

(43) International Publication Date
25 September 2014 (25.09.2014)(51) International Patent Classification:
G06K 9/00 (2006.01)(21) International Application Number:
PCT/US2014/020123(22) International Filing Date:
4 March 2014 (04.03.2014)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
13/837,296 15 March 2013 (15.03.2013) US(71) Applicant: **APPLE INC.** [US/US]; 1 Infinite Loop, M/S 169-3IPL, Cupertino, California 95014 (US).(72) Inventors: **MINTEER, Gregory, T.**; 20425 Stevens Creek Blvd, M/S 85-1SEG, Cupertino, California 95014 (US). **LANDY, Patrick, J.**; 20425 Stevens Creek Blvd, M/S 85-1SEG, Cupertino, California 95014 (US). **KONOPKA, Ondrej**; Husinecka 7, M/S 7001RE, 130 00 Prague 3, Bohemia (CZ).(74) Agents: **REGAN, Christopher F.** et al.; Allen, Dyer, Doppelt, Milbrath & Gilchrist, P.A., 255 S. Orange Avenue, Suite 1401, Orlando, Florida 32801 (US).

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

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

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

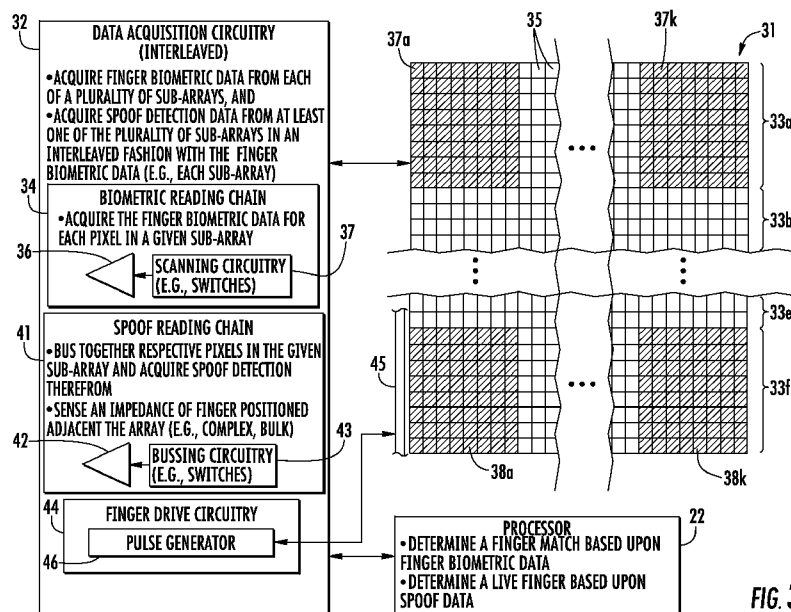
Declarations under Rule 4.17:

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

Published:

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

(54) Title: ELECTRONIC FINGERPRINT ACQUISITION WITH INTERLEAVED SPOOF DETECTION

**FIG. 3**

(57) Abstract: An electronic device may include an array of finger sensing pixels and data acquisition circuitry coupled to the array. The data acquisition circuitry may be capable of acquiring finger biometric data from each sub-array of the array, and acquiring spoof detection data from at least one of the sub-arrays in an interleaved fashion with the finger biometric data.

ELECTRONIC FINGERPRINT ACQUISITION WITH INTERLEAVED SPOOF DETECTION

Field of the Invention

[0001] The present invention relates to the field of electronics, and, more particularly, to the field of finger sensors and related methods.

Background of the Invention

[0002] Fingerprint sensing and matching is a reliable and widely used technique for personal identification or verification. In particular, a common approach to fingerprint identification involves scanning a sample fingerprint or an image thereof and storing the image and/or unique characteristics of the fingerprint image. The characteristics of a sample fingerprint may be compared to information for reference fingerprints already in a database to determine proper identification of a person, such as for verification purposes.

[0003] A particularly advantageous approach to fingerprint sensing is disclosed in U.S. Patent No. 5,963,679 to Setlak et al. and assigned to the assignee of the present invention. The fingerprint sensor is an integrated circuit sensor that drives the user's finger with an electric field signal and senses the electric field with an array of electric field sensing pixels on the integrated circuit substrate. Such sensors are used to control access for many different types of electronic devices such as computers, cell phones, personal digital assistants (PDA's), and the like. In particular, fingerprint sensors are used because they may have a small footprint, are relatively easy for a user to use and they provide reasonable authentication capabilities.

[0004] Another significant advance in finger sensing technology is disclosed in U.S. Patent No. 5,953,441 also to Setlak et al., assigned to the assignee of the present invention, and the entire contents of which are incorporated by reference. This patent discloses a fingerprint sensor

including an array of impedance sensing elements for generating signals related to an object positioned adjacent thereto, and a spoof reducing circuit for determining whether or not an impedance of the object positioned adjacent the array of impedance sensing elements corresponds to a live finger to thereby reduce spoofing of the fingerprint sensor by an object other than a live finger. A spoofing may be indicated and/or used to block further processing. The spoof reducing circuit may detect a complex impedance having a phase angle in a range of about 10 to 60 degrees corresponding to a live finger. The fingerprint sensor may include a drive circuit for driving the array of impedance sensing elements, and a synchronous demodulator for synchronously demodulating signals from the array of impedance sensing elements.

