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

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
31 August 2017 (31.08.2017)

WIPO | PCT

(10) International Publication Number
WO 2017/144768 A1

(51) International Patent Classification:
A61B 5/0404 (2006.01) *H04L 9/32* (2006.01)
A61B 5/00 (2006.01) *G06F 21/32* (2013.01)
H04L 29/06 (2006.01) *G06K 9/00* (2006.01)

(21) International Application Number:
PCT/FI2016/050124

(22) International Filing Date:
26 February 2016 (26.02.2016)

(25) Filing Language: English

(26) Publication Language: English

(71) Applicant: **NOKIA TECHNOLOGIES OY** [FI/FI]; Karaportti 3, 02610 Espoo (FI).

(72) Inventors: **MARTIN-LÓPEZ, Enrique**; 22b Carlyle Road, Cambridge CB4 3NDN (GB). **LI, Hongwei**; 42 Green End Road, Cambridge CB4 1RY (GB).

(74) Agent: **SEPPO LAINE OY**; Itämerenkatu 3 A, 00180 Helsinki (FI).

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

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

[Continued on next page]

(54) Title: BEHAVIOURAL BIOMETRIC AUTHENTICATION

(57) Abstract: According to an example aspect of the present invention, there is provided an apparatus comprising a memory configure to store feature data characterizing a signature gesture, at least one processing core configured to determine whether a set of sensor data corresponds to the feature data, the determination being based, at least partly, on a reliability threshold, and wherein the at least one processing core is configured to select the reliability threshold at least partly in dependence of at least one ancillary authentication mechanism, wherein the at least one processing core is configured to select the reliability threshold as less strict responsive to the at least one ancillary authentication mechanism being applicable.

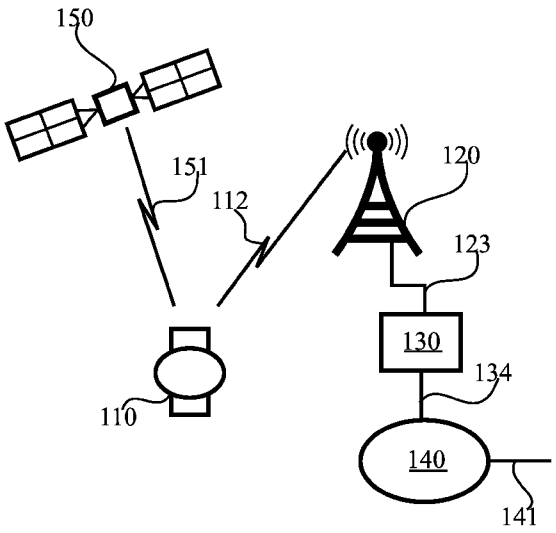

FIGURE 1

WO 2017/144768 A1

Declarations under Rule 4.17:

— *of inventorship (Rule 4.17(iv))*

Published:

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

BEHAVIOURAL BIOMETRIC AUTHENTICATION

FIELD

[0001] The present invention relates to the field of behavioural and/or biometric authentication, such as, for example, authentication based on acceleration sensor and/or gyroscope data from characteristic movements of an individual.

BACKGROUND

[0002] Authenticating a user or client may take a number of forms, depending on the circumstances. A bank may request a client to present a passport before offering services, and subsequently the bank may rely on authentication methods derived from the initial authentication, where a passport was presented. For example, when providing online service, the bank may request the client to enter a one-time numeric code from one-time pad authentication response material provided to the client when she was present in the bank. The online transaction may further be authenticated and secured by use of a secured communication protocol, such as HTTPS, for example. HTTPS uses cryptographic certificates to authenticate at least the server side, and in variants, also the client side.

[0003] In legal documents, a handwritten signature is often used as an authentication method. In some jurisdictions, a signature transmitted over telefax is also considered legally valid. Credit card transactions, previously authenticated by handwritten signature, are now authenticated using a two-factor authentication method wherein the client presents a credit card with a cryptographic chip, and then enters a secret numerical code to cause the transaction to proceed. Such a two-factor authentication is seen as more secure than a handwritten signature, in part since the reverse side of a credit card often has a genuine handwritten signature a thief can emulate.

[0004] Biometric authentication is used in machine-readable passports. For example, a passport may be furnished with a machine-readable image of the passport holder's face and/or fingerprints, which may be compared in a passport control point against a freshly obtained machine-readable image of a person's face and/or fingerprints, who presents the passport as her own.

[0005] Biometric information is more difficult, although not impossible, to copy in a bid to fraudulently compromise an authentication process. For example, while a pin code of a credit card may be surreptitiously observed when the client uses the card, her fingerprints are more difficult to obtain, and replicating her iris pattern is more difficult still. Behavioural biometric authentication may be even more difficult to replicate than certain forms of physical biometric authentication, such as fingerprints. Moreover, if compromised, a behavioural gesture could be replaced by another one, whereas a physical biometric would become useless.

SUMMARY OF THE INVENTION

[0006] The invention is defined by the features of the independent claims. Some specific embodiments are defined in the dependent claims.

[0007] According to a first aspect of the present invention, there is provided an apparatus comprising a memory configure to store feature data characterizing a signature gesture, at least one processing core configured to determine whether a set of sensor data corresponds to the feature data, the determination being based, at least partly, on a reliability threshold, and wherein the at least one processing core is configured to select the reliability threshold at least partly in dependence of at least one ancillary authentication mechanism, wherein the at least one processing core is configured to select the reliability threshold as less strict responsive to the at least one ancillary authentication mechanism being applicable.

[0008] Various embodiments of the first aspect may comprise at least one feature from the following bulleted list:

- the at least one processing core is configured to modify the feature data using the set of sensor data responsive to a determination the set corresponds to the feature data in accordance with the less strict reliability threshold
- the at least one ancillary authentication mechanism comprises that a continuous flow of data has been obtained since a reliable past event

- the continuous flow of data is a continuous flow of biometric data concerning a user and the reliable past event comprises a pairing of a wrist-wearable device with a data sink device
- the biometric data concerning the user comprises at least one of the following: a heart rate, a skin temperature and a galvanic skin response
- the continuous flow of data comprises a flow of sensor data, and the reliable past event comprises a pairing of a wrist-wearable device with a data sink device
- the apparatus is configured to obtain positive training data and negative training data, and to derive the feature data characterizing the signature based at least partly on the positive training data and negative training data
- the positive training data comprises acceleration sensor data characterizing a plurality of repetitions of the signature gesture and the negative training data comprises acceleration sensor data characterizing a plurality of gestures that do not comprise performing the signature gesture
- the at least one processing core is configured to determine whether the set of sensor data corresponds to the feature data by using at least one of a linear regression classifier, a support vector machine and a neural network
- the feature data comprises acceleration sensor data and angular velocity sensor data
- at least one of the acceleration sensor data comprises three axis acceleration sensor data and the angular velocity sensor data comprises three axis angular velocity sensor data
- the at least one processing core is configured to, in connection with the deriving of the feature data characterizing the signature, obtain derived sensor data describing trends in the positive training data

[0009] According to a second aspect of the present invention, there is provided a method comprising storing feature data characterizing a signature gesture, determining whether a set of sensor data corresponds to the feature data, the determination being based, at least partly, on a reliability threshold, and selecting the reliability threshold at least partly in dependence of at least one ancillary authentication mechanism, wherein a less strict reliability threshold is selected responsive to the at least one ancillary authentication mechanism being applicable.

[0010] Various embodiments of the second aspect may comprise at least one feature from the following bulleted list:

- modifying the feature data using the set of sensor data responsive to a determination the set corresponds to the feature data in accordance with the less strict reliability threshold
- the at least one ancillary authentication mechanism comprises that a continuous flow of data has been obtained since a reliable past event
- the continuous flow of data is a continuous flow of biometric data concerning a user and the reliable past event comprises a pairing of a wrist-wearable device with a data sink device
- the biometric data concerning the user comprises at least one of the following: a heart rate, a skin temperature and a galvanic skin response
- the continuous flow of data comprises a flow of sensor data, and the reliable past event comprises a pairing of a wrist-wearable device with a data sink device
- obtaining positive training data and negative training data, and deriving the feature data characterizing the signature gesture based at least partly on the positive training data and negative training data
- the positive training data comprises acceleration sensor data characterizing a plurality of repetitions of the signature gesture and the negative training data comprises acceleration sensor data characterizing a plurality of gestures that do not comprise performing the signature gesture
- determining whether the set of sensor data corresponds to the feature data by using at least one of a linear regression classifier, a support vector machine and a neural network
- the feature data comprises acceleration sensor data and angular velocity sensor data
- at least one of the acceleration sensor data comprises three axis acceleration sensor data and the angular velocity sensor data comprises three axis angular velocity sensor data
- in connection with the deriving of the feature data characterizing the signature, obtaining derived sensor data describing trends in the positive training data.

