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

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
11 October 2018 (11.10.2018)

WIPO | PCT

(10) International Publication Number
WO 2018/186793 A1

(51) International Patent Classification:
G06F 21/32 (2013.01) *H04L 9/32* (2006.01)
G06K 9/00 (2006.01)

(21) International Application Number:
PCT/SE2018/050351

(22) International Filing Date:
04 April 2018 (04.04.2018)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
1750421-8 07 April 2017 (07.04.2017) SE

(71) Applicant: SAFE PATIENT IDENTIFICATION SWEDEN AB [SE/SE]; BOX 182, 30105 HALMSTAD (SE).

(72) Inventors: SKARP, Rolf M; BERGSGÅRDSVÄGEN 26, 30272 HALMSTAD (SE). SVENSSON, Stig-Arne; KUTTERVÄGEN 5, 30272 HALMSTAD (SE).

(74) Agent: GOTAPATENT AB; BOX 3127, 55003 JÖNKÖPING (SE).

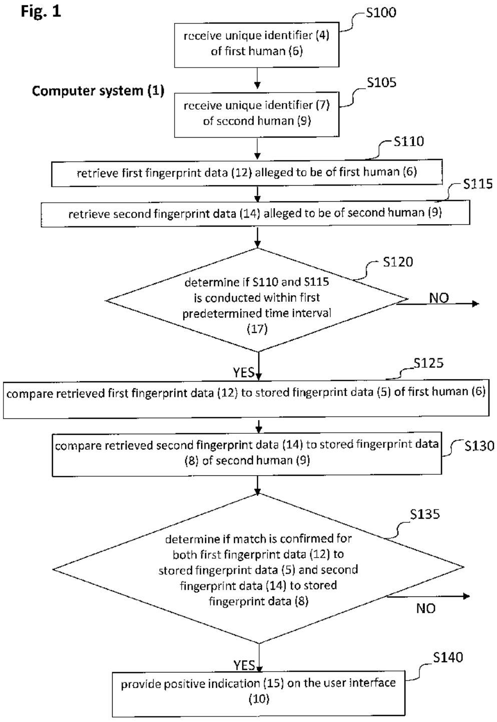
(81) Designated States *(unless otherwise indicated, for every kind of national protection available)*: AE, AG, AL, AM, AO, AT, AU, AZ, BA, BB, BG, BH, BN, BR, BW, BY, BZ, CA, CH, CL, CN, CO, CR, CU, CZ, DE, DJ, DK, DM, DO, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, GT, HN, HR, HU, ID, IL, IN, IR, IS,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

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

Published:
— *with international search report (Art. 21(3))*
— *before the expiration of the time limit for amending the claims and to be republished in the event of receipt of amendments (Rule 48.2(h))*

(54) Title: METHOD PERFORMED BY A COMPUTER SYSTEM FOR BIOMETRIC AUTHENTICATION OF HUMAN BEINGS OF A FIRST OR A SECOND CATEGORY

Fig. 1


Computer system (1)
S100
receive unique identifier (4) of first human (6)
S105
receive unique identifier (7) of second human (9)
S110
retrieve first fingerprint data (12) alleged to be of first human (6)
S115
retrieve second fingerprint data (14) alleged to be of second human (9)
S120
determine if S110 and S115 is conducted within first predetermined time interval (17)
NO
YES
S125
compare retrieved first fingerprint data (12) to stored fingerprint data (5) of first human (6)
S130
compare retrieved second fingerprint data (14) to stored fingerprint data (8) of second human (9)
S135
determine if match is confirmed for both first fingerprint data (12) to stored fingerprint data (5) and second fingerprint data (14) to stored fingerprint data (8)
NO
YES
S140
provide positive indication (15) on the user interface (10)

(57) Abstract: Method performed by a computer system (1) for biometric authentication. The method comprising the steps of retrieving a first fingerprint data (12) alleged to be of the first human (6) and retrieving a second fingerprint data alleged to be of the second human (9). If the retrieving of the first fingerprint data (12) is conducted within a first predetermined time interval (17) from the retrieving of the second fingerprint data (14), comparing the retrieved first fingerprint data (12) and the retrieved second fingerprint data (14) to the stored fingerprint data (8) of the first (6) respectively the second human (9). Providing a positive indication (15) when a match is confirmed for both the first fingerprint data (12) and the second fingerprint data (14) compared to the stored fingerprint data (8) of the first (6) respectively the second human (9).

WO 2018/186793 A1

METHOD PERFORMED BY A COMPUTER SYSTEM FOR BIOMETRIC AUTHENTICATION OF HUMAN BEINGS OF A FIRST OR A SECOND CATEGORY

Technical field

[0001] The present invention relates to a method performed by a computer system for biometric authentication of human beings of a first or a second category.

Background

[0002] First generations of biometric authentication systems have in the last decade been introduced on the global market. These systems have primarily been developed for authentication at a particular geographical place. Recently some mobile computer systems, including laptops and smartphones, also have had biometric authentication devices included in the hardware.

[0003] Authentication of at least two human beings belonging to different categories of people, such as a medical doctor vs. a patient, or a dentist vs. a patient, or an examiner/teacher vs. a student, or a courier vs. a recipient of a package/envelope, will in the near future become an important feature of e.g. business activities, the health care system and the educational system.

[0004] There are for instance relatively large sums of money lost annually due to insurance fraud in the health care and dental sector, where patient examinations allegedly have been conducted where in reality no such examinations have been conducted. This type of fraud causes further economical strains on the private and/or the tax funded health care and dental system.

[0005] Incidents have been revealed where the candidate signing in at an examination in reality has not been the alleged student. This type of fraud undermines the perception and the overall confidence of the scholar system.

[0006] Recipients of packages and envelopes claiming to be the true addressee, where in reality this is not true, can cause private and commercial economical losses and further disruption in commercial activities.

[0007] There is no biometric authentication system on the market supporting the authentication of at least two human beings belonging to different categories of people at one geographical location at a certain time. The current hardware and software are developed to authenticate one person at a time. These systems do not entirely solve the problem of fraud in the described situations above. Some personnel in the health care and dental sector might for instance by biometric authentication confirm that an examination has been conducted even if this is not correct. There could for instance be economic reasons for triggering this behaviour. Having to provide biometric authentication of both the patient and the medical personnel at one geographical location at the date and time for the alleged examination strongly decreases the risks of fraud.

[0008] Biometric authentication by comparing fingerprints is a well proven technique. There are furthermore quite a few different electronic fingerprint readers available on the market.

[0009] It is therefore desirable to accomplish a system for biometric authentication of human beings of at least a first and a second category at one geographical location at a certain time. Furthermore the system should use some type of comparison technique of fingerprint data. There should also be additional security features implemented in the solution supporting the described technology.

Summary of invention

[0010] An objective of the present invention is thus to accomplish a method performed by a computer system for biometric authentication of human beings of a first or a second category at one geographical location at a certain time, which uses some type of comparison technique of fingerprint data and has additional security features implemented in the solution.

[0011] According to one aspect, the invention concerns a method performed by a computer system for biometric authentication of human beings of a first or a second category. Wherein the computer system has access to stored unique identifier and fingerprint data of a first human being of the first category and stored unique identifier and fingerprint data of a second human being of the second category. The method comprising the steps of receiving the unique identifier of the first human being at a user interface of a computer, and receiving the unique identifier of the second human being at the user interface of the computer, and retrieving a first fingerprint data at a fingerprint reader of the computer. The first fingerprint data alleged to be of the first human being, and retrieving a second fingerprint data at the fingerprint reader of the computer. The second fingerprint data alleged to be of the second human being, and if the retrieving of the first fingerprint data is conducted within a first predetermined time interval from the retrieving of the second fingerprint data, comparing the retrieved first fingerprint data to the stored fingerprint data of the first human being, and comparing the retrieved second fingerprint data to the stored fingerprint data of the second human being, and providing a positive indication on the user interface of the computer when a match is confirmed for both the first fingerprint data compared to the stored fingerprint data of the first human being, and the second fingerprint data compared to the stored fingerprint data of the second human being.