[0005] "Spoof" fingerprints are typically made using natural and artificial materials, such as gelatin, gum, gummy bears, meat products, clay, Play-Doh, auto body filler, resins, metal, etc. that can be used to imitate the ridges and valleys present in a real fingerprint. As it is desirable to be able to acquire a fingerprint image under any skin condition (dry, moist, etc.) some fingerprint sensors employ real-time gain and other adjustments to obtain the best possible images. In doing so, sensors that detect fingerprints using these approaches are sometimes susceptible to attack using spoofs because these systems are capable of imaging widely varying skin conditions (and other materials).

[0006] Spoof detection approaches can be broadly classified into hardware and software based approaches. Hardware based approaches typically involve coupling a biometric device to a finger sensor. For example, previous work in the area of spoof detection and reduction may be considered as having used: A.) impedance classification: determining the impedance characteristics of a material over some frequency range; B.) optical dispersion characteristics; C.) thermal measurements; D.) phase setting and signal amplitude; and E.) finger settling detection. In contrast, a software based approach to spoof detection may not involve changes or

additions to a finger sensor. A software based approach may involve additional comparisons of finger samples from a user.

[0007] Abhyankar et al., Fingerprint Liveness Detection Using Local Ridge Frequencies and Multiresolution Texture Analysis Techniques, *Proc. Int. Conf. Image Processing*, 2006, discloses adopting statistical features obtained through multi-resolution texture and local-ridge frequency analysis. Classification is performed using a fuzzy c-means classifier. U.S. Patent No. 7,505,613 to Russo, also assigned to the present assignee, discloses a method of finger spoof detection that is similar to Abhyankar et al., but adds user adaptability.

Summary of the Invention

[0008] In view of the foregoing background, it is therefore an object of the present invention to provide an electronic device having increased security.

[0009] This and other objects, features, and advantages in accordance with the present invention are provided by an electronic device that may include an array of finger sensing pixels and data acquisition circuitry coupled to the array of finger sensing pixels. The data acquisition circuitry may be capable of acquiring finger biometric data from each of a plurality of sub-arrays of the array of finger sensing pixels. The data acquisition circuitry may also be capable of acquiring spoof detection data from at least one of the plurality of sub-arrays in an interleaved fashion with the finger biometric data. Accordingly, the electronic device may advantageously provide increased security, for example, by making it increasingly difficult to switch between a “live” finger and a “spoof” finger while acquiring finger biometric data.

[0010] The acquisition circuitry may include a biometric reading chain capable of acquiring the finger biometric data for each finger sensing pixel in a given sub-array, for example. A spoof reading chain may be capable of bussing together respective finger sensing pixels in the given sub-array and acquiring spoof detection data therefrom.

[0011] The biometric reading chain may include at least one first amplifier and scanning circuitry associated therewith. The spoof reading chain may include at least one second amplifier and bussing circuitry associated therewith, for example.

[0012] The spoof reading chain may be capable of sensing an impedance of a finger positioned adjacent the array of finger sensing pixels, for example. The data acquisition circuitry may further include finger drive circuitry coupled to the array of finger sensing pixels. The finger drive circuitry may include a finger drive electrode adjacent the array of finger sensing pixels and a pulse generator coupled between the finger drive electrode and the array of finger sensing pixels.

[0013] The electronic device may further include a processor coupled to the data acquisition circuitry and capable of determining a finger match and a live finger based upon the finger biometric data and spoof data, respectively, for example.

[0014] Each of the finger sensing pixels may include an electric field finger sensing pixel, for example. The data acquisition circuitry may be capable of acquiring spoof detection data from each of the plurality of sub-arrays. The array of finger sensing pixels may define a rectangle, for example, and each of the sub-arrays may extend across a side of the rectangle.

[0015] A method aspect is directed to a method of spoof detection. The method may include using data acquisition circuitry coupled to an array of finger sensing pixels to acquire finger biometric data from each of a plurality of sub-arrays of the array of finger sensing pixels. The method may also include using the data acquisition circuitry to acquire spoof detection data from at least one of the plurality of sub-arrays in an interleaved fashion with the finger biometric data.

Brief Description of the Drawings

[0016] FIG. 1 is a plan view of an electronic device according to the present invention.

[0017] FIG. 2 is a schematic block diagram of a portion of the electronic device of FIG. 1.

[0018] FIG. 3 is another schematic block diagram of a portion of the electronic device of FIG. 1.

[0019] FIG. 4 is a flowchart of a method of spoof detection in accordance with the present invention.

Detailed Description

[0020] The present invention will now be described more fully hereinafter with reference to the accompanying drawings, in which preferred embodiments of the invention are shown. This invention may, however, be embodied in many different forms and should not be construed as limited to the embodiments set forth herein. Rather, these embodiments are provided so that this disclosure will be thorough and complete, and will fully convey the scope of the invention to those skilled in the art. Like numbers refer to like elements throughout.

[0021] Referring initially to FIGS. 1-3, an electronic device **20** is now described. The electronic device **20** illustratively includes a portable housing **21** and a processor **22** carried by the portable housing. The electronic device **20** is illustratively a mobile wireless communications device, for example, a cellular telephone. The electronic device **20** may be another type of electronic device, for example, a tablet computer, laptop computer, etc.

[0022] Wireless communications circuitry **25** (e.g. a wireless transceiver, cellular, WLAN Bluetooth, etc.) is also carried within the housing **21** and coupled to the processor **22**. The wireless transceiver **25** cooperates with the processor **22** to perform at least one wireless communications function, for example, for voice and/or data. In some embodiments, the electronic device **20** may not include a wireless transceiver **25**.