[0011] According to a third aspect of the present invention, there is provided an apparatus comprising means for storing feature data characterizing a signature gesture, means for determining whether a set of sensor data corresponds to the feature data, the determination being based, at least partly, on a reliability threshold, and means for selecting the reliability threshold at least partly in dependence of at least one ancillary

authentication mechanism, wherein a less strict reliability threshold is selected responsive to the at least one ancillary authentication mechanism being applicable.

[0012] According to a fourth aspect of the present invention, there is provided a non-transitory computer readable medium having stored thereon a set of computer readable instructions that, when executed by at least one processor, cause an apparatus to at least store feature data characterizing a signature gesture, determine whether a set of sensor data corresponds to the feature data, the determination being based, at least partly, on a reliability threshold, and select the reliability threshold at least partly in dependence of at least one ancillary authentication mechanism, wherein a less strict reliability threshold is selected responsive to the at least one ancillary authentication mechanism being applicable.

[0013] According to a fifth aspect of the present invention, there is provided a computer program configured to cause a method in accordance with the second aspect to be performed.

BRIEF DESCRIPTION OF THE DRAWINGS

[0014] FIGURE 1 illustrates an example system in accordance with at least some embodiments of the present invention;

[0015] FIGURE 2 illustrates an example system in accordance with at least some embodiments of the present invention;

[0016] FIGURE 3 illustrates an example apparatus capable of supporting at least some embodiments of the present invention;

[0017] FIGURE 4 illustrates signalling in accordance with at least some embodiments of the present invention, and

[0018] FIGURE 5 is a flow graph of a method in accordance with at least some embodiments of the present invention.

EMBODIMENTS

[0019] By selecting a reliability threshold for a determination whether a gesture corresponds to a correct signature gesture, confidence in gesture based authentication may be enhanced while simultaneously enabling use of the gesture based authentication for actual transactions. The reliability threshold may be selected in dependence of ancillary authentication mechanisms, such that when at least one ancillary authentication mechanism is present, a reliability threshold for the gesture-based authentication is less strict than when no ancillary authentication mechanism is available. In other words, when authentication is based solely on gesture based authentication, a higher level of confidence the gesture is correct is required. The higher level of confidence may increase a rate of false negative results, necessitating the user to repeat the gesture. A signature gesture may comprise a gesture corresponding to writing the user's signature, or it may be a more general signature gesture the user has chosen to use in a gesture based authentication process.

[0020] FIGURE 1 illustrates an example system in accordance with at least some embodiments of the present invention. FIGURE 1 illustrates a system in accordance with at least some embodiments of the present invention. The system comprises device 110, which may comprise, for example, a smart watch, digital watch, activity bracelet, smart ring or another kind of suitable device. Device 110 may comprises at least one of an acceleration sensor and an angular velocity sensor. Such an acceleration sensor may be configured to measure acceleration along three orthogonal axes. Such an angular velocity sensor may be configured to measure angular velocity along three orthogonal angles, for example. In general, device 110 may be wrist-wearable or finger-wearable. An angular velocity sensor may comprise a gyro sensor, for example. Accelerometers may be based on piezoelectric, piezoresistive or capacitive technology, for example.

[0021] When worn by a user on a hand that is used to sign, that is, perform a signature gesture, the sensor arrangement comprised in device 110 may obtain sensor data characterizing the gesture of signing. The gesture may be performed on a surface, akin to signing on paper, or the gesture may be performed in the air. In general, the sensor data obtained, by sensors in device 110, during the gesture may be referred to as a set of sensor data. The set may comprise acceleration sensor data and/or angular velocity sensor data. The acceleration sensor data may comprise three separate sequences of sensor data values, each sequence corresponding to a distinct axis. Likewise, angular velocity sensor data may

comprise three separate sequences, each sequence corresponding to a distinct base angle, the base angles being orthogonal to each other.

[0022] Device 110 may be communicatively coupled with a communications network. For example, in FIGURE 1 device 110 is coupled, via wireless link 112, with base station 120. Base station 120 may comprise a cellular or non-cellular base station, wherein a non-cellular base station may be referred to as an access point. Examples of cellular technologies include wideband code division multiple access, WCDMA, and long term evolution, LTE, while examples of non-cellular technologies include wireless local area network, WLAN, and worldwide interoperability for microwave access, WiMAX. Base station 120 may be coupled with network node 130 via connection 123. Connection 123 may be a wire-line connection, for example. Network node 130 may comprise, for example, a controller or gateway device. Network node 130 may interface, via connection 134, with network 140, which may comprise, for example, the Internet or a corporate network. Network 140 may be coupled with further networks via connection 141. In some embodiments, device 110 is not configured to couple with base station 120. Network 140 may comprise cloud-based servers, for example cloud servers that participate in transactions that are authenticated by gestures. Cloud servers may be arranged to back-up data, such as reference feature data, used in gesture-based authentication.

[0023] Device 110 may be configured to receive, from satellite constellation 150, satellite positioning information via satellite link 151. The satellite constellation may comprise, for example the global positioning system, GPS, or Galileo constellation. Satellite constellation 150 may comprise more than one satellite, although only one satellite is illustrated in FIGURE 1 for the same of clarity. Likewise, receiving the positioning information over satellite link 151 may comprise receiving data from more than one satellite. In some embodiments, a timing signal is received from satellite constellation 150 alternatively or additionally to positioning information.

[0024] In embodiments where device 110 is not enabled to receive data from a satellite constellation, device 110 may obtain positioning and/or timing information by interacting with a network in which base station 120 is comprised. For example, cellular networks may employ various ways to position a device, such as trilateration, multilateration or positioning based on an identity of a base station with which attachment is possible. Likewise a non-cellular base station, or access point, may know its own

location and provide it to device 110, enabling device 110 to position itself within communication range of this access point.

[0025] Device 110 may be configured to obtain a current time from satellite constellation 150, base station 120 or by requesting it from a user, for example. Once device 110 has the current time and an estimate of its location, device 110 may consult a look-up table, for example, to determine how much time is remaining to sunset, and/or sunrise. Device 110 may comprise further sensors, enabled to determine, for example from skin temperature, skin galvanic response or from heart rate, whether device 110 has been worn in an uninterrupted fashion.

[0026] FIGURE 2 illustrates a system in accordance with at least some embodiments of the present invention. Like numbering denotes like structure as in FIGURE 1. FIGURE 2 embodiments comprise an auxiliary device 110x.

[0027] Device 110 may be communicatively coupled, for example communicatively paired, with an auxiliary device 110x. The communicative coupling, or pairing, is illustrated in FIGURE 2 as interface 111, which may be wireless, as illustrated, or wire-line, depending on the embodiment. Interface 111 may comprise a Bluetooth interface, for example. Auxiliary device 110x may comprise a smartphone, tablet computer or other computing device, for example. Auxiliary device 110x may comprise a device that the owner of device 110 uses to consume media, communicate or interact with applications. Auxiliary device 110x may be furnished with a larger display screen than device 110, which may make auxiliary device 110x preferable to the user when a complex interaction with an application is needed, as a larger screen enables a more detailed rendering of interaction options. Auxiliary device 110x may store feature data usable in determining if a gesture-based authentication is to be accepted or refused, for example. In some embodiments, such as those illustrated in FIGURE 1, auxiliary device 110x is absent.

[0028] In some embodiments, where auxiliary device 110x is present, device 110 may be configured to use connectivity capability of auxiliary device 110x. For example, device 110 may access a network via auxiliary device 110x. In these embodiments, device 110 need not be furnished with connectivity toward base station 120, for example, since device 110 may access network resources via interface 111 and a connection auxiliary device 110x has with base station 120. Such a connection is illustrated in FIGURE 2 as connection 112x. For example, device 110 may comprise a smart watch and auxiliary

device 110x may comprise a smartphone, which may have connectivity to cellular and/or non-cellular data networks. Likewise, in some embodiments device 110 may receive satellite positioning information, or positioning information derived therefrom, via auxiliary device 110x where device 110 lacks a satellite positioning receiver of its own. A satellite connection of auxiliary device 151x is illustrated in FIGURE 2 as connection 151X.

