1	12/01/2012
		US 2012-0059699 A1	08/03/2012
		US 2013-0006788 A1	03/01/2013
		US 2013-0018715 A1	17/01/2013
		US 2013-0018782 A1	17/01/2013
		US 2013-0026232 A1	31/01/2013
		US 2013-0043305 A1	21/02/2013
		US 2013-0141313 A1	06/06/2013
		US 2013-0146659 A1	13/06/2013
		US 2013-0172068 A1	04/07/2013
		US 2013-0173362 A1	04/07/2013
		US 2013-0191174 A1	25/07/2013
		US 2013-0225290 A1	29/08/2013
		US 2013-0236877 A1	12/09/2013
		US 2013-0238401 A1	12/09/2013
		US 2013-0240622 A1	19/09/2013
		US 2013-0311484 A1	21/11/2013
		US 2014-0058804 A1	27/02/2014
		US 2014-0098758 A1	10/04/2014
		US 2014-0129422 A1	08/05/2014
		US 2014-0143037 A1	22/05/2014
		US 2014-0189354 A1	03/07/2014
		US 2014-0236750 A1	21/08/2014
		US 2014-0239065 A1	28/08/2014
		US 2014-0254896 A1	11/09/2014
		US 2014-0330656 A1	06/11/2014
		US 2014-0349692 A1	27/11/2014
		US 2015-0026072 A1	22/01/2015
		US 2015-0066613 A1	05/03/2015
		US 2015-0088757 A1	26/03/2015
		US 2015-0161721 A1	11/06/2015
		US 2015-0229750 A1	13/08/2015
		US 2015-0339696 A1	26/11/2015
		US 2015-0371215 A1	24/12/2015
		US 2016-0086161 A1	24/03/2016

INTERNATIONAL SEARCH REPORT

Information on patent family members

International application No.

PCT/US2017/029394

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
		US 2016-0110695 A1	21/04/2016
		US 2016-0114887 A1	28/04/2016
		US 2016-0162873 A1	09/06/2016
		US 2016-0189137 A1	30/06/2016
		US 2016-0225019 A1	04/08/2016
		US 2016-0232620 A1	11/08/2016
		US 2016-0275482 A1	22/09/2016
		US 2016-0275483 A1	22/09/2016
		US 2016-0286128 A1	29/09/2016
		US 8851372 B2	07/10/2014
		US 8968103 B2	03/03/2015
		US 8985442 B1	24/03/2015
		US 9009166 B2	14/04/2015
		US 9016565 B2	28/04/2015
		US 9047600 B2	02/06/2015
		US 9098190 B2	04/08/2015
		US 9100493 B1	04/08/2015
		US 9153074 B2	06/10/2015
		US 9208505 B1	08/12/2015
		US 9317883 B2	19/04/2016
		US 9342829 B2	17/05/2016
		US 9361616 B2	07/06/2016
		US 9367841 B2	14/06/2016
		US 9406063 B2	02/08/2016
		US 9489671 B2	08/11/2016
		US 9493235 B2	15/11/2016
		US 9510277 B2	29/11/2016
		US 9563890 B2	07/02/2017
		US 9576285 B2	21/02/2017
		US 9600832 B2	21/03/2017
		US 9619794 B2	11/04/2017
		WO 2013-064986 A1	10/05/2013
		WO 2014-041456 A1	20/03/2014
		WO 2014-041458 A1	20/03/2014
		WO 2014-045145 A1	27/03/2014
		WO 2014-053924 A1	10/04/2014
		WO 2014-064549 A1	01/05/2014
		WO 2014-118703 A1	07/08/2014
		WO 2014-122558 A1	14/08/2014
		WO 2014-132192 A1	04/09/2014
		WO 2014-141076 A2	18/09/2014
		WO 2014-141076 A3	29/01/2015
		WO 2014-162257 A2	09/10/2014
		WO 2014-162257 A3	05/02/2015
		WO 2014-174398 A2	30/10/2014
		WO 2014-174398 A3	24/12/2014
		WO 2014-174399 A2	30/10/2014
		WO 2014-174399 A3	26/02/2015
		WO 2015-025251 A1	26/02/2015
		WO 2015-063627 A1	07/05/2015

INTERNATIONAL SEARCH REPORT

Information on patent family members

International application No.