[0023] A display **23** is also carried by the portable housing **21** and is coupled to the processor **22**. The display **23** may be a liquid crystal display (LCD), for example, or may be another type of display, as will be

appreciated by those skilled in the art. A memory **26** is also coupled to the processor **22**.

[0024] A finger-operated user input device **24**, illustratively in the form of a pushbutton switch, is also carried by the portable housing **21** and is coupled to the processor **22**. The pushbutton switch **24** cooperates with the processor **22** to perform a device function in response to the pushbutton switch. For example, a device function may include a powering on or off of the electronic device **20**, initiating communication via the wireless communications circuitry **25**, and/or performing a menu function.

[0025] More particularly, with respect to a menu function, the processor **22** may change the display **23** to show a menu of available applications based upon pressing of the pushbutton switch **24**. In other words, the pushbutton switch **24** may be a home switch or button, or key. Of course, other device functions may be performed based upon the pushbutton switch **24**. In some embodiments, the finger-operated user input device **24** may be a different type of finger-operated user input device, for example, forming part of a touch screen display. Other or additional finger-operated user input devices may be carried by the portable housing **21**.

[0026] An array of finger sensing pixels **31** is carried by the pushbutton switch **24** to sense a user's finger **40** or an object placed adjacent the array of finger sensing pixels. The array of finger sensing pixels **31** is carried by the pushbutton switch **24** so that when a user or object contacts and/or presses downward on the pushbutton switch, data from the user's finger **40** is acquired, for example, for finger matching and/or spoof detection, as will be described in further detail below. In other words, the array of finger sensing pixels **31** may cooperate with circuitry, as will be explained in further detail below, to be responsive to static contact or placement of the user's finger **40** or object. Of course, in other embodiments, for example, where the array of finger sensing pixels **31** is not carried by a pushbutton switch, the array of finger sensing pixels may cooperate with circuitry to be responsive to sliding contact (i.e. a slide

sensor), or responsive to static placement (i.e. a standalone static placement sensor).

[0027] The array of finger sensing pixels **31** is illustratively an 88x88 array of finger sensing pixels. In other words, conceptually, the array of can be organized into 88 rows of 88 pixels and defines a rectangle. Of course, in some embodiments, the array of finger sensing pixels **31** may be a different size. Each finger sensing pixel **35** may be an electric field sensing pixel such as disclosed in U.S. Patent No. 5,940,526 to Setlak et al., assigned to the present assignee, and the entire contents of which are herein incorporated by reference. Of course, in some embodiments, each finger sensing pixel **35** may another type of finger sensing pixel.

[0028] The electronic device **20** also includes data acquisition circuitry **32** coupled to the array of finger sensing pixels **31**. The data acquisition circuitry **32** is capable of acquiring finger biometric data from each of a plurality of sub-arrays **33a-33f** of the array of finger sensing pixels **31**. The data acquisition circuitry **32** illustratively includes a biometric reading chain **34** capable of acquiring the finger biometric data for each pixel in a given sub-array **33a-33f**. The biometric reading chain **34** includes first amplifier **36** and scanning circuitry associated therewith **37**. One or more additional first amplifiers may be used, as will be appreciated by those skilled in the art.

[0029] Illustratively, for the 88x88 array of finger sensing pixels **31**, each sub-array **33a-33f** includes 8 rows of 88 pixels (i.e., 11 sub-arrays). In other words, each of the sub-arrays **33a-33f** extends across a side of the rectangle. Of course, each sub-array **33a-33f** may include a different amount of pixels **35** and may be in a different configuration. For example, in some embodiments, it may be particularly desirable to have each sub-array **33a-33f** have less than 10% of a total of finger sensing pixels **35** in the array of finger sensing pixels **31**. Each sub-array **33a-33f** may be divided in 8x8 regions **37a, 37k, 38a, 38k**. The finger sensing pixels **35** of each sub-array **33a-33f** may be acquired by region. In other words, finger biometric data in each sub-array **33a-33f** may be acquired by scanning

across the regions **37a**, **37k**, **38a**, **38k**. In some embodiments, the finger biometric data from the sub-arrays **33a-33f** may be averaged to reduce noise.

[0030] The data acquisition circuitry **32** is also capable of acquiring spoof detection data from the sub-arrays **33a-33f** in an interleaved fashion with the finger biometric data. The spoof detection data may be impedance data, for example, complex or bulk impedance data.

[0031] A spoof reading chain **41** is capable of bussing together respective pixels **35** in the given sub-array **33a-33f** and acquiring spoof detection data therefrom. The spoof reading chain **41** includes a second amplifier **42** and bussing circuitry **43** associated therewith. One or more additional second amplifiers may be used, as will be appreciated by those skilled in the art. The bussing circuitry **43** may include switches, for example, for bussing together pixels in the given sub-array **33a-33f** for the acquisition of the spoof detection data.

[0032] In some embodiments, the data acquisition circuitry **32** may be capable of acquiring spoof detection data corresponding to each acquisition of finger biometric data. Of course, the spoof detection data may be interleaved with the finger biometric data in other or additional acquisition configurations.

[0033] The data acquisition circuitry **32** also includes finger drive circuitry **44** coupled to the array of finger sensing pixels **31**. The finger drive circuitry **44** includes a finger drive electrode **45** adjacent the array of finger sensing pixels **31**, and a pulse generator **46** coupled between the finger drive electrode and the array of finger sensing pixels. The pulse generator **46** may generate a square wave, for example, a 16V square wave at a frequency of about 1.5MHz that may be used to drive the user's finger **40** or object when positioned adjacent the array of finger sensing pixels **35**. By driving the user's finger **40**, those skilled in the art will understand that in some embodiments, it is meant that instead of driving the user's finger with a drive signal, the user's finger may be grounded while the circuitry associated with and/or array of finger sensing pixels **31**

may be driven with the drive signal. Of course, the pulse generator **46** may generate a pulse having another shape, frequency, and/or amplitude.