[0029] In some embodiments, device 110 may have some connectivity and be configured to use both that and connectivity provided by auxiliary device 110x. For example, device 110 may comprise a satellite receiver enabling device 110 to obtain satellite positioning information directly from satellite constellation 150. Device 110 may then obtain network connectivity to base station 120 via auxiliary device 110x.

[0030] To enable using sensors of device 110 in a gesture based authentication scheme, feature data characterising an authentic signature gesture may first be established. The feature data may comprise a set of reference sequences of sensor data values, corresponding to sensor data that device 110 is capable of generating during a gesture, so that freshly generated sensor data can be compared to the feature data to determine, whether the gesture corresponds to an authentic signature gesture.

[0031] The feature data may comprise, alternatively or additionally to reference sequences of sensor data, features derived from reference sequences of sensor data, which features characterize the reference sequence data. Such data may be referred to as derived sensor data. For example, first and/or second order derivatives may be obtained from the reference sequences, turning points may be identified when angular velocities or accelerations turn from positive to negative or vice versa, and/or timing characteristics of the reference sequences of sensor data may be obtained. In general, the feature data therefore comprises data that enables a determination as to what extent a freshly obtained set of sensor data corresponds to reference sensor data of genuine signature gestures. In other words, the feature data may comprise sensor data in unprocessed form, in processed form or a combination of the two.

[0032] In establishing the feature data, a user may initially be prompted to perform a number of repetitions of the correct, authentic signature gesture. For example, three, five, seven or ten repetitions may be recorded by sensors of device 110. Sensor data obtained during these repetitions may be referred to as positive training data, as the genuine

signature gesture is comprised therein. Additionally the user may be prompted to gesture in a way that does not comprise the signature gesture, again, repeatedly. Sensor data obtained during these gestures may be referred to as negative training data, as the genuine signature gesture is absent therein.

[0033] The feature data may be determined based on the positive training data, and, optionally, the negative training data as well. Where the negative training data is not used in establishing the feature data, it of course need not be collected either. The negative training data may be useful in establishing the feature data, since the user may have characteristic motion features that are present in both the genuine signature gesture and other gestures the user makes. For example, arm length, muscle tone and rhythm may be typical of the user in general, and affect characteristics of his gestures. In general, where it can be established a gesture is not even made by the correct user, it is trivial to conclude it cannot be the authentic signature gesture. The negative training data, like the positive training data, may comprise or be derived from acceleration and/or angular velocity sensor data obtained by device 110. One example of negative training data is a case where the user seeks to protect the authentication from specific people around him. For example, a parent may ask his child to perform a signature gesture, providing instructions on how it should be performed. Sensor data characterizing this gesture can be employed, in some embodiments, to help guard the authentication against unauthorized access.

[0034] Once the feature data is established, matching of a freshly generated set of sensor data against the feature data may be performed, for example in device 110 or in auxiliary device 110x. Alternatively, the matching may be performed in a cloud server that is in possession of, or has access to, the feature data. When the matching is performed in a cloud server, the set of sensor data may be provided to the server in a request, and the server may be arranged to provide a result of the matching as a response. The request may comprise an identifier of a node, where the result should be transmitted to. The request may be encrypted. The matching comprises determining, whether the set of sensor data corresponds to the feature data, that is, whether the gesture now performed is the correct signature gesture. The matching may be based on at least one of a linear regression classifier, a support vector machine, SVM, and a neural network, for example. A result of the matching may comprise a determined probability the fresh set of sensor data is from a genuine signature gesture. Where the set of sensor data very closely matches the feature data, the probability may be high, and where there are differences between the set of sensor

data and the feature data, the probability may be lower. The larger the differences are, the lower is the probability.

[0035] A decision whether to accept the fresh gesture as authentic may depend on a reliability threshold. For example, it may be required that the determined probability the set of sensor data is from a genuine signature has to be at least 0,9 or 0,95 for the gesture to be accepted as authentic. Therefore, to perform a gesture-based authentication, a user may perform the signature gesture, during which time device 110 captures a set of sensor data, which set of sensor data is then compared against the feature data, established prior, to derive a probability the two are consistent. The derived probability is then compared to the reliability threshold to decide, whether to accept the gesture authentication or to reject it.

[0036] The reliability threshold to be used in the authentication process may be selected in dependence of at least one ancillary authentication method. In detail, where an ancillary authentication method can be at least partly relied on, a less strict reliability threshold can be employed in the gesture recognition, as the compound authentication consisting of the gesture and the at least one ancillary authentication method nonetheless will satisfy also a stricter reliability threshold. In other words, when an ancillary authentication method is applicable, the gesture-based authentication method is used together with the ancillary authentication method.

[0037] For example, an ancillary authentication method may be present where a user has paired device 110 with an ancillary device 110x, and the pairing has not been broken. This may be the case, for example, where the user has caused device 110 to interact with ancillary device 110x in the morning, and then he has worn device 110, and kept ancillary device 110x with him, such that the pairing has remained unbroken. The pairing may rely on the Bluetooth protocol, for example. Auxiliary device 110x may act as a data sink device in the sense that device 110 transmits sensor data it obtains from sensors to auxiliary device 110x. The pairing may require entry of a pin code, or it may rely on a previously established trust relationship between device 110 and auxiliary device 110x.

[0038] Another example is a case, where the use has interacted with device 110, for example in a way that has required entry of a pin code, and/or a pairing, and device 110 has been worn continuously since then. For example, when device 110 has been able to measure a continuous biometric data stream, it may be determined device 110 has been worn continuously and consequently by the legitimate user. Therefore, an ancillary

authentication method is in place, since a degree of confidence can thereby be established the user is the legitimate user. Heart rate, galvanic skin response and skin temperature are examples of biometric information usable in determining device 110 has been continuously worn. In general, a continuous flow of data may be obtained since a reliable past event.

[0039] In some embodiments, biometric data is used as an ancillary authentication method in a sense, that presence of biometric data matching the user is used as a trigger to make the reliability threshold less strict. On the other hand, biometric data not matching the user may in these embodiments make the reliability threshold more strict. For example, the user may have a characteristic heart rate when at rest. In case a heart rate consistent with the characteristic heart rate is present, the less strict reliability threshold may be used, but where a heart rate inconsistent with the characteristic heart rate is present, the more strict reliability threshold may be used. For example, where the characteristic heart rate is 70 beats per minute, a reading of 95 beats per minute could be considered inconsistent with the characteristic heart rate. A combination of at least two biometric datapoints could provide a more characterizing effect than a single biometric datapoint.

[0040] One example of an ancillary authentication method is a method wherein it is verified, whether device 110 has been continually worn and a pairing of device 110 to auxiliary device 110x has been continually present since a reliable past event, such as a password or pin entry or a pairing. The verification device 110 has been continually worn may be based on biometric sensor data, as described above.

[0041] Where the reliability threshold is made less strict based on an ancillary authentication method, the reliability threshold may be once more made more strict in case the ancillary authentication method is no longer usable. For example, where a discontinuity or anomaly is detected in pairing data, or biometric data, the ancillary authentication method may be considered no longer present, as it is possible the user has taken device 110 off, for example in case he is robbed and device 110 is stolen. In this case, the threshold should return to the stricter level as the additional confidence provided by the ancillary authentication method is no longer present.

[0042] When a gesture is accepted in the presence of an ancillary authentication method, the gesture may be considered as a further element of positive training data, and used to refine the feature data, to render the gesture-based authentication method more reliable and usable. In detail, as the quantity of training data used in establishing the

feature data increases, the rate of false negatives and false positives decreases. Here a false negative may comprise a gesture that is a genuine signature gesture, but which nonetheless is rejected in the gesture authentication process. A false positive is here a gesture that is accepted despite it not being a genuine signature gesture. This has the advantage that the user may start using the gesture based authentication mechanism after initially entering a reduced quantity of training data, compared to a case where the reliability threshold were always kept at a strict level and ancillary authentication methods were not employed. Also, the proportion of gestures in the beginning, when the feature data is not yet entirely complete, in the false negative class can reduce, as the threshold is less strict. Examples of a less strict threshold are 0,6 and 0,7.