[0012] The fact that there always within a short period of time has to be two human beings of two different categories involved for a biometric authentication to be validated at one geographical location at a certain time, implies that the described method and the social control taking place dramatically decreases the risks of fraud/tampering of the computer/control system. This decreases the risk of potential financial loss in the organisation and/or the society as a whole.

[0013] The method above may be configured according to different optional embodiments. For example, wherein in response to a confirmed match for the first fingerprint data compared to the stored fingerprint data of the first human being the method may capture a picture of the confirmed first human being within a second predetermined time interval after the match is confirmed, and store the captured picture in connection with the stored unique identifier and stored fingerprint data of the first human being and possibly also in connection with a time and a date of the capturing.

[0014] Capturing a picture of the confirmed first human being will provide the owner of the computer system a further possibility to confirm the identity of the confirmed first human being. It also enhances the possibility that a potential fraudster will not try to be accepted/confirmed as someone else.

[0015] Storing the captured picture in connection with the other personal data stored, and possibly also in connection with a time and a date of the capturing, will provide the owner of the computer system a possibility later on in the process to re-confirm that the event has taken place.

[0016] According to an embodiment of the invention wherein in response to a confirmed match for both the first fingerprint data compared to the stored fingerprint data of the first human being and the second fingerprint data compared to the stored fingerprint data of the second human being the method may comprise the step of unlocking and/or locking a device that is communicatively connected to the computer system by sending an unlocking signal to the device.

[0017] By giving the possibility to unlock/lock a device that is communicatively connected to the computer system by sending an unlocking signal to the device, will for instance give the possibility to unlock/lock medical/dental devices for a certain medical/dental procedure, to unlock/lock doors/gates based on biometrical authentication from at least two human beings, to unlock/lock other technical devices for a certain procedure.

[0018] According to an embodiment of the invention wherein for achieving the computer system's access to stored unique identifier and fingerprint data of the first human being of the first category the method may comprise the steps of receiving an indication for adding a unique identifier of the first human being at the user interface of the computer, and receiving the unique identifier of the first human being at the user interface of the computer, and storing the unique identifier of the first human being, and receiving an indication for adding a fingerprint data of the first human being at the user interface of the computer, and retrieving the fingerprint data of the first human being at the fingerprint reader of the computer, and storing the fingerprint data of the first human being in connection with the stored unique identifier of the first human being and possibly also in connection with a time and a date of the retrieving.

[0019] By providing the possibility for the computer system to, prior to the described process, receive/collect and store personal data of the first human being supposed to use and be confirmed by the system, the computer system can function as a stand-alone system for covering the full process from collection of biometrical and personal data to confirmation of the alleged first human being by comparison of biometrical and personal data to the stored data.

[0020] According to an embodiment of the invention wherein for achieving the computer system's access to stored unique identifier and fingerprint data of the second human being of the second category the method may comprises the steps of receiving an indication for adding a unique identifier of the second human being at the user interface of the computer, and receiving the unique identifier of the second human being at the user interface of the computer, and storing the unique identifier of the second human being, and receiving an indication for adding a fingerprint data of the second human being at the user interface of the computer, and retrieving the fingerprint data of the second human being at the fingerprint reader of the computer, and storing the fingerprint data of the second human being in connection with the stored unique identifier of the second human being and possibly also in connection with a time and a date of the retrieving.

[0021] By providing the possibility for the computer system to, prior to the described process, receive/collect and store personal data of the second human being supposed to use and be confirmed by the system, the computer system can function as a stand-alone system for covering the full process from collection of biometrical and personal data to confirmation of the alleged second human being by comparison of biometrical and personal data to the stored data.

[0022] According to an embodiment of the invention wherein in response when a match is not confirmed for any of the first fingerprint data compared to the stored fingerprint data of the first human being and the second fingerprint data compared to the stored fingerprint data of the second human being the method may comprise the step of providing a negative indication on the user interface of the computer.

[0023] By providing the possibility for the computer system to provide a negative indication on the user interface of the computer, the user will be informed if/when they have been confirmed by the computer system for not being the same/correct human being in comparison to their alleged identity.

[0024] According to an embodiment of the invention wherein when the positive indication or the negative indication has been provided the method may comprise the step of storing the positive indication or the negative indication in connection with the stored unique identifiers and the stored fingerprint data of the first and the second human being and possibly also in connection with a time and a date of the comparing.

[0025] Storing the positive or the negative indication in connection with the other personal data stored of the user, and possibly also in connection with a time and a date of the capturing, will provide the owner of the computer system a possibility later on in the process to e.g. re-confirm or do statistical analysis on the outcome of the events.

[0026] According to one aspect, the invention concerns a computer system for biometric authentication of human beings of a first or a second category. Wherein the computer system has access to stored unique identifier and fingerprint data of a first human being of the first category and stored unique identifier and fingerprint data of a second human being of the second category. Wherein the computer system is arranged to receive the unique identifier of the first human being at a user interface of a computer, and receive the unique identifier of the second human being at the user interface of the computer, and retrieve a first fingerprint data at a fingerprint reader of the computer. The first fingerprint data alleged to be of the first human being, and retrieve a second fingerprint data at the fingerprint reader of the computer. The second fingerprint data alleged to be of the second human being, and if the retrieving of the first fingerprint data is conducted within a first predetermined time interval from the retrieving of the second fingerprint data, compare the retrieved first fingerprint data to the stored fingerprint data of the first human being, and compare the retrieved second fingerprint data to the stored fingerprint data of the second human being, and provide a positive indication on the user interface of the computer when a match is confirmed for both the first fingerprint data compared to the stored fingerprint data of the first human being, and the second fingerprint data compared to the stored fingerprint data of the second human being.

[0027] The fact that there always within a short period of time has to be two human beings of two different categories involved for a biometric authentication to be validated at one geographical location at a certain time, implies that the described computer system and the social control taking place dramatically decreases the risks of fraud/tampering of the computer/control system. This decreases the risk of potential financial loss in the organisation and/or the society as a whole.

[0028] According to another aspect a computer program comprises computer readable code means, which when run on a computer system causes the computer system to perform the corresponding method.

[0029] According to another aspect a computer program product comprises a computer readable medium and a computer program. Wherein the computer program is stored on the computer readable medium.

[0030] The computer system may comprise a mobile device, which may include devices such as at least one fingerprint reader, at least one user interface and at least one PCB for data handling. The device may comprise two fingerprint readers, wherein one reader is specifically implemented for the first human being and a second reader is specifically implemented for the second human being. The mobile device may be connected by cable or wireless to the rest of the computer system for transferring of data.

[0031] One example for the computer system to be deployed is when a medical doctor is making a home visit at a patient. Personal data, such as fingerprints and unique identifiers, is prior to this visit stored in a central database. A mobile device is then used for selecting unique identifiers and collecting fingerprints from the medical doctor and the patient at site. The collected data is transferred wirelessly from the mobile device to the central server where the comparing step is conducted. A positive or negative indication of a match is transferred from the central server to the mobile device.

[0032] Another example for the computer system to be deployed is when a patient visits the dentist. The patient and the dentist can then at the local dentist's surgery make biometric authentications in the same manner as in the example when a patient is visited by a medical doctor at home.

[0033] In the method described the human being of a first category may be the patient described above and the human being of a second category may be medical/dental practitioner described above.