[0034] The acquisition of spoof data is calculated from the rising edge of the pulse from the pulse generator **46**. In particular, the reading chain **41** busses together the finger sensing pixels **35** in a given sub-array **33a-33f** and acquires about 50-100 spoof measurement data samples to be used for an impedance measurement. The falling edge of the pulse may also be used to acquire the acquisition of spoof data.

[0035] In some embodiments, the samples or spoof detection data may be sent to the processor **22** (i.e., host processor) for processing. The processor **22** may determine, whether the object positioned adjacent the array of finger sensing pixels **31** have characteristics indicative of a spoof based upon a response step size, for example. The response step size or pulse size may be determined by calculating the difference between the amplitude after the step or pulse has settled and the amplitude prior to the step or pulse being applied.

[0036] The processor **22** may also determine whether the object positioned adjacent the array of finger sensing pixels **31** has characteristics indicative of a spoof based upon a response rise time. The response rise time may be measured between 10% and 90% of the sampled response. The processor **22** may further determine whether the object positioned adjacent the array of finger sensing pixels **31** has characteristics indicative of a spoof based upon performing a frequency response analysis. For example, a derivative of the samples of spoof detection data may be taken and the results are subject to a fast Fourier transform (FFT). The derivative of the response is the impulse response of the user's finger or object. A discrete Fourier transform (DFT) of the 50-100 samples of spoof detection data for the sub-array may also be calculated to determine whether the object positioned adjacent the array of finger sensing pixels **31** has characteristics indicative of a spoof. In other words, the processor **22** determines whether the user's finger **40** or object is a "live finger" i.e., not a spoof. For example, the processor **22** may make a spoof determination

several times in the sensing of a given user's finger **40** or object (e.g. 10-11 times for the 88x88 array of finger sensing pixels described above).

Additionally, similar to the acquisition of finger biometric data, the acquired spoof detection data may be averaged to reduce noise.

[0037] Of course, any of the techniques described above may be used individually or together along with other or additional spoof determining techniques. For example, the processor **22** may cooperate with the array of finger sensing pixels **31** and the finger drive electrode **45** to determine whether the object has characteristics of a spoof based upon a differential sensing. Moreover, the drive signal or the pulse from the pulse generator **46** may have its output impedance, common mode level, and/or slew rate controlled or adopted for different fingers or conditions. Calibration techniques may also be used with respect to the drive signal.

[0038] Additionally, the processor **22** may determine a finger match based upon the finger biometric data. In other words, in some embodiments, the finger biometric data may be matched against enrolled finger biometric data, for example, to permit access to the electronic device **20**, enable certain functionality, and/or perform certain functions, as will be appreciated by those skilled in the art. Of course, the processor **22** may use other techniques to determine whether the user's finger **40** or object is "live" or a spoof as will be appreciated by those skilled in the art.

[0039] Also, in some embodiments, the finger sensor or finger sensing circuitry can be integrated on one or more integrated circuits as will be appreciated by those skilled in the art. The spoof detection data may not be sent to the processor **22** (i.e., a host processor) and may be processed using a finger sensing processor or circuitry included on the finger sensing integrated circuit (IC).

[0040] Advantageously, by acquiring spoof detection data from the sub-arrays **33a-33f** in an interleaved fashion with the finger biometric data, for example, used for matching, the chances of passing off a spoof, for example, from a latent image, may be decreased, thus increasing security.

In other words, the interleaving of spoof detection data may make it increasingly difficult to switch between a “live” finger and a “spoof” finger.

[0041] Referring now to the flowchart **60** in FIG. 4, beginning at Block **62**, the associated method of spoof detection is now described. Upon placement of the user’s finger **40** or object adjacent the array of finger sensing pixels **31**, data acquisition circuitry **32** coupled to the array of finger sensing pixels acquires finger biometric data from a given sub-array **33a-33f** of the array of finger sensing pixels (Block **64**). After each acquisition of the finger biometric data the given sub-array **33a-33f**, the data acquisition circuitry **32** busses pixels together of the given sub-array and acquires spoof detection data from the given sub-array **33a-33f** (Block **66**). After acquiring spoof detection data from the given sub-array **33a-33f**, a determination is made as to whether data from the last sub-array **33a-33f** or the end of the array of finger sensing pixels has been acquired. (Block **68**). If the data from the last sub-array **33a-33f** has been acquired, then the method ends at Block **72**. Alternatively, if there are more sub-arrays **33a-33f** from which to acquire data, the data acquisition circuitry **32** acquires finger biometric data from the next sub-array (Block **64**) and spoof detection data (Block **66**) from the next sub-array so that the spoof detection data is acquired in an interleaved fashion with the finger biometric data. The process continues until finger biometric data and spoof detection data from the last sub-array **33a-33f** have been acquired, when the method ends at Block **72**.

[0042] It should be understood that while the embodiments described may be particularly useful for both spoof detecting and matching operations, the matching operation may be performed independently of the spoof detecting operation, and vice versa. Many modifications and other embodiments of the invention will come to the mind of one skilled in the art having the benefit of the teachings presented in the foregoing descriptions and the associated drawings. Therefore, it is understood that the invention is not to be limited to the specific embodiments disclosed, and that

modifications and embodiments are intended to be included within the scope of the appended claims.