[0043] FIGURE 3 illustrates an example apparatus capable of supporting at least some embodiments of the present invention. Illustrated is device 300, which may comprise, for example, a device such as device 110 or auxiliary device 110x of FIGURE 1 or FIGURE 2. Comprised in device 300 is processor 310, which may comprise, for example, a single- or multi-core processor wherein a single-core processor comprises one processing core and a multi-core processor comprises more than one processing core. Processor 310 may comprise more than one processor. A processing core may comprise, for example, a Cortex-A8 processing core manufactured by ARM Holdings or a Steamroller processing core produced by Advanced Micro Devices Corporation. Processor 310 may comprise at least one Qualcomm Snapdragon and/or Intel Atom processor. Processor 310 may comprise at least one application-specific integrated circuit, ASIC. Processor 310 may comprise at least one field-programmable gate array, FPGA. Processor 310 may be means for performing method steps in device 300. Processor 310 may be configured, at least in part by computer instructions, to perform actions.

[0044] Device 300 may comprise memory 320. Memory 320 may comprise random-access memory and/or permanent memory. Memory 320 may comprise at least one RAM chip. Memory 320 may comprise solid-state, magnetic, optical and/or holographic memory, for example. Memory 320 may be at least in part accessible to processor 310. Memory 320 may be at least in part comprised in processor 310. Memory 320 may be means for storing information. Memory 320 may comprise computer instructions that processor 310 is configured to execute. When computer instructions configured to cause processor 310 to perform certain actions are stored in memory 320, and device 300 overall is configured to run under the direction of processor 310 using computer instructions from

memory 320, processor 310 and/or its at least one processing core may be considered to be configured to perform said certain actions. Memory 320 may be at least in part comprised in processor 310. Memory 320 may be at least in part external to device 300 but accessible to device 300.

[0045] Device 300 may comprise a transmitter 330. Device 300 may comprise a receiver 340. Transmitter 330 and receiver 340 may be configured to transmit and receive, respectively, information in accordance with at least one cellular or non-cellular standard. Transmitter 330 may comprise more than one transmitter. Receiver 340 may comprise more than one receiver. Transmitter 330 and/or receiver 340 may be configured to operate in accordance with global system for mobile communication, GSM, wideband code division multiple access, WCDMA, long term evolution, LTE, IS-95, wireless local area network, WLAN, Ethernet and/or worldwide interoperability for microwave access, WiMAX, standards, for example.

[0046] Device 300 may comprise a near-field communication, NFC, transceiver 350. NFC transceiver 350 may support at least one NFC technology, such as NFC, Bluetooth, Wibree or similar technologies.

[0047] Device 300 may comprise user interface, UI, 360. UI 360 may comprise at least one of a display, a keyboard, a touchscreen, a vibrator arranged to signal to a user by causing device 300 to vibrate, a speaker and a microphone. A user may be able to operate device 300 via UI 360, for example to cause pairings to occur, to enter pin codes and/or to participate in gesture based authentication.

[0048] Device 300 may comprise or be arranged to accept a user identity module 370. User identity module 370 may comprise, for example, a subscriber identity module, SIM, card installable in device 300. A user identity module 370 may comprise information identifying a subscription of a user of device 300. A user identity module 370 may comprise cryptographic information usable to verify the identity of a user of device 300 and/or to facilitate encryption of communicated information and billing of the user of device 300 for communication effected via device 300.

[0049] Processor 310 may be furnished with a transmitter arranged to output information from processor 310, via electrical leads internal to device 300, to other devices comprised in device 300. Such a transmitter may comprise a serial bus transmitter arranged

to, for example, output information via at least one electrical lead to memory 320 for storage therein. Alternatively to a serial bus, the transmitter may comprise a parallel bus transmitter. Likewise processor 310 may comprise a receiver arranged to receive information in processor 310, via electrical leads internal to device 300, from other devices comprised in device 300. Such a receiver may comprise a serial bus receiver arranged to, for example, receive information via at least one electrical lead from receiver 340 for processing in processor 310. Alternatively to a serial bus, the receiver may comprise a parallel bus receiver.

[0050] Device 300 may comprise further devices not illustrated in FIGURE 3. For example, where device 300 comprises a smartphone, it may comprise at least one digital camera. Some devices 300 may comprise a back-facing camera and a front-facing camera, wherein the back-facing camera may be intended for digital photography and the front-facing camera for video telephony. Device 300 may comprise a fingerprint sensor arranged to authenticate, at least in part, a user of device 300. In some embodiments, device 300 lacks at least one device described above. For example, some devices 300 may lack a NFC transceiver 350 and/or user identity module 370.

[0051] Processor 310, memory 320, transmitter 330, receiver 340, NFC transceiver 350, UI 360 and/or user identity module 370 may be interconnected by electrical leads internal to device 300 in a multitude of different ways. For example, each of the aforementioned devices may be separately connected to a master bus internal to device 300, to allow for the devices to exchange information. However, as the skilled person will appreciate, this is only one example and depending on the embodiment various ways of interconnecting at least two of the aforementioned devices may be selected without departing from the scope of the present invention.

[0052] FIGURE 4 illustrates signalling in accordance with at least some embodiments of the present invention. On the vertical axes are disposed, from the left, devices 110 and 110x of FIGURE 2, and finally on the right, correspondent node 400. Time advances from the top toward the bottom.

[0053] In phase 410, device 110 is worn by the user, and in phase 420 a pairing is established between device 110 and auxiliary device 110x. Heartbeat packets and/or biometric data may be transmitted over the pairing, for example. In phase 430, auxiliary

device 110x modifies the reliability threshold to a less strict level, since the pairing has occurred and has not been interrupted.

[0054] In phase 440, the user interacts with correspondent node 400, which may comprise, for example, a media store. The user may request to download the contents of a current newspaper edition to auxiliary device 110x, for example. As the contents are subject to payment, correspondent node 400 requests payment from auxiliary device 110x. Responsively, auxiliary device 110x, being in possession of payment credentials, requests the user to accept the transaction by providing the gesture authentication, to thereby accept the charge.

[0055] In phase 450, the user performs the signature gesture, which is recorded by sensors of device 110, to thereby obtain a set of sensor data. The set of sensor data is provided to auxiliary device 110x in phase 460. In phase 470, auxiliary device 110x determines, whether the set of sensor data corresponds to the feature data, established earlier. In phase 470, auxiliary device 110x may determine whether the pairing of phase 420 remains in place uninterrupted, and responsive to this being the case, a less strict reliability threshold may be applied in performing the determination as to whether the set of sensor data corresponds to the feature data. In case the pairing has been interrupted, the more strict reliability threshold may be used in the determination of phase 470. In case the less strict threshold is used and the set of sensor data is found to correspond to the feature data in accordance with this less strict threshold, the feature data may be enhanced with the set of sensor data, wherein the set of sensor data is used as positive training data.

[0056] In the example of FIGURE 4, the authentication succeeds, and responsively auxiliary device 110x obtains the requested content from correspondent node 400. In some embodiments, the determination, whether the set of sensor data corresponds to the feature data may be performed in device 110, rather than in auxiliary device 110x, as illustrated in FIGURE 4.

[0057] FIGURE 5 is a flow graph of a method in accordance with at least some embodiments of the present invention. The phases of the illustrated method may be performed in device 110, an auxiliary device 110x or a personal computer, for example, or in a control device configured to control the functioning thereof, when implanted therein.

[0058] Phase 510 comprises storing feature data characterizing a signature gesture. The stored feature data may comprise at least a part of the overall feature data. Phase 520 comprises determining whether a set of sensor data corresponds to the feature data, the determination being based, at least partly, on a reliability threshold. Finally, phase 530 comprises selecting the reliability threshold at least partly in dependence of at least one ancillary authentication mechanism, wherein a less strict reliability threshold is selected responsive to the at least one ancillary authentication mechanism being applicable. Phase 530 may precede phase 520, such that the selected reliability threshold is used in the determination of phase 520. The storing of phase 510 may comprise storing the feature data in encrypted form, for example. Alternatively or additionally, the storing of phase 510 may comprise storing an encrypted form of a classifier function.

[0059] It is to be understood that the embodiments of the invention disclosed are not limited to the particular structures, process steps, or materials disclosed herein, but are extended to equivalents thereof as would be recognized by those ordinarily skilled in the relevant arts. It should also be understood that terminology employed herein is used for the purpose of describing particular embodiments only and is not intended to be limiting.