[0034] The described computer system may not be manipulated by non-authorised personnel, as the user interface of the computer system does not give the possibility to change, delete or manipulate data. The described method further strengthens the case for a non-manipulative system.

[0035] The signal used for, unlocking/locking a device that is communicatively connected to the computer system by sending an unlocking signal to the device, could e.g. be of electronic or optical type sent e.g. via cable or by wireless means.

[0036] The time and date may be taken from external sources from e.g. the internet and stored centrally. The time and date cannot in the computer system be changed, deleted or altered by non-authorised personnel.

[0037] There could also be more than two human beings using the system for a biometric authentication process.

[0038] A unique identifier could for instance be a national identification number, a national identity number, a personal identity number, a national insurance number, a national health service number, a social security number, a passport number, a name, an e-mail address, a telephone number among others.

[0039] The first predetermined time interval in claim 1 could be any time interval which the organisation determines to be a sufficient time interval for at least two human beings providing their fingerprint data to the system. The predetermined time interval could for instance be 0-60 seconds, among others.

[0040] The second predetermined time interval in claim 2 could be any time interval which the organisation determines to be a suitable time interval in between the match is confirmed and for the picture to be taken of the first human being. The second predetermined time interval could for instance be 0-10 seconds, among others.

[0041] The capturing of a picture of the confirmed first human being within a predetermined time interval after the match is confirmed could for instance be conducted via a camera connected to the computer.

[0042] In claim 1 prior to the retrieving step of the fingerprint data of an alleged first human being at the fingerprint reader of the computer, the following step could be implemented: receiving at the user interface of the computer an indication for retrieving a fingerprint data of the first human being and the second human being.

Brief description of drawings

[0043] The invention is now described, by way of example, with reference to the accompanying drawings, in which:

[0044] Fig. 1 is a flow chart of a procedure according to an embodiment.

[0045] Fig. 2 is a flow chart of a procedure according to an embodiment.

[0046] Fig. 3 is a flow chart of a procedure according to an embodiment.

[0047] Fig. 4 is a flow chart of a procedure according to an embodiment.

[0048] Fig. 5 is a flow chart of a procedure according to an embodiment.

[0049] Fig. 6 is a flow chart of a procedure according to an embodiment.

[0050] Fig. 7 is a block diagram illustrating, according to a possible embodiment.

[0051] Fig. 8 is a block diagram illustrating, according to a possible embodiment.

Description of embodiments

[0052] In the following, a detailed description of a method performed by a computer system for biometric authentication of human beings of a first or a second category is provided.

[0053] Fig. 1 shows a flow chart illustrating a procedure in a computer system. The various actions may come in different orders than presented in this description, or in a different order than shown in this or other flowcharts related to this description, or some steps may be performed in parallel.

[0054] In a step S100 a unique identifier 4 of the first human being 6 is received at a user interface 10 of a computer 11. In a step S105 a unique identifier 7 of the second human being 9 is received at the user interface 10 of the computer 11. In a step S110 a first fingerprint data 12 is retrieved at a fingerprint reader 13 of the computer 11. The first fingerprint data 12 alleged to be of the first human being 6. In a step S115 a second fingerprint data 14 is retrieved at the fingerprint reader 13 of the computer 11. The second fingerprint data 14 alleged to be of the second human being 9. In a step S120 it is determined if the retrieving of the first fingerprint data 12 is conducted within a first predetermined time interval 17 from the retrieving of the second fingerprint data 14. In a step S125 the retrieved first fingerprint data 12 is compared to the stored fingerprint data 5 of the first human being 6. In a step S130 the retrieved second fingerprint data 14 is compared to the stored fingerprint data 8 of the second human being 9. In a step S135 determine if a match is confirmed for both the first fingerprint data 12 compared to the stored fingerprint data 5 of the first human being 6, and the second fingerprint data 14 compared to the stored fingerprint data 8 of the second human being 9. In a step S140 provided a positive indication 15 on the user interface 10 of the computer 11.

[0055] Fig. 2 shows a flow chart illustrating a procedure in a computer system. The various actions may come in different orders than presented in this description, or in a different order than shown in this or other flowcharts related to this description, or some steps may be performed in parallel.

[0056] In a step S200 a match for the first fingerprint data 12 compared to the stored fingerprint data 5 of the first human being 5 is confirmed. In a step S205 a picture 16 of the confirmed first human being 6 is captured within a second predetermined time interval 18 after the match is confirmed. In a step S210 the captured picture 16 is stored in connection with the stored unique identifier 4 and stored fingerprint data 5 of the first human being 6 and possibly also in connection with a time 19 and a date 20 of the capturing.

[0057] Fig. 3 shows a flow chart illustrating a procedure in a computer system. The various actions may come in different orders than presented in this description, or in a different order than shown in this or other flowcharts related to this description, or some steps may be performed in parallel.

[0058] In a step S300 a match for both the first fingerprint data 12 compared to the stored fingerprint data 5 of the first human being 6 and the second fingerprint data 14 compared to the stored fingerprint data 8 of the second human being 9 is confirmed. In a step S305 a device 21 that is communicatively connected to the computer system 1 is unlocked and/or locked by sending an unlocking signal 22 to the device 21.

[0059] Fig. 4 shows a flow chart illustrating a procedure in a computer system. The various actions may come in different orders than presented in this description, or in a different order than shown in this or other flowcharts related to this description, or some steps may be performed in parallel.

[0060] In a step S400 an indication for adding a unique identifier 4 of the first human being 6 is received at the user interface 10 of the computer 11. In a step S405 the unique identifier 4 of the first human being 6 is received at the user interface 10 of the computer 11. In a step S410 the unique identifier 4 of the first human being 6 is stored. In a step S415 an indication for adding a fingerprint data 5 of the first human being 6 is received at the user interface 10 of the computer 11. In a step S420 the fingerprint data 5 of the first human being 6 is retrieved at the fingerprint reader 13 of the computer 11. In a step S425 the fingerprint data 5 of the first human being 6 is stored in connection with the stored unique identifier 4 of the first human being 6 and possibly also in connection with a time 19 and a date 20 of the retrieving.

[0061] Fig. 5 shows a flow chart illustrating a procedure in a computer system. The various actions may come in different orders than presented in this description, or in a different order than shown in this or other flowcharts related to this description, or some steps may be performed in parallel.

[0062] In a step S500 an indication for adding a unique identifier 7 of the second human being 9 is received at the user interface 10 of the computer 11. In a step S505 the unique identifier 7 of the second human being 9 is received at the user interface 10 of the computer 11. In a step S510 the unique identifier 7 of the second human being 9 is stored. In a step S515 an indication for adding a fingerprint data 8 of the second human being 9 is received at the user interface 10 of the computer 11. In a step S520 the fingerprint data 8 of the second human being 9 is retrieved at the fingerprint reader 13 of the computer 11. In a step S525 the fingerprint data 8 of the second human being 9 is stored in connection with the stored unique identifier 7 of the second human being 9 and possibly also in connection with a time 19 and a date 20 of the retrieving.

[0063] Fig. 6 shows a flow chart illustrating a procedure in a computer system. The various actions may come in different orders than presented in this description, or in a different order than shown in this or other flowcharts related to this description, or some steps may be performed in parallel.