THAT WHICH IS CLAIMED IS:

1. An electronic device comprising:
an array of finger sensing pixels; and
data acquisition circuitry coupled to said array of finger sensing pixels and capable of
acquiring finger biometric data from each of a plurality of sub-arrays of said array of finger sensing pixels, and
acquiring spoof detection data from at least one of the plurality of sub-arrays in an interleaved fashion with the finger biometric data.
2. The electronic device of Claim 1, wherein said data acquisition circuitry comprises:
a biometric reading chain capable of acquiring the finger biometric data for each finger sensing pixel in a given sub-array; and
a spoof reading chain capable of bussing together respective finger sensing pixels in the given sub-array and acquiring spoof detection data therefrom.
3. The electronic device of Claim 2, wherein said biometric reading chain comprises at least one first amplifier and scanning circuitry associated therewith; and wherein said spoof reading chain comprises at least one second amplifier and bussing circuitry associated therewith.
4. The electronic device of Claim 2, wherein said spoof reading chain is capable of sensing an impedance of a finger positioned adjacent said array of finger sensing pixels.
5. The electronic device of Claim 1, wherein said data acquisition circuitry further comprises finger drive circuitry coupled to said array of finger sensing pixels.
6. The electronic device of Claim 5, wherein said finger drive circuitry comprises:

a finger drive electrode adjacent said array of finger sensing pixels; and

a pulse generator coupled between said finger drive electrode and said array of finger sensing pixels.

7. The electronic device of Claim 1, further comprising a processor coupled to said data acquisition circuitry and capable of determining a finger match and a live finger based upon the finger biometric data and spoof data, respectively.

8. The electronic device of Claim 1, wherein each of said finger sensing pixels comprises an electric field finger sensing pixel.

9. The electronic device of Claim 1, wherein said data acquisition circuitry is capable of acquiring spoof detection data from each of the plurality of sub-arrays.

10. The electronic device of Claim 1, wherein said array of finger sensing pixels defines a rectangle; and wherein each of said sub-arrays extends across a side of the rectangle.

11. An electronic device comprising:
an array of electric field finger sensing pixels; and
data acquisition circuitry coupled to said array of electric field finger sensing pixels and capable of acquiring finger biometric data from each of a plurality of sub-arrays of said array of electric field finger sensing pixels and acquiring spoof detection data from at least one of the plurality of sub-arrays in an interleaved fashion with the finger biometric data;

said data acquisition circuitry and comprising

a biometric reading chain capable of acquiring the finger biometric data for each electric field finger sensing pixel in a given sub-array, and

a spoof reading chain capable of bussing together respective electric field finger sensing pixels in the given sub-array and acquiring spoof detection data therefrom.

12. The electronic device of Claim 11, wherein said biometric reading chain comprises at least one first amplifier and scanning

circuitry associated therewith; and wherein said spoof reading chain comprises at least one second amplifier and bussing circuitry associated therewith.

13. The electronic device of Claim 11, wherein said spoof reading chain is capable of sensing an impedance of a finger positioned adjacent said array of electric field finger sensing pixels.

14. The electronic device of Claim 11, wherein said data acquisition circuitry further comprises finger drive circuitry coupled to said array of electric field finger sensing pixels.

15. The electronic device of Claim 14, wherein said finger drive circuitry comprises:

a finger drive electrode adjacent said array of electric field finger sensing pixels; and

a pulse generator coupled between said finger drive electrode and said array of electric field finger sensing pixels.

16. The electronic device of Claim 11, further comprising a processor coupled to said data acquisition circuitry and capable of determining a finger match and a live finger based upon the finger biometric data and spoof data, respectively.

17. The electronic device of Claim 11, wherein said data acquisition circuitry is capable of acquiring spoof detection data from each of the plurality of sub-arrays.

18. A method of spoof detection comprising:
using data acquisition circuitry coupled to an array of finger sensing pixels to

acquire finger biometric data from each of a plurality of sub-arrays of the array of finger sensing pixels, and

acquire spoof detection data from at least one of the plurality of sub-arrays in an interleaved fashion with the finger biometric data.

19. The method of Claim 18, wherein using the data acquisition circuitry comprises:

using a biometric reading chain to acquire the finger biometric data for each finger sensing pixel in a given sub-array; and

using a spoof reading chain to bus together respective finger sensing pixels in the given sub-array and acquiring spoof detection data therefrom.

20. The method of Claim 19, wherein using the spoof reading chain comprises using the spoof reading chain to sense an impedance of a finger positioned adjacent the array of finger sensing pixels.

21. The method of Claim 18, wherein using the data acquisition circuitry further comprises using finger drive circuitry coupled to the array of finger sensing pixels.

22. The method of Claim 18, further comprising using a processor coupled to the data acquisition circuitry to determine a finger match and a live finger based upon the finger biometric data and spoof data, respectively.