[0060] Reference throughout this specification to one embodiment or an embodiment means that a particular feature, structure, or characteristic described in connection with the embodiment is included in at least one embodiment of the present invention. Thus, appearances of the phrases “in one embodiment” or “in an embodiment” in various places throughout this specification are not necessarily all referring to the same embodiment. Where reference is made to a numerical value using a term such as, for example, about or substantially, the exact numerical value is also disclosed.

[0061] As used herein, a plurality of items, structural elements, compositional elements, and/or materials may be presented in a common list for convenience. However, these lists should be construed as though each member of the list is individually identified as a separate and unique member. Thus, no individual member of such list should be construed as a de facto equivalent of any other member of the same list solely based on their presentation in a common group without indications to the contrary. In addition, various embodiments and example of the present invention may be referred to herein along with alternatives for the various components thereof. It is understood that such embodiments, examples, and alternatives are not to be construed as de facto equivalents of one another, but are to be considered as separate and autonomous representations of the

present invention.

[0062] Furthermore, the described features, structures, or characteristics may be combined in any suitable manner in one or more embodiments. In the preceding description, numerous specific details are provided, such as examples of lengths, widths, shapes, etc., to provide a thorough understanding of embodiments of the invention. One skilled in the relevant art will recognize, however, that the invention can be practiced without one or more of the specific details, or with other methods, components, materials, etc. In other instances, well-known structures, materials, or operations are not shown or described in detail to avoid obscuring aspects of the invention.

[0063] While the forgoing examples are illustrative of the principles of the present invention in one or more particular applications, it will be apparent to those of ordinary skill in the art that numerous modifications in form, usage and details of implementation can be made without the exercise of inventive faculty, and without departing from the principles and concepts of the invention. Accordingly, it is not intended that the invention be limited, except as by the claims set forth below.

[0064] The verbs “to comprise” and “to include” are used in this document as open limitations that neither exclude nor require the existence of also un-recited features. The features recited in depending claims are mutually freely combinable unless otherwise explicitly stated. Furthermore, it is to be understood that the use of "a" or "an", that is, a singular form, throughout this document does not exclude a plurality.

INDUSTRIAL APPLICABILITY

[0065] At least some embodiments of the present invention find industrial application in gesture based authentication, in enhancing information security.

ACRONYMS LIST

GPS	Global positioning system
HTTPS	hypertext transfer protocol over TLS
LTE	Long term evolution
TLS	transport layer security
UI	User interface

WCDMA	Wideband code division multiple access
WiMAX	Worldwide interoperability for microwave access
WLAN	Wireless local area network

REFERENCE SIGNS LIST

110	Device
110x	Auxiliary device
120	Base station
130	Network node
140	Network
150	Satellite constellation
310 - 370	Elements of FIGURE 3
410 – 480	Phases of the signalling illustrated in FIGURE 4
510 - 530	Phases of the method of FIGURE 5

CLAIMS:

1. An apparatus comprising:
   - a memory configured to store feature data characterizing a signature gesture;
   - at least one processing core configured to determine whether a set of sensor data corresponds to the feature data, the determination being based, at least partly, on a reliability threshold, and
   - wherein the at least one processing core is configured to select the reliability threshold at least partly in dependence of at least one ancillary authentication mechanism, wherein the at least one processing core is configured to select the reliability threshold as less strict responsive to the at least one ancillary authentication mechanism being applicable.

2. The apparatus according to claim 1, wherein the at least one processing core is configured to modify the feature data using the set of sensor data responsive to a determination the set corresponds to the feature data in accordance with the less strict reliability threshold.

3. The apparatus according to claim 1 or 2, wherein the at least one ancillary authentication mechanism comprises that a continuous flow of data has been obtained since a reliable past event.

4. The apparatus according to claim 3, wherein the continuous flow of data is a continuous flow of biometric data concerning a user and the reliable past event comprises a pairing of a wrist-wearable device with a data sink device.

5. The apparatus according to claim 4, wherein the biometric data concerning the user comprises at least one of the following: a heart rate, a skin temperature and a galvanic skin response.

6. The apparatus according to claim 3, wherein the continuous flow of data comprises a flow of sensor data, and the reliable past event comprises a pairing of a wrist-wearable device with a data sink device.

7. The apparatus according to any preceding claim, wherein the apparatus is configured to obtain positive training data and negative training data, and to derive the feature data characterizing the signature based at least partly on the positive training data and negative training data.

8. The apparatus according to claim 7, wherein the positive training data comprises acceleration sensor data characterizing a plurality of repetitions of the signature gesture and the negative training data comprises acceleration sensor data characterizing a plurality of gestures that do not comprise performing the signature gesture.

9. The apparatus according to any of claims 1 – 8, wherein the at least one processing core is configured to determine whether the set of sensor data corresponds to the feature data by using at least one of a linear regression classifier, a support vector machine and a neural network.

10. The apparatus according to any of claims 1 – 9, wherein the feature data comprises acceleration sensor data and angular velocity sensor data.

11. The apparatus according to claim 10, wherein at least one of the acceleration sensor data comprises three axis acceleration sensor data and the angular velocity sensor data comprises three axis angular velocity sensor data.

12. The apparatus according to any of claims 7 – 11, wherein the at least one processing core is configured to, in connection with the deriving of the feature data characterizing the signature, obtain derived sensor data describing trends in the positive training data.

13. A method comprising:

- storing feature data characterizing a signature gesture;
- determining whether a set of sensor data corresponds to the feature data, the determination being based, at least partly, on a reliability threshold, and
- selecting the reliability threshold at least partly in dependence of at least one ancillary authentication mechanism, wherein a less strict reliability threshold is selected responsive to the at least one ancillary authentication mechanism being applicable.

14. The method according to claim 13, further comprising modifying the feature data using the set of sensor data responsive to a determination the set corresponds to the feature data in accordance with the less strict reliability threshold.

15. The method according to claim 13 or 4, wherein the at least one ancillary authentication mechanism comprises that a continuous flow of data has been obtained since a reliable past event.

16. The method according to claim 15, wherein the continuous flow of data is a continuous flow of biometric data concerning a user and the reliable past event comprises a pairing of a wrist-wearable device with a data sink device.

17. The method according to claim 16, wherein the biometric data concerning the user comprises at least one of the following: a heart rate, a skin temperature and a galvanic skin response.

18. The method according to claim 15, wherein the continuous flow of data comprises a flow of sensor data, and the reliable past event comprises a pairing of a wrist-wearable device with a data sink device.

19. The method according to any of claims 13 - 18, further comprising obtaining positive training data and negative training data, and deriving the feature data characterizing the signature gesture based at least partly on the positive training data and negative training data.

20. The method according to claim 19, wherein the positive training data comprises acceleration sensor data characterizing a plurality of repetitions of the signature gesture and the negative training data comprises acceleration sensor data characterizing a plurality of gestures that do not comprise performing the signature gesture.

21. The method according to any of claims 13 – 20, further comprising determining whether the set of sensor data corresponds to the feature data by using at least one of a linear regression classifier, a support vector machine and a neural network.

22. The method according to any of claims 13 – 21, wherein the feature data comprises acceleration sensor data and angular velocity sensor data.

23. The method according to claim 22, wherein at least one of the acceleration sensor data comprises three axis acceleration sensor data and the angular velocity sensor data comprises three axis angular velocity sensor data.

24. The method according to any of claims 19 – 23, further comprising, in connection with the deriving of the feature data characterizing the signature, obtaining derived sensor data describing trends in the positive training data.

25. An apparatus comprising:

- means for storing feature data characterizing a signature gesture ;
- means for determining whether a set of sensor data corresponds to the feature data, the determination being based, at least partly, on a reliability threshold, and
- means for selecting the reliability threshold at least partly in dependence of at least one ancillary authentication mechanism, wherein a less strict reliability threshold is selected responsive to the at least one ancillary authentication mechanism being applicable.

26. A non-transitory computer readable medium having stored thereon a set of computer readable instructions that, when executed by at least one processor, cause an apparatus to at least:

- store feature data characterizing a signature gesture;
- determine whether a set of sensor data corresponds to the feature data, the determination being based, at least partly, on a reliability threshold, and
- select the reliability threshold at least partly in dependence of at least one ancillary authentication mechanism, wherein a less strict reliability threshold is selected responsive to the at least one ancillary authentication mechanism being applicable.