[0064] In a step 6.1 a unique identifier 4 of the first human being 6 is received at a user interface 10 of a computer 11. In a step 6.2 a unique identifier 7 of the second human being 9 is received at the user interface 10 of the computer 11. In a step 6.3 a first fingerprint data 12 is retrieved at a fingerprint reader 13 of the computer 11. The first fingerprint data 12 alleged to be of the first human being 6. In a step 6.4 a second fingerprint data 14 is retrieved at the fingerprint reader 13 of the computer 11. The second fingerprint data 14 alleged to be of the second human being 9. In a step 6.5 it is determined if the retrieving of the first fingerprint data 12 is conducted within a first predetermined time interval 17 from the retrieving of the second fingerprint data 14. In a step 6.6 the retrieved first fingerprint data 12 is compared to the stored fingerprint data 5 of the first human being 6. Furthermore the retrieved second fingerprint data 14 is compared to the stored fingerprint data 8 of the second human being 9. In a step 6.7 determine if a match is confirmed for both the first fingerprint data 12 compared to the stored fingerprint data 5 of the first human being 6, and the second fingerprint data 14 compared to the stored fingerprint data 8 of the second human being 9. Furthermore provide a positive indication 15 on the user interface 10 of the computer 11 when a match is confirmed.

[0065] Fig. 7 shows a computer 11, including components such as a processor 7.1, a memory 7.2, a data management unit 7.3, a database 7.4 and a user interface 7.5.

[0066] Fig. 8 shows a user interface (10) of the computer (11), a camera connected to the computer (11), a first human being (6) and a second human being (9).

- - -

CLAIMS

1. Method performed by a computer system (1) for biometric authentication of human beings of a first (2) or a second category (3), wherein the computer system (1) has access to stored unique identifier (4) and fingerprint data (5) of a first human being (6) of the first category (2) and stored unique identifier (7) and fingerprint data (8) of a second human being (9) of the second category (3), the method comprising the steps of:

receiving the unique identifier (4) of the first human being (6) at a user interface (10) of a computer (11), and

receiving the unique identifier (7) of the second human being (9) at the user interface (10) of the computer (11), and

retrieving a first fingerprint data (12) at a fingerprint reader (13) of the computer (11), the first fingerprint data (12) alleged to be of the first human being (6), and

retrieving a second fingerprint data (14) at the fingerprint reader (13) of the computer (11), the second fingerprint data (14) alleged to be of the second human being (9), and

if the retrieving of the first fingerprint data (12) is conducted within a first predetermined time interval (17) from the retrieving of the second fingerprint data (14),

comparing the retrieved first fingerprint data (12) to the stored fingerprint data (5) of the first human being (6), and

comparing the retrieved second fingerprint data (14) to the stored fingerprint data (8) of the second human being (9), and

providing a positive indication (15) on the user interface (10) of the computer (11) when a match is confirmed for both the first fingerprint data (12) compared to the stored fingerprint data (5) of the first human being (6), and the second fingerprint data (14) compared to the stored fingerprint data (8) of the second human being (9).

2. Method according to claim 1, wherein in response to a confirmed match for the first fingerprint data (12) compared to the stored fingerprint data (5) of the first human being (5),:

capturing a picture (16) of the confirmed first human being (6) within a second predetermined time interval (18) after the match is confirmed, and

storing the captured picture (16) in connection with the stored unique identifier (4) and stored fingerprint data (5) of the first human being (6) and possibly also in connection with a time (19) and a date (20) of the capturing.

3. Method according to claim 1 or 2, wherein in response to a confirmed match for both the first fingerprint data (12) compared to the stored fingerprint data (5) of the first human being (6) and the second fingerprint data (14) compared to the stored fingerprint data (8) of the second human being (9), the method comprises the step of:

unlocking and/or locking a device (21) that is communicatively connected to the computer system (1) by

sending an unlocking signal (22) to the device (21).

4. Method according to any of claims 1-3, wherein for achieving the computer system's access to stored unique identifier (4) and fingerprint data (5) of the first human being (6) of the first category (2), the method comprises the steps of:

receiving an indication for adding a unique identifier (4) of the first human being (6) at the user interface (10) of the computer (11), and receiving the unique identifier (4) of the first human being (6) at the user interface (10) of the computer (11), and

storing the unique identifier (4) of the first human being (6), and

receiving an indication for adding a fingerprint data (5) of the first human being (6) at the user interface (10) of the computer (11), and

retrieving the fingerprint data (5) of the first human being (6) at the fingerprint reader (13) of the computer (11), and

storing the fingerprint data (5) of the first human being (6) in connection with the stored unique identifier (4) of the first human being (6) and possibly also in connection with a time (19) and a date (20) of the retrieving.

5. Method according to any of claims 1-4, wherein for achieving the computer system's access to stored unique identifier (7) and fingerprint data (8) of the second human being (9) of the second category (3), the method comprises the steps of:

receiving an indication for adding a unique identifier (7) of the second human being (9) at the user interface (10) of the computer (11), and

receiving the unique identifier (7) of the second human being (9) at the user interface (10) of the computer (11), and

storing the unique identifier (7) of the second human being (9), and

receiving an indication for adding a fingerprint data (8) of the second human being (9) at the user interface (10) of the computer (11), and

retrieving the fingerprint data (8) of the second human being (9) at the fingerprint reader (13) of the computer (11), and

storing the fingerprint data (8) of the second human being (9) in connection with the stored unique identifier (7) of the second human being (9) and possibly also in connection with a time (19) and a date (20) of the retrieving.

6. Method according to any of claims 1-5, wherein in response when a match is not confirmed for any of the first fingerprint data (12) compared to the stored fingerprint data (5) of the first human being (6), and the second fingerprint data (14) compared to the stored fingerprint data (8) of the second human being (9), the method comprises the step of:

providing a negative indication (25) on the user interface (10) of the computer (11).

7. Method according to any of claims 1-6, wherein when the positive indication (15) or the negative indication (25) has been provided, the method comprises the step of:

storing the positive indication (15) or the negative indication (25) in connection with the stored unique identifiers (4, 7) and the stored fingerprint data (5, 8) of the first (6) and the second human being (9) and possibly also in connection with a time (19) and a date (20) of the comparing.

8. A computer system (1) for biometric authentication of human beings of a first (2) or a second category (3), wherein the computer system (1) has access to stored unique identifier (4) and fingerprint data (5) of a first human being (6) of the first category (2) and stored unique identifier (7) and fingerprint data (8) of a second human being (9) of the second category (3), wherein the computer system (1) is arranged to:

receive the unique identifier (4) of the first human being (6) at a user interface (10) of a computer (11), and

receive the unique identifier (7) of the second human being (9) at the user interface (10) of the computer (11), and retrieve a first fingerprint data (12) at a fingerprint reader (13) of the computer (11), the first fingerprint data (12) alleged to be of the first human being (6), and

retrieve a second fingerprint data (14) at the fingerprint reader (13) of the computer (11), the second fingerprint data (14) alleged to be of the second human being (9), and

if the retrieving of the first fingerprint data (12) is conducted within a first predetermined time interval (17) from the retrieving of the second fingerprint data (14),

compare the retrieved first fingerprint data (12) to the stored fingerprint data (5) of the first human being (6), and

compare the retrieved second fingerprint data (14) to the stored fingerprint data (8) of the second human being (9), and

provide a positive indication (15) on the user interface (10) of the computer (11) when a match is confirmed for both the first fingerprint data (12) compared to the stored fingerprint data (5) of the first human being (6), and the second fingerprint data (14) compared to the stored fingerprint data (8) of the second human being (9).

9. A computer program, comprising computer readable code means, which when run on a computer system according to claim 8 causes the computer system to perform the corresponding method according to any of the claims 1-7.

10. A computer program product, comprising a computer readable medium and a computer program according to claim 9, wherein the computer program is stored on the computer readable medium.