1/4

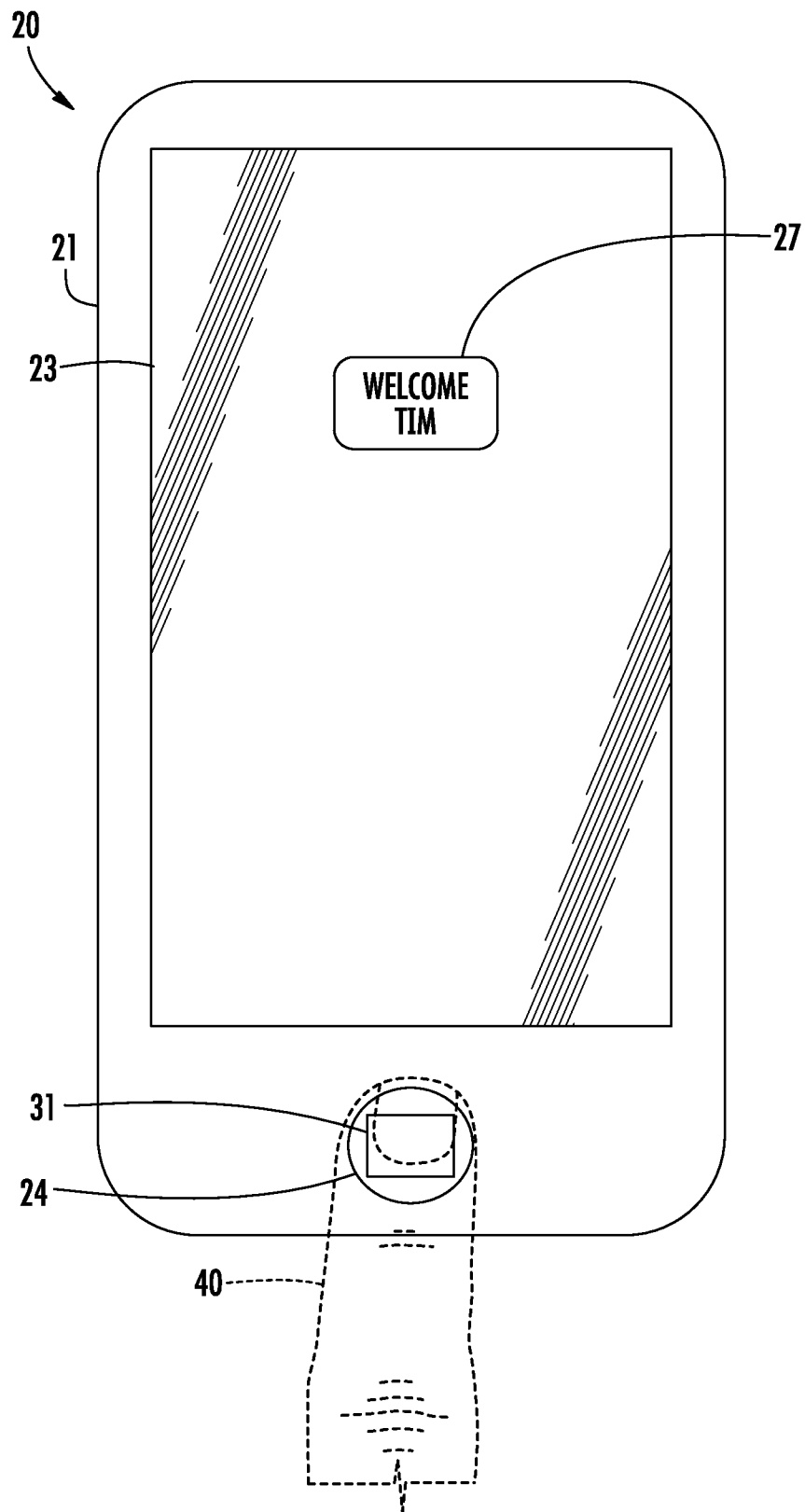


FIG. 1

2/4

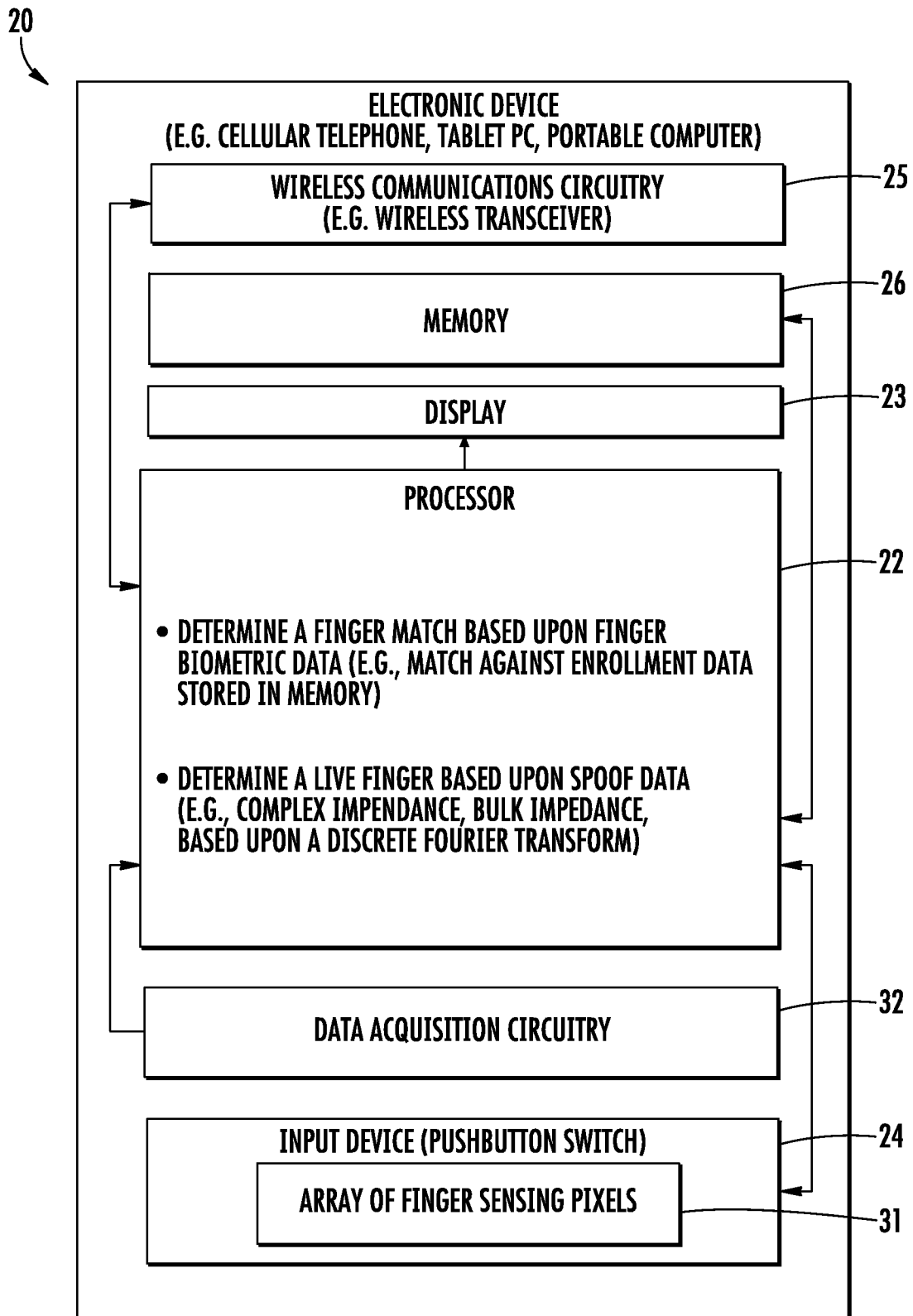


FIG. 2

3/4

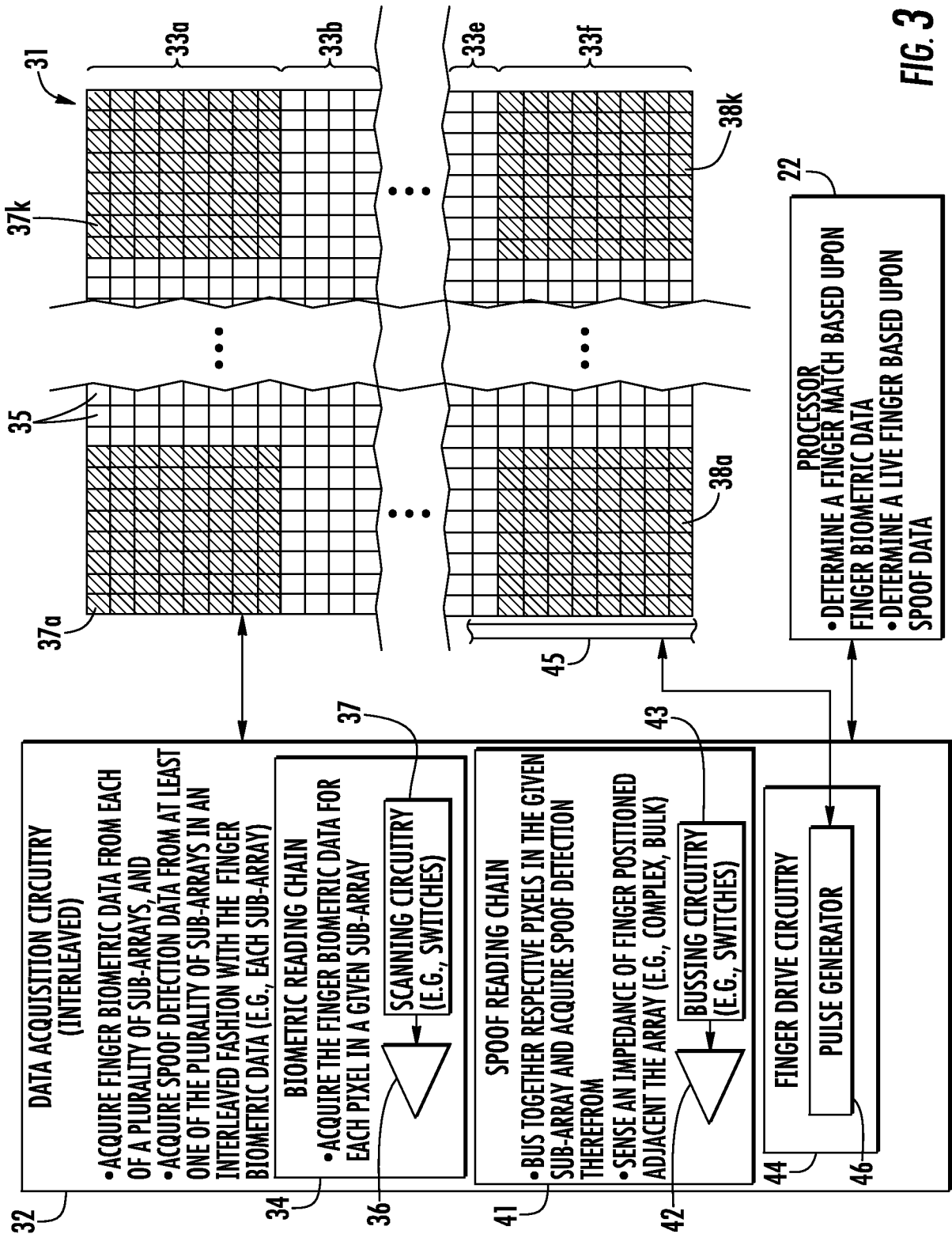


FIG. 3

4/4

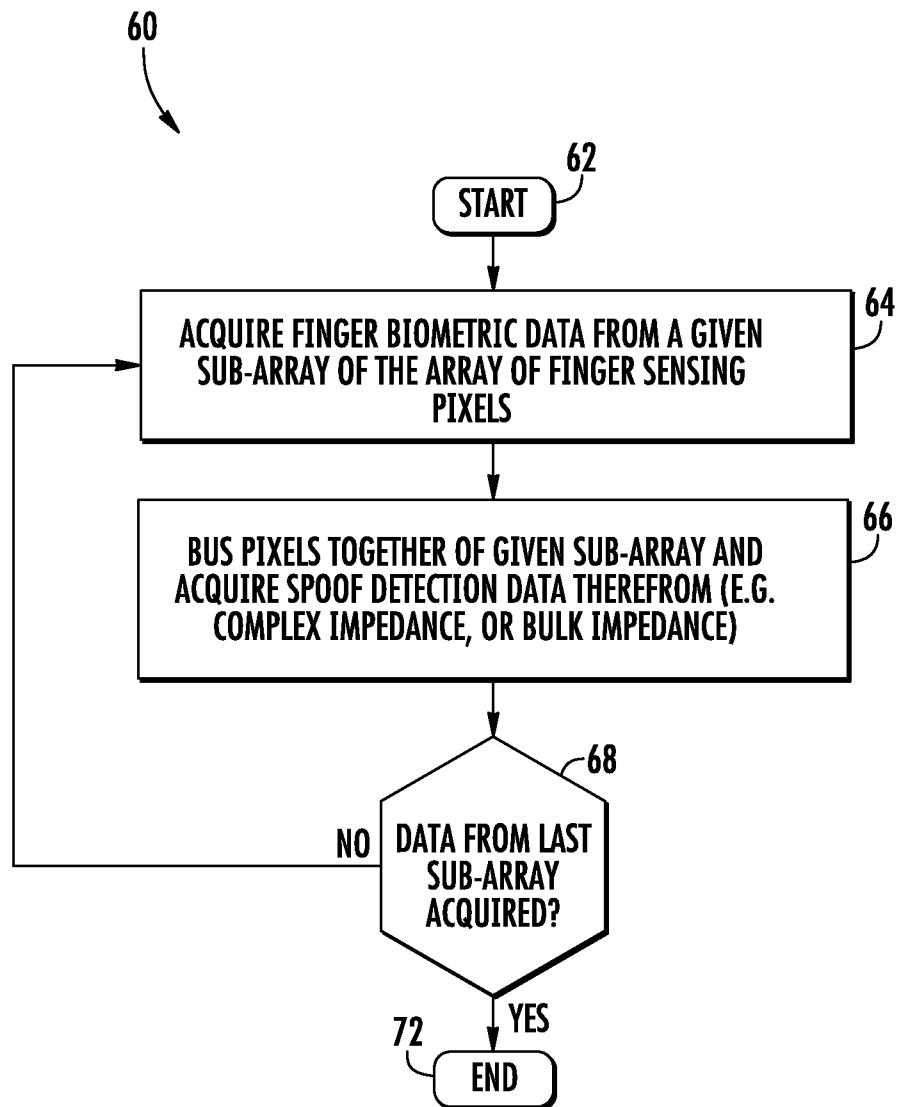


FIG. 4

INTERNATIONAL SEARCH REPORT

International application No
PCT/US2014/020123

A. CLASSIFICATION OF SUBJECT MATTER
INV. G06K9/00
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)
G06K G06F A61B

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

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	US 2006/115128 A1 (MAINGUET JEAN-FRANCOIS [FR]) 1 June 2006 (2006-06-01)	1,7,9, 10,18,22