PCT/US2017/029394

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
		WO 2015-107442 A1	23/07/2015
		WO 2015-114475 A1	06/08/2015
		WO 2015-132767 A1	11/09/2015
		WO 2015-162565 A1	29/10/2015
		WO 2015-170253 A1	12/11/2015
		WO 2015-177760 A2	26/11/2015
		WO 2015-177760 A3	14/01/2016
		WO 2016-009287 A1	21/01/2016
		WO 2016-024183 A2	18/02/2016
		WO 2016-024183 A3	21/04/2016
		WO 2016-055877 A1	14/04/2016
		WO 2016-075598 A2	19/05/2016
		WO 2016-075598 A3	07/07/2016
		WO 2016-083906 A1	02/06/2016
		WO 2016-132252 A1	25/08/2016
		WO 2016-170445 A2	27/10/2016
		WO 2016-170445 A3	15/12/2016
		WO 2017-021882 A1	09/02/2017
KR 10-1497829 B1	04/03/2015	None	
US 2014-0317028 A1	23/10/2014	EP 2646904 A1	09/10/2013
		EP 3011483 A1	27/04/2016
		EP 3019991 A1	18/05/2016
		US 2013-0239195 A1	12/09/2013
		US 2013-0288647 A1	31/10/2013
		US 2014-0317726 A1	23/10/2014
		US 2014-0317744 A1	23/10/2014
		US 2014-0325223 A1	30/10/2014
		US 2014-0325645 A1	30/10/2014
		US 2014-0325646 A1	30/10/2014
		US 2014-0325682 A1	30/10/2014
		US 2014-0344927 A1	20/11/2014
		US 2015-0094030 A1	02/04/2015
		US 2015-0205944 A1	23/07/2015
		US 2015-0205955 A1	23/07/2015
		US 2015-0205957 A1	23/07/2015
		US 2015-0205958 A1	23/07/2015
		US 2015-0212843 A1	30/07/2015
		US 2015-0213246 A1	30/07/2015
		US 2015-0213251 A1	30/07/2015
		US 2015-0256528 A1	10/09/2015
		US 2015-0264572 A1	17/09/2015
		US 2015-0310196 A1	29/10/2015
		US 2016-0132105 A1	12/05/2016
		US 2016-0197918 A1	07/07/2016
		US 2016-0294837 A1	06/10/2016
		US 2016-0300054 A1	13/10/2016
		US 2016-0306974 A1	20/10/2016
		US 2016-0307191 A1	20/10/2016

INTERNATIONAL SEARCH REPORT

Information on patent family members

International application No.

PCT/US2017/029394

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
US 2015-0301606 A1	22/10/2015	US 2016-0307201 A1	20/10/2016
		US 2016-0321445 A1	03/11/2016
		US 2016-0321689 A1	03/11/2016
		US 2016-0366177 A1	15/12/2016
		US 2016-0371476 A1	22/12/2016
		US 8938787 B2	20/01/2015
		US 9069942 B2	30/06/2015
		US 9071969 B2	30/06/2015
		US 9275337 B2	01/03/2016
		US 9418221 B2	16/08/2016
		US 9450971 B2	20/09/2016
		US 9477826 B2	25/10/2016
		US 9483292 B2	01/11/2016
		US 9526006 B2	20/12/2016
		US 9531701 B2	27/12/2016
		US 9531733 B2	27/12/2016
		US 9536071 B2	03/01/2017
		US 9541995 B2	10/01/2017
		US 9547766 B2	17/01/2017
		US 9552470 B2	24/01/2017
		US 9558339 B2	31/01/2017
		US 9621567 B2	11/04/2017
		US 9626677 B2	18/04/2017
		US 9665703 B2	30/05/2017
		US 9674218 B2	06/06/2017
		WO 2012-073233 A1	07/06/2012
		WO 2014-203163 A1	24/12/2014
		WO 2015-004598 A1	15/01/2015
		WO 2017-006268 A1	12/01/2017
		KR 10-2016-0122816 A	24/10/2016
		TW 201606573 A	16/02/2016
		TW 1567587 B	21/01/2017
		WO 2015-160481 A1	22/10/2015