Fig. 1

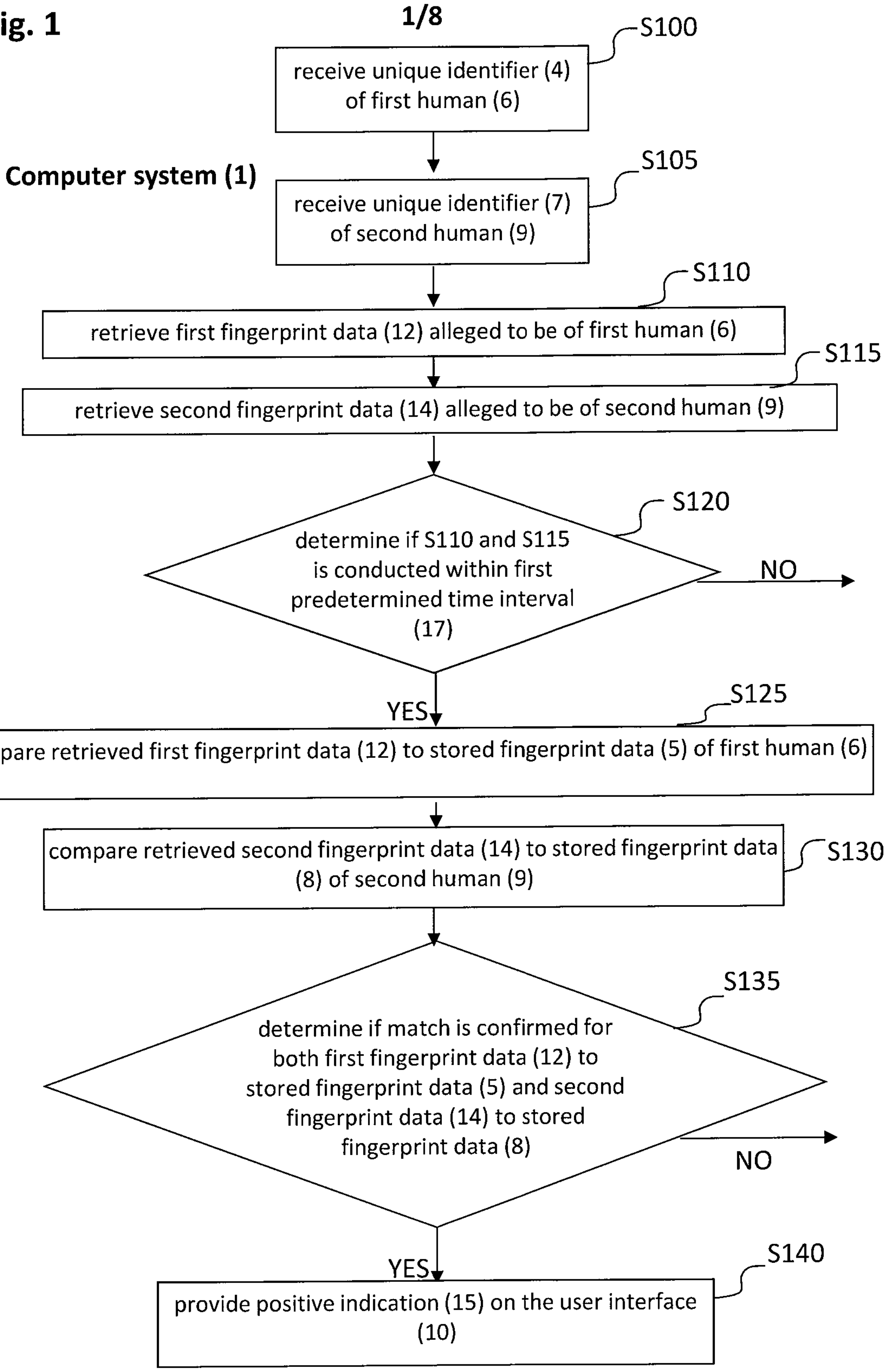

Computer system (1)
S100
receive unique identifier (4) of first human (6)
S105
receive unique identifier (7) of second human (9)
S110
retrieve first fingerprint data (12) alleged to be of first human (6)
S115
retrieve second fingerprint data (14) alleged to be of second human (9)
S120
determine if S110 and S115 is conducted within first predetermined time interval (17)
NO
YES
S125
compare retrieved first fingerprint data (12) to stored fingerprint data (5) of first human (6)
compare retrieved second fingerprint data (14) to stored fingerprint data (8) of second human (9)
S130
S135
determine if match is confirmed for both first fingerprint data (12) to stored fingerprint data (5) and second fingerprint data (14) to stored fingerprint data (8)
NO
YES
S140
provide positive indication (15) on the user interface (10)

Fig. 2

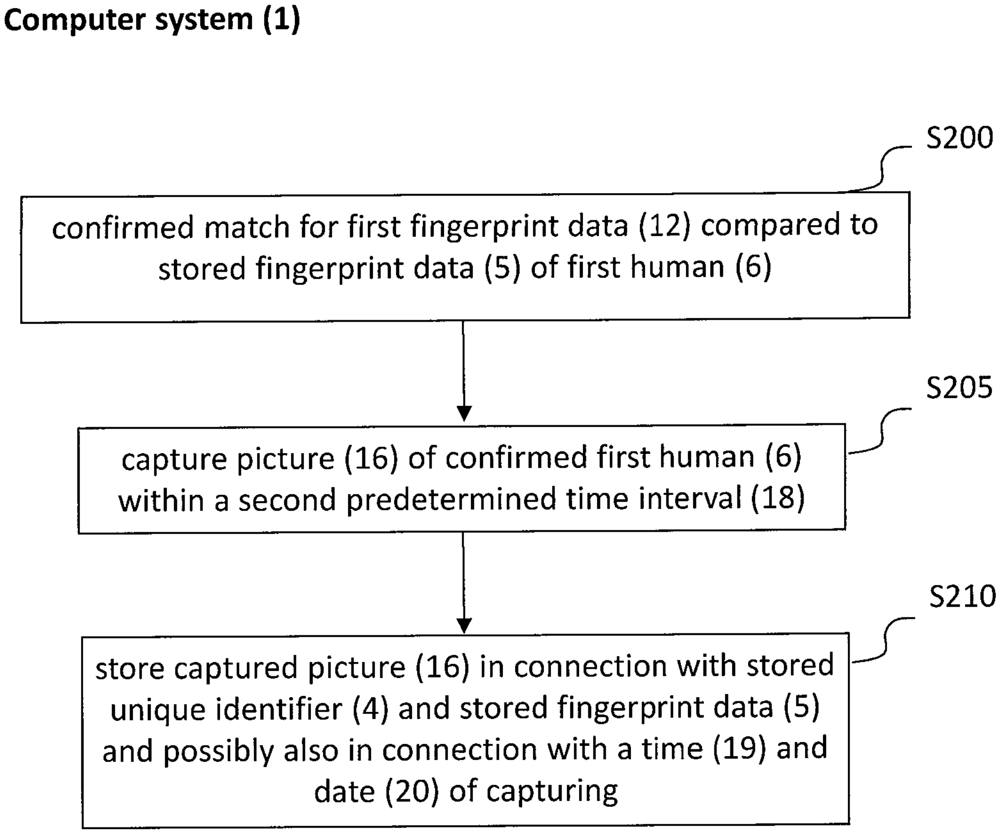

Computer system (1)
S200
confirmed match for first fingerprint data (12) compared to stored fingerprint data (5) of first human (6)
S205
capture picture (16) of confirmed first human (6) within a second predetermined time interval (18)
S210
store captured picture (16) in connection with stored unique identifier (4) and stored fingerprint data (5) and possibly also in connection with a time (19) and date (20) of capturing

Fig. 3

Computer system (1)