Y	paragraphs [0002] - [0004] paragraphs [0011], [0012] paragraphs [0016], [0026] paragraphs [0042] - [0055] figure 5	2-6,8, 11-17, 19-21
Y	----- EP 1 678 655 A1 (AUTHENTEC INC [US]) 12 July 2006 (2006-07-12) paragraphs [0003] - [0005] paragraphs [0026] - [0029] paragraphs [0039], [0054], [0057] ----- -/-	2-6,8, 11-17, 19-21



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

12 June 2014

Date of mailing of the international search report

23/06/2014

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

Hermes, Lothar

INTERNATIONAL SEARCH REPORT

International application No

PCT/US2014/020123

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 5 953 441 A (SETLAK DALE R [US]) 14 September 1999 (1999-09-14) cited in the application column 4, lines 27-67 column 9, line 42 - column 10, line 15 -----	4-6,8, 13-15, 20,21

INTERNATIONAL SEARCH REPORT

Information on patent family members

International application No

PCT/US2014/020123

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
US 2006115128	A1	01-06-2006	CA 2513412 A1 12-08-2004
			CN 1777896 A 24-05-2006
			EP 1586074 A1 19-10-2005
			FR 2850190 A1 23-07-2004
			JP 2006518068 A 03-08-2006
			KR 20050096142 A 05-10-2005
			US 2006115128 A1 01-06-2006
			WO 2004068394 A1 12-08-2004
EP 1678655	A1	12-07-2006	CN 1882951 A 20-12-2006
			EP 1678655 A1 12-07-2006
			US 2005110103 A1 26-05-2005
			WO 2005031636 A1 07-04-2005
US 5953441	A	14-09-1999	NONE