27. A computer program configured to cause a method in accordance with at least one of claims 13 –24 to be performed.

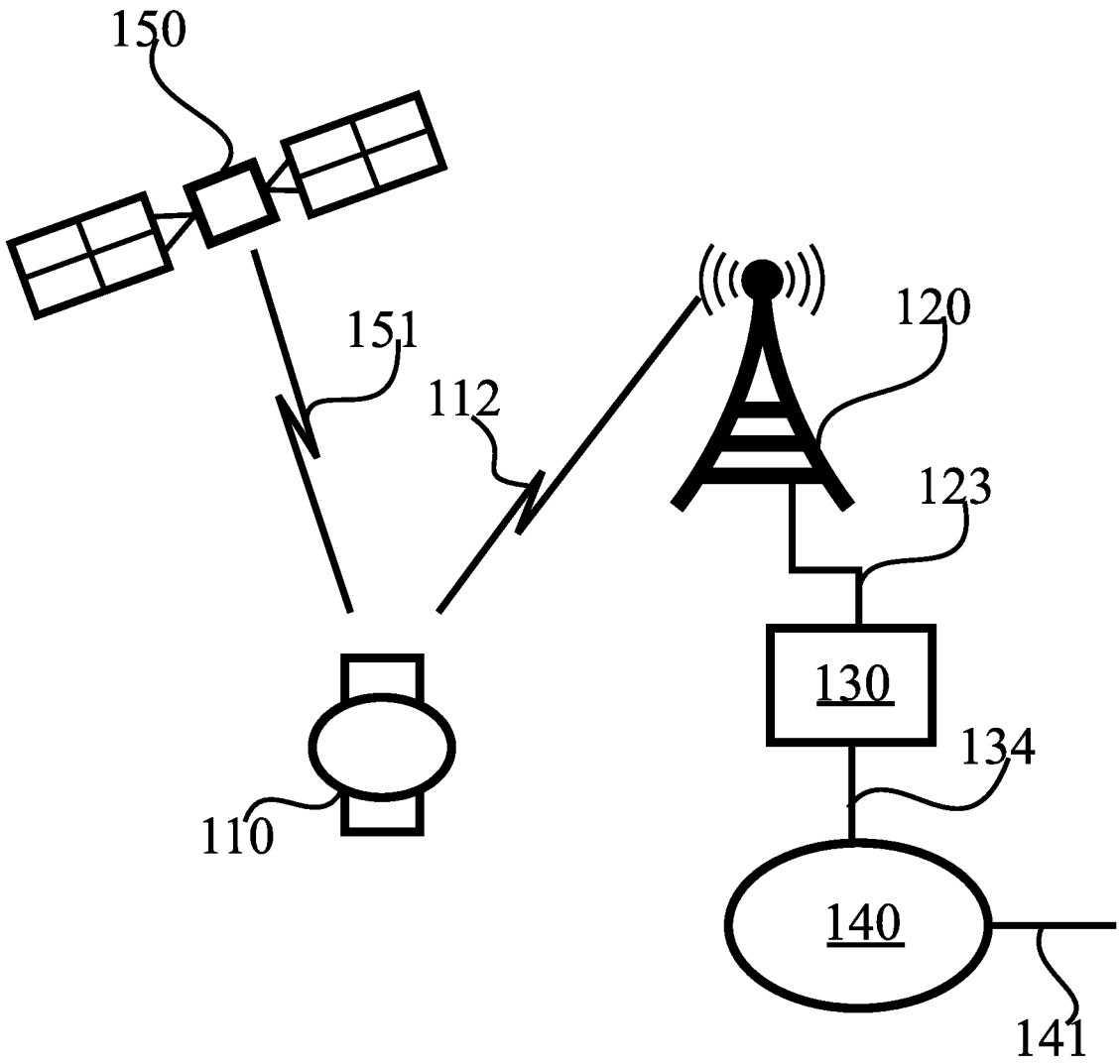

FIGURE 1

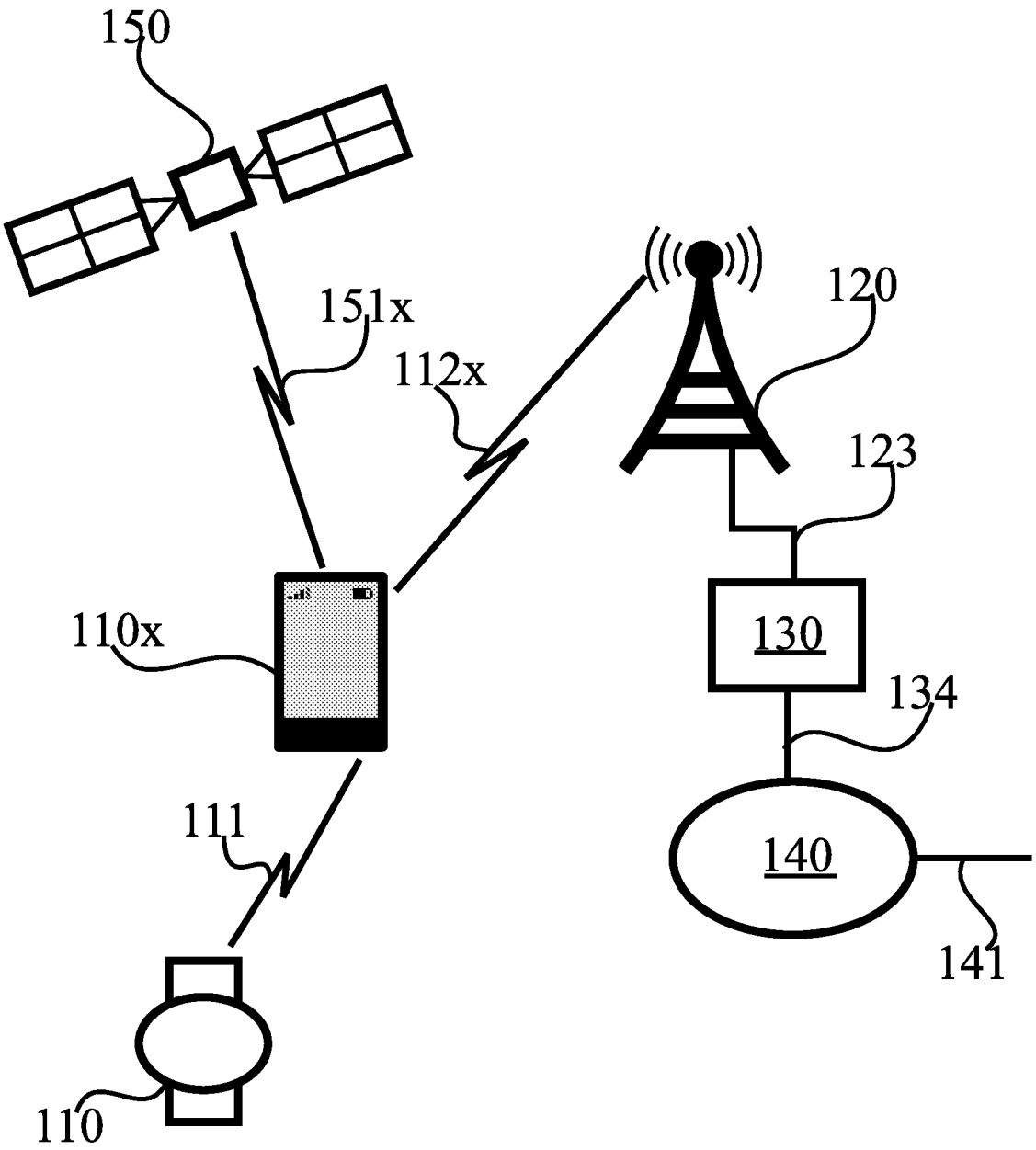

FIGURE 2

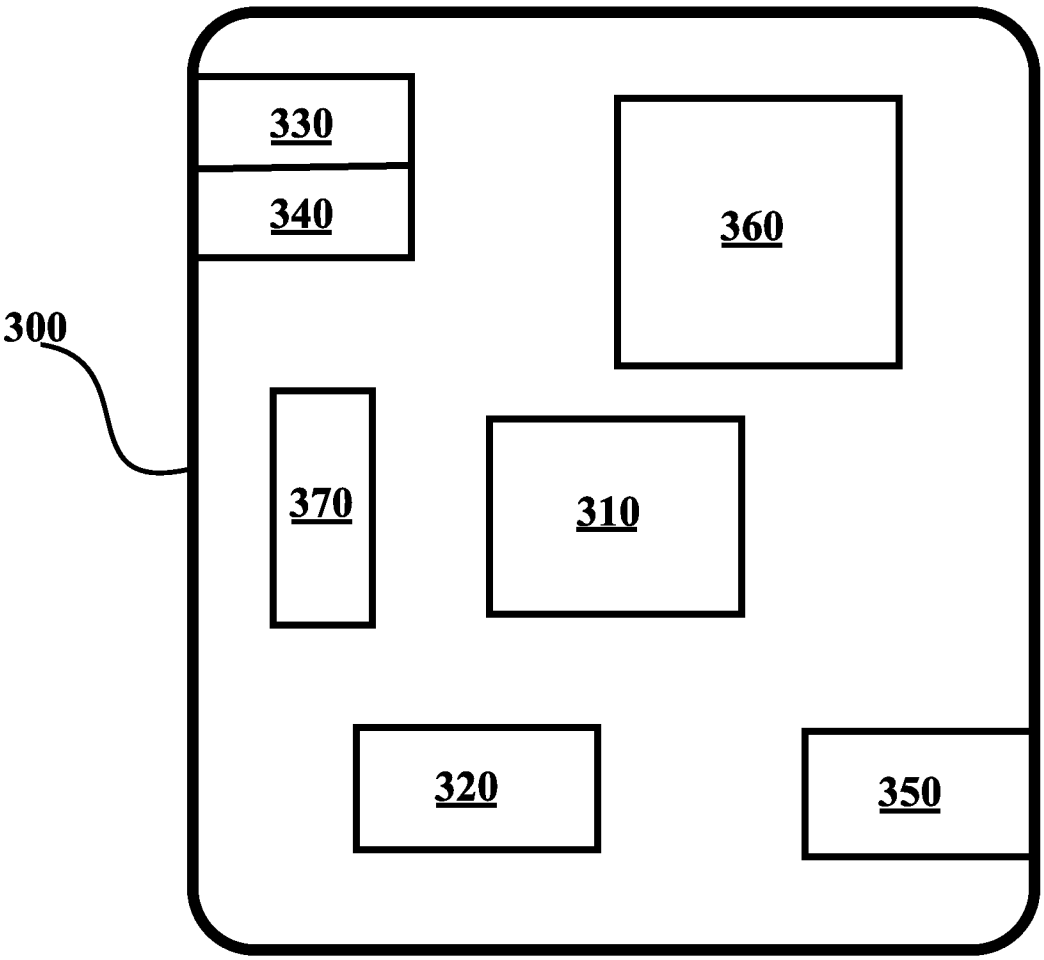

FIGURE 3

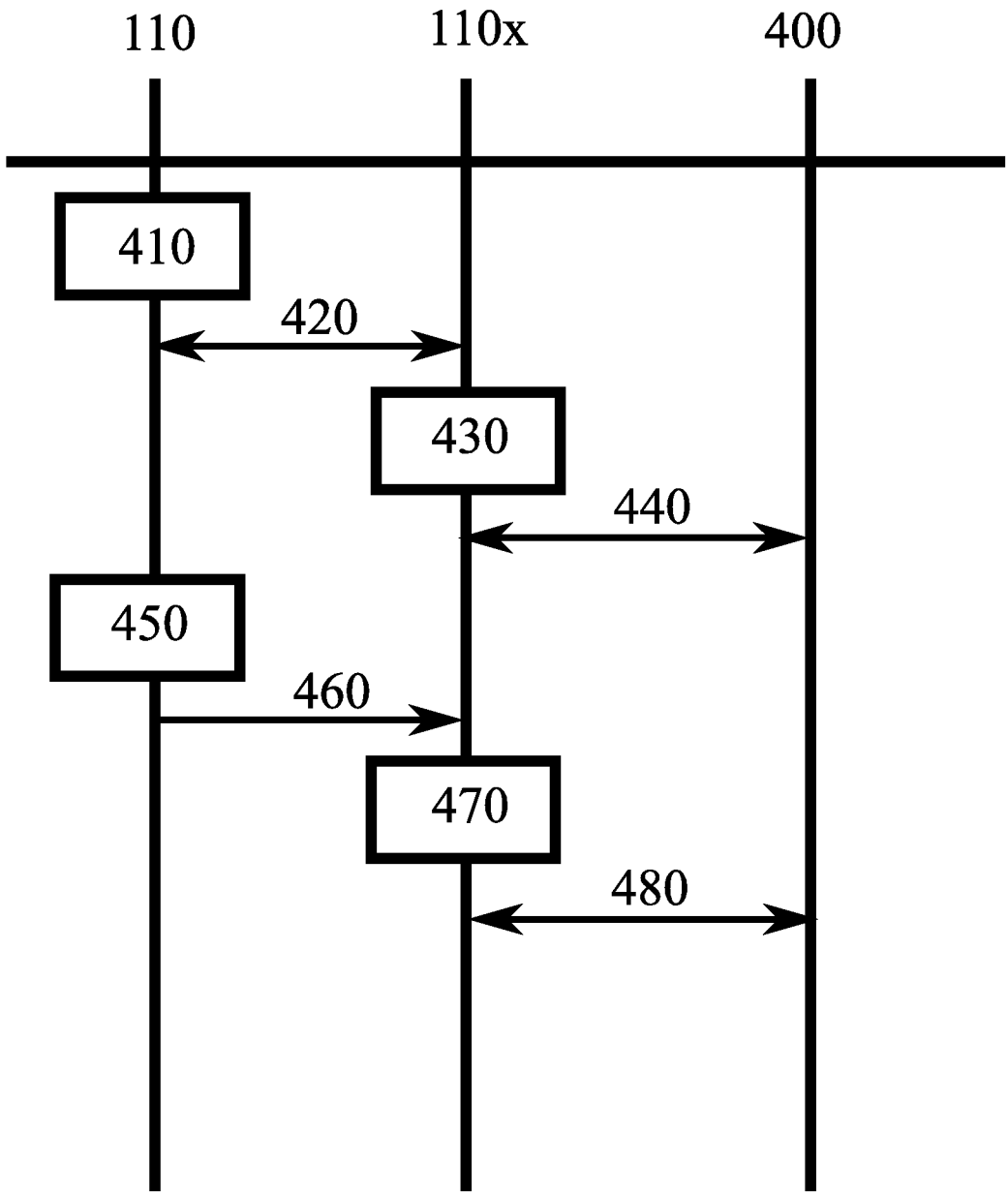

FIGURE 4

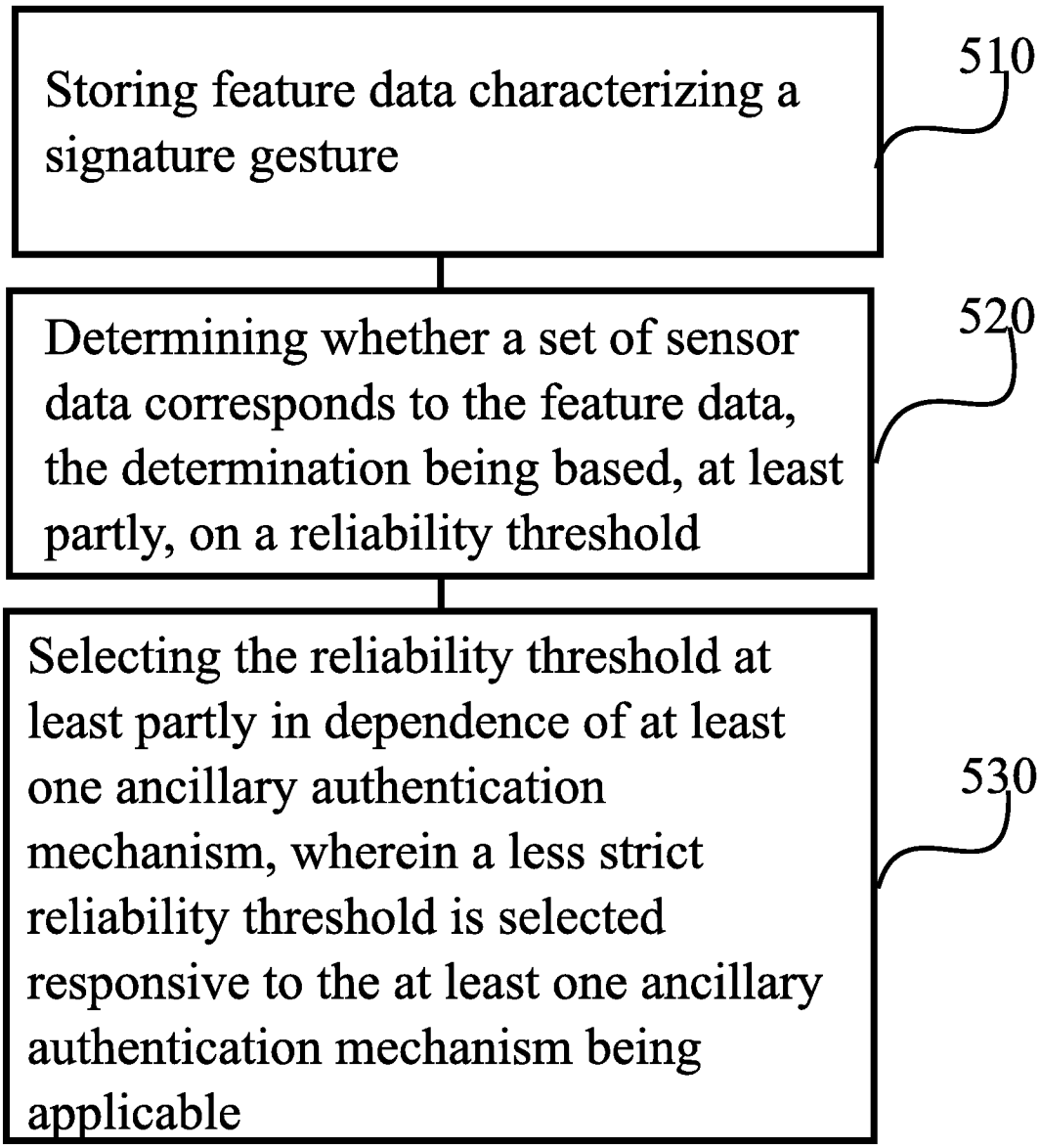
Storing feature data characterizing a signature gesture
510
Determining whether a set of sensor data corresponds to the feature data, the determination being based, at least partly, on a reliability threshold
520
Selecting the reliability threshold at least partly in dependence of at least one ancillary authentication mechanism, wherein a less strict reliability threshold is selected responsive to the at least one ancillary authentication mechanism being applicable
530

FIGURE 5

INTERNATIONAL SEARCH REPORT

International application No.
PCT/FI2016/050124

A. **CLASSIFICATION OF SUBJECT MATTER**

See extra sheet

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)

IPC: A61B, G06F, G06K, G06T, H04L

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

FI, SE, NO, DK

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

EPO-Internal, WPIAP, XP3GPP, XPAIP, XPESP, XPETSI, XPI3E, XPIEE, XPIETF, XPIOP, XPIPCOM, XPJPEG, XPMISC, XPOAC, XPRD, XPTK, BIOSIS, COMPDX, INSPEC, MEDLINE, TDB, NPL, Internet, PRH-Internal

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	WO 2015127256 A1 (QUALCOMM INC [US]) 27 August 2015 (27.08.2015) abstract; Figs. 1-9, 13F; paragraphs [0027], [0031]-[0076], [0087], [0094]	1-27
X	US 2016018872 A1 (TU XIAOYUAN [US] et al.) 21 January 2016 (21.01.2016) abstract; Figs. 2A-6, 11, 15; paragraphs [0005]-[0010], [0033]-[0034], [0042], [0049]-[0084], [0109]-[0121], [0145]-[0153]	1, 13, 25-27