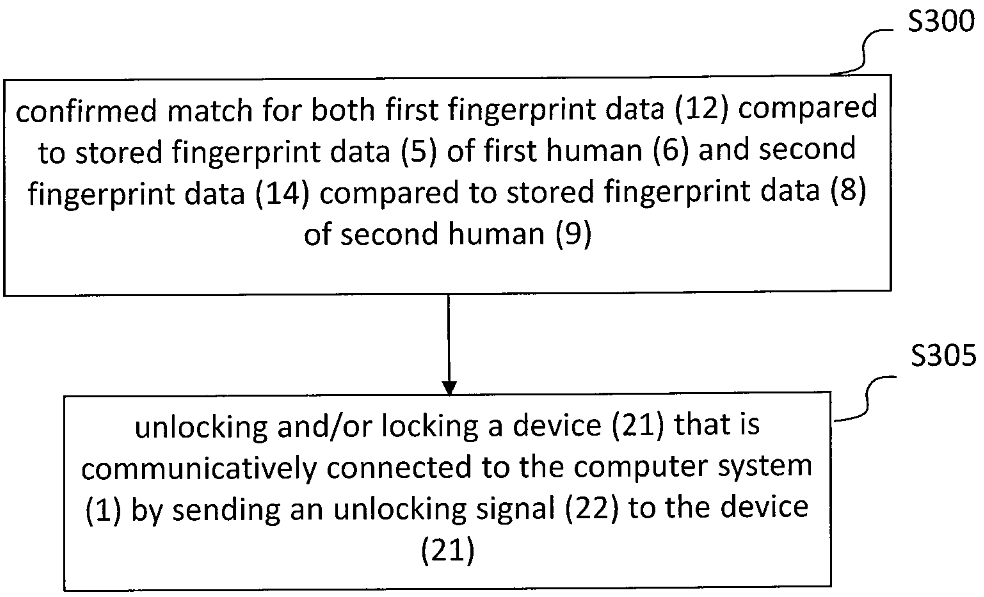

S300
confirmed match for both first fingerprint data (12) compared to stored fingerprint data (5) of first human (6) and second fingerprint data (14) compared to stored fingerprint data (8) of second human (9)
S305
unlocking and/or locking a device (21) that is communicatively connected to the computer system (1) by sending an unlocking signal (22) to the device (21)

Fig. 4

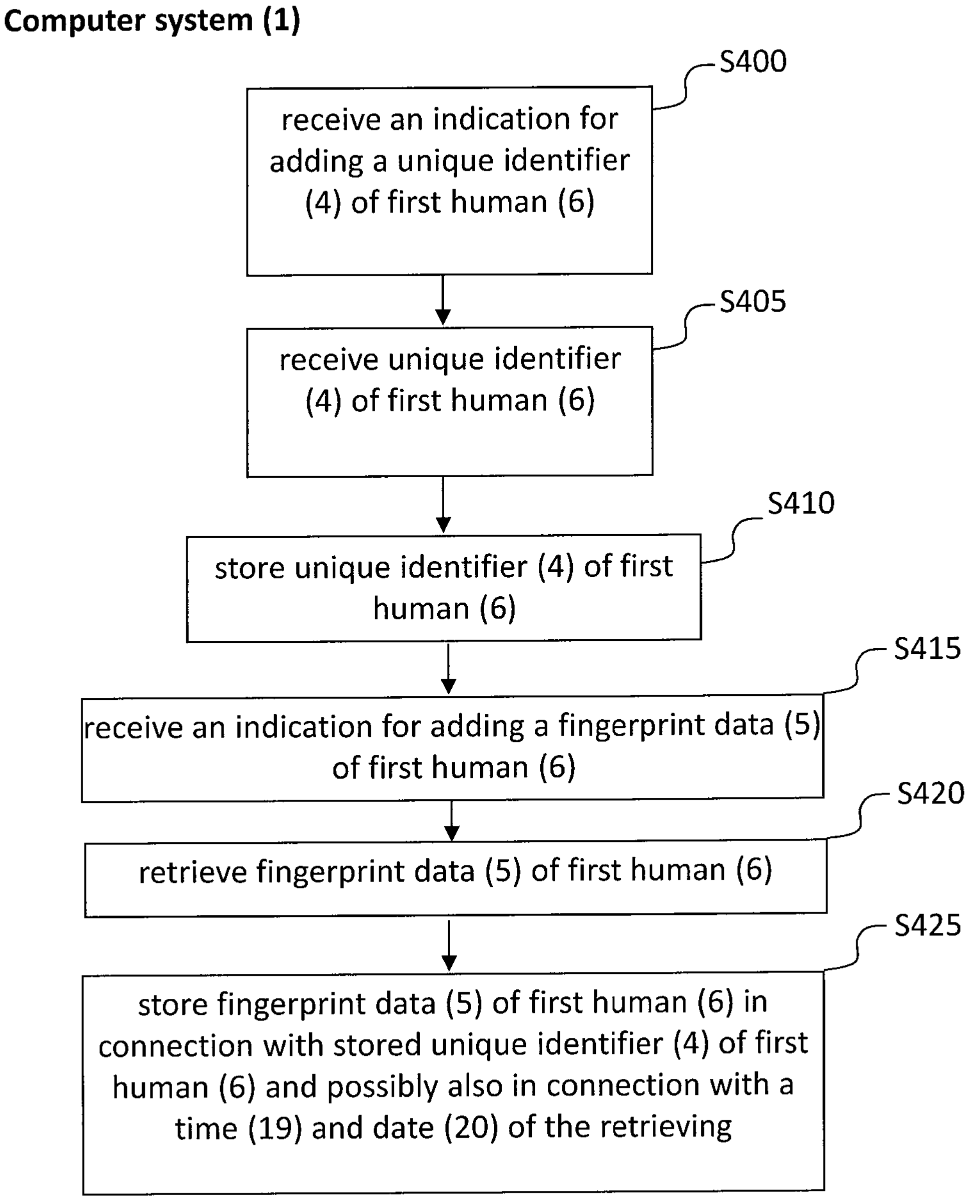

Computer system (1)
S400
receive an indication for adding a unique identifier (4) of first human (6)
S405
receive unique identifier (4) of first human (6)
S410
store unique identifier (4) of first human (6)
S415
receive an indication for adding a fingerprint data (5) of first human (6)
S420
retrieve fingerprint data (5) of first human (6)
S425
store fingerprint data (5) of first human (6) in connection with stored unique identifier (4) of first human (6) and possibly also in connection with a time (19) and date (20) of the retrieving

Fig. 5

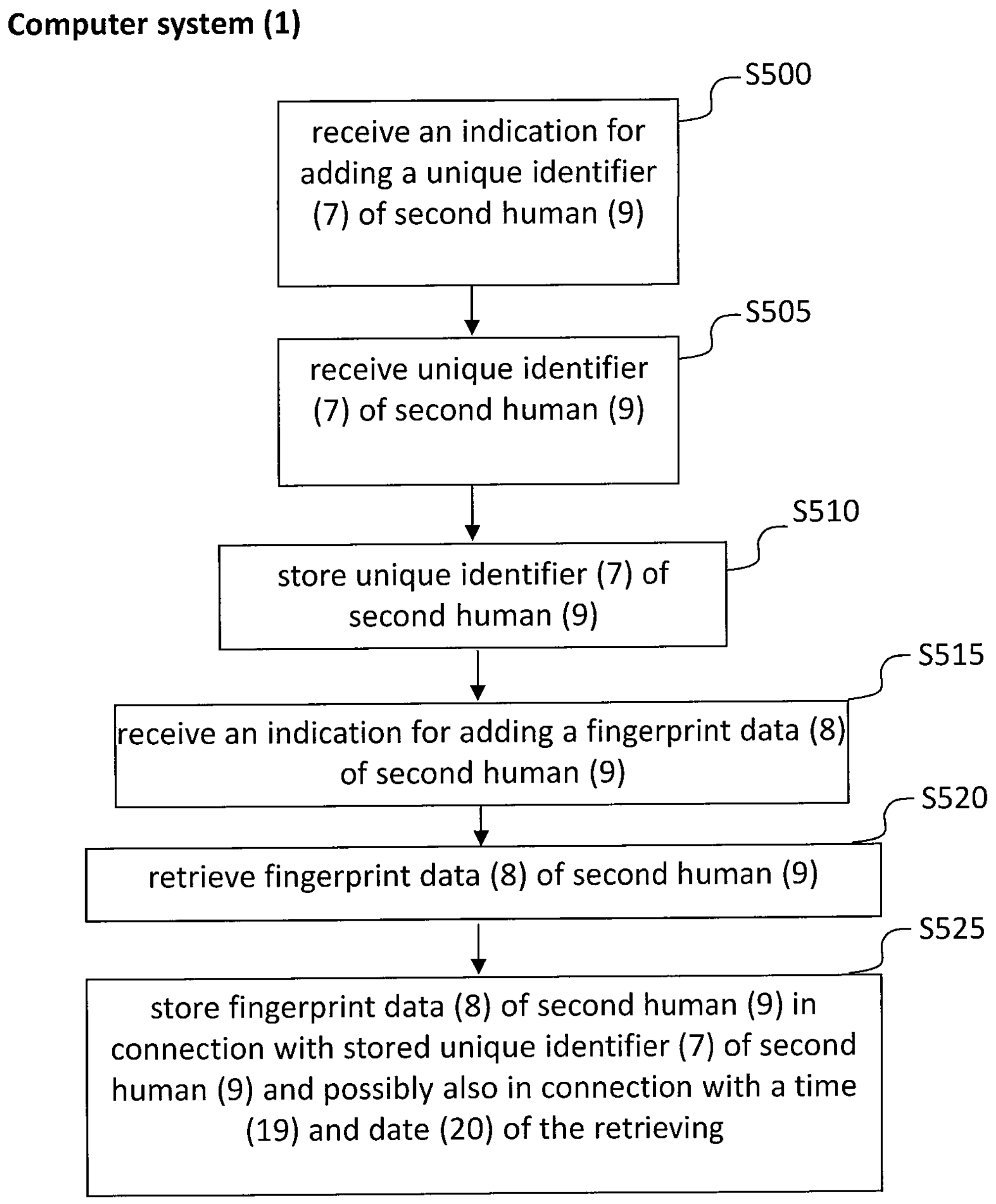

Computer system (1)
S500
receive an indication for adding a unique identifier (7) of second human (9)
S505
receive unique identifier (7) of second human (9)
S510
store unique identifier (7) of second human (9)
S515
receive an indication for adding a fingerprint data (8) of second human (9)
S520
retrieve fingerprint data (8) of second human (9)
S525
store fingerprint data (8) of second human (9) in connection with stored unique identifier (7) of second human (9) and possibly also in connection with a time (19) and date (20) of the retrieving

Fig. 6

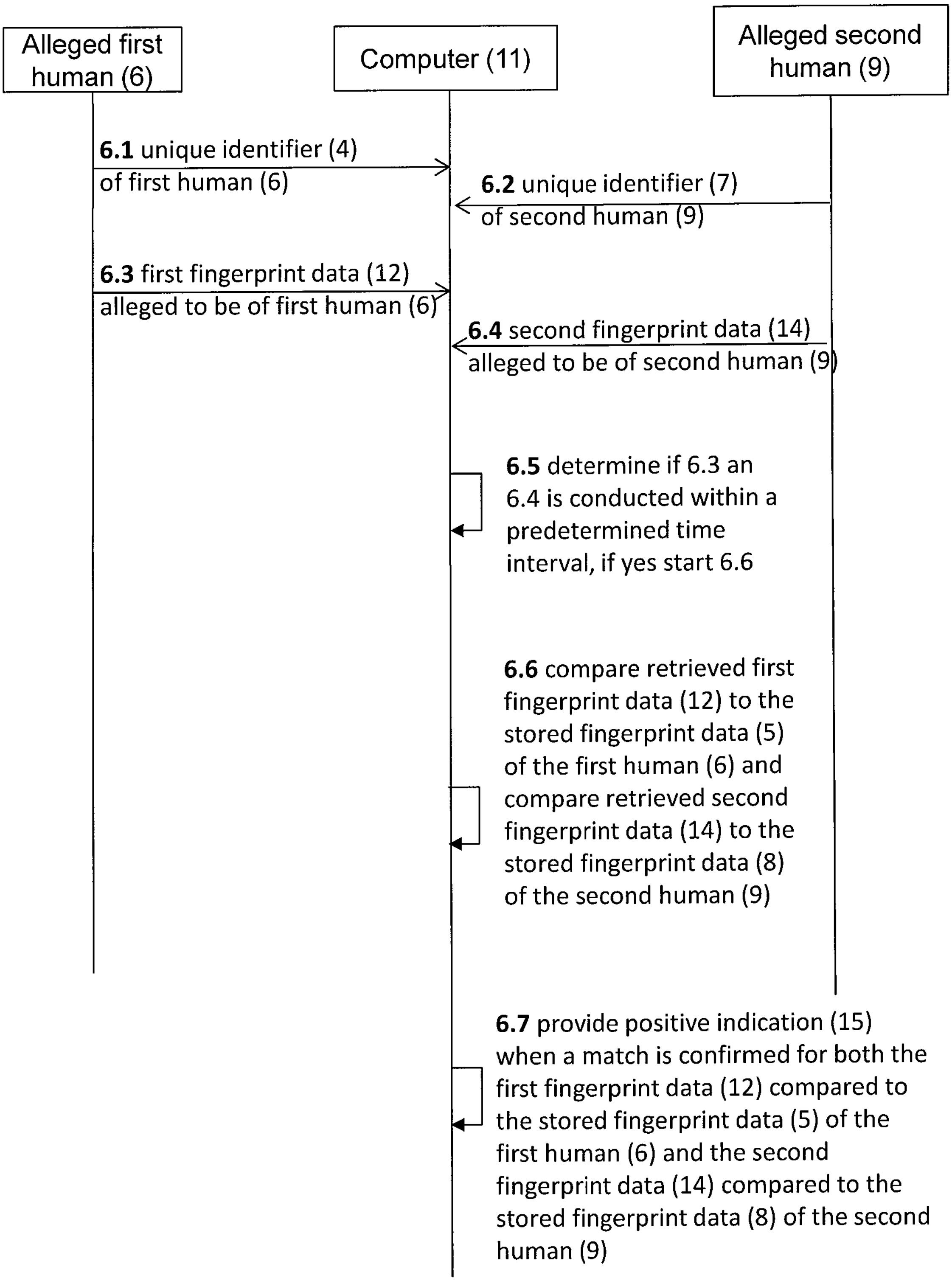
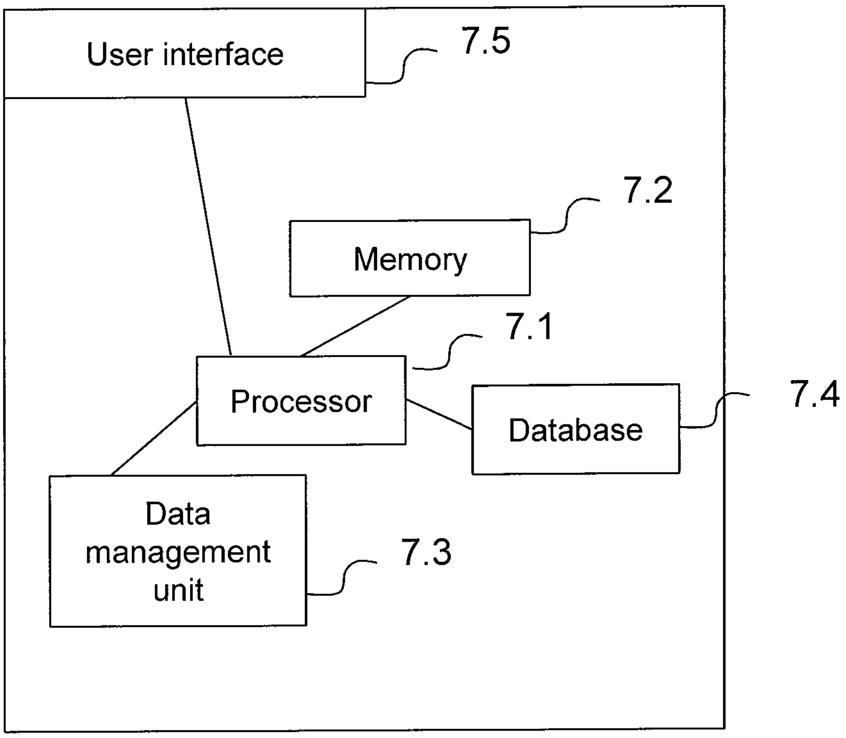