☒ 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	Date of mailing of the international search report
15 June 2016 (15.06.2016)	20 June 2016 (20.06.2016)

Name and mailing address of the ISA/FI
Finnish Patent and Registration Office
P.O. Box 1160, FI-00101 HELSINKI, Finland
Facsimile No. +358 9 6939 5328

Authorized officer
Yrjö Raivio
Telephone No. +358 9 6939 500

INTERNATIONAL SEARCH REPORT

International application No.
PCT/FI2016/050124

C (Continuation). DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	US 2015278498 A1 (HONG SAYOON [KR] et al.) 01 October 2015 (01.10.2015) abstract; Figs. 1-5, 7, 11; paragraphs [0010]-[0015], [0021], [0160], [0178]-[0184], [0210]-[0212], [0224]-[0225], [0240]-[0244], [0266]-[0269]	1, 13, 25-27
X	US 2015074797 A1 (CHOI CHANG MOK [KR] et al.) 12 March 2015 (12.03.2015) abstract; Figs. 1-8; paragraphs [0003], [0007]-[0009], [0020]-[0026], [0045]-[0070], [0077], [0085], [0096]-[0097], [0102]-[0104], [0108]-[0110]	1, 13, 25-27
A	US 8922342 B1 (ASHENFELTER TIMOTHY PATRICK [US] et al.) 30 December 2014 (30.12.2014) abstract; Figs. 1, 5A-8; column 1, lines 36–60; column 2, line 60 – column 3, line 13; column 10, lines 5-21; column 12, lines 10-17; column 13, line 16 – column 14, line 21	1-27
A	US 2013055348 A1 (STRAUSS KARIN [US] et al.) 28 February 2013 (28.02.2013) abstract; Figs. 1-4; paragraphs [0003]-[0005], [0014], [0023]-[0031], [0045]-[0050]	1-27
A	WO 2012018326 A1 (RESEARCH IN MOTION LTD [CA]) 09 February 2012 (09.02.2012) abstract; Figs. 1-5B; paragraphs [0016]-[0024], [0030], [0033], [0035]	1-27
A	YANG, J et al. MotionAuth: Motion-based Authentication for Wrist Worn Smart Devices. IEEE International Conference on Pervasive Computing and Communication Workshops (PerCom Workshops) [online], March 2015 [retrieved on 2016-06-08]. Retrieved from the Internet: <URL: http://ieeexplore.ieee.org/xpls/abs_all.jsp?arnumber=7134097&tag=1>. The whole document.	7-8, 19-20
A	MARE, S et al. ZEBRA: Zero-Effort Bilateral Recurring Authentication. IEEE Symposium on Security and Privacy [online], May 2014 [retrieved on 2006-06-08]. Retrieved from the Internet: <URL: http://ieeexplore.ieee.org/xpls/abs_all.jsp?arnumber=6956596&tag=1>. The whole document.	1-27

INTERNATIONAL SEARCH REPORT
Information on Patent Family Members

International application No.
PCT/FI2016/050124

Patent document cited in search report	Publication date	Patent family members(s)	Publication date
WO 2015127256 A1	27/08/2015	US 2015242601 A1	27/08/2015
		US 2015242605 A1	27/08/2015
		WO 2015127253 A1	27/08/2015
US 2016018872 A1	21/01/2016	CN 105278681 A	27/01/2016
		CN 204731730 U	28/10/2015
		US 2016018898 A1	21/01/2016
		US 2016018899 A1	21/01/2016
		US 2016018900 A1	21/01/2016
		WO 2016010857 A1	21/01/2016
US 2015278498 A1	01/10/2015	US 9223956 B2	29/12/2015
		KR 20150112621 A	07/10/2015
		WO 2015147383 A1	01/10/2015
US 2015074797 A1	12/03/2015	CN 105556529 A	04/05/2016
		KR 20150029105 A	18/03/2015
		WO 2015034149 A1	12/03/2015
US 8922342 B1	30/12/2014	None	
US 2013055348 A1	28/02/2013	US 8839358 B2	16/09/2014
WO 2012018326 A1	09/02/2012	CA 2807189 A1	09/02/2012
		CN 103155509 A	12/06/2013
		EP 2601769 A1	12/06/2013
		US 2013133055 A1	23/05/2013
		US 9342677 B2	17/05/2016

INTERNATIONAL SEARCH REPORT

International application No.
PCT/FI2016/050124

CLASSIFICATION OF SUBJECT MATTER

IPC
A61B 5/0404 (2006.01)
A61B 5/00 (2006.01)
H04L 29/06 (2006.01)
H04L 9/32 (2006.01)
G06F 21/32 (2013.01)
G06K 9/00 (2006.01)