Alleged first human (6)
Computer (11)
Alleged second human (9)
6.1 unique identifier (4) of first human (6)
6.2 unique identifier (7) of second human (9)
6.3 first fingerprint data (12) alleged to be of first human (6)
6.4 second fingerprint data (14) alleged to be of second human (9)
6.5 determine if 6.3 an 6.4 is conducted within a predetermined time interval, if yes start 6.6
6.6 compare retrieved first fingerprint data (12) to the stored fingerprint data (5) of the first human (6) and compare retrieved second fingerprint data (14) to the stored fingerprint data (8) of the second human (9)
6.7 provide positive indication (15) when a match is confirmed for both the first fingerprint data (12) compared to the stored fingerprint data (5) of the first human (6) and the second fingerprint data (14) compared to the stored fingerprint data (8) of the second human (9)

Fig. 7

Computer (11)



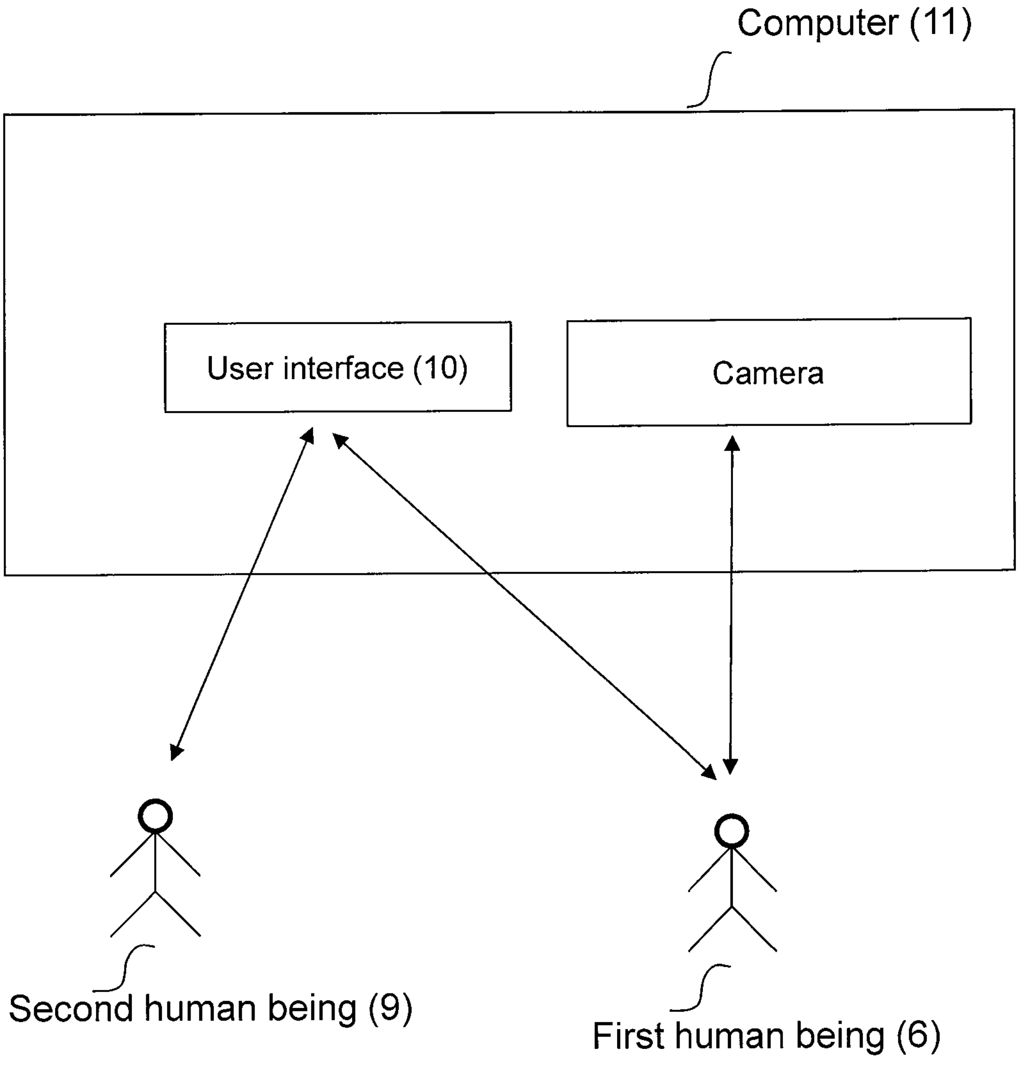

Computer (11)
User interface (10)
Camera
Second human being (9)
First human being (6)

Fig. 8

INTERNATIONAL SEARCH REPORT

International application No.
PCT/SE2018/050351

A. CLASSIFICATION OF SUBJECT MATTER

IPC: 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: G06F, G06K, H04L

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

SE, DK, FI, NO classes as above

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

EPO-Internal, PAJ, WPI data, COMPENDEX, INSPEC

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	CN 105260643 A (NANCHANG OUFEI BIOLOGY IDENTIFICATION TECHNOLOGY CO LTD ET AL), 20 January 2016 (2016-01-20); abstract --	1-10
A	US 20070198436 A1 (WEISS KENNETH P), 23 August 2007 (2007-08-23); abstract; paragraphs [0164]-[0173]; figures 22A,22B --	1-10
A	KR 20030086527 A (PLUSTEC CO LTD), 10 November 2003 (2003-11-10); abstract --	1-10
A	KR 20020011577 A (LEE SOON CHAE), 9 February 2002 (2002-02-09); abstract --	1-10

☒ Further documents are listed in the continuation of Box C. ☒ See patent family annex.

* Special categories of cited documents:

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

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

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

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

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

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

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

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

"&" document member of the same patent family

Date of the actual completion of the international search 06-09-2018	Date of mailing of the international search report 06-09-2018
Name and mailing address of the ISA/SE Patent- och registreringsverket Box 5055 S-102 42 STOCKHOLM Facsimile No. + 46 8 666 02 86	Authorized officer Ralf Boström Telephone No. + 46 8 782 28 00

Continuation of: second sheet

International Patent Classification (IPC)

G06F 21/32 (2013.01)
G06K 9/00 (2006.01)
H04L 9/32 (2006.01)

CN	105260643	A	20/01/2016	NONE			
US	20070198436	A1	23/08/2007	EP	1987463	A1	05/11/2008
				US	7805372	B2	28/09/2010
				US	9530137	B2	27/12/2016
				US	20160162902	A1	09/06/2016
				US	20160155121	A1	02/06/2016
				US	8538881	B2	17/09/2013
				US	8271397	B2	18/09/2012
				US	8001055	B2	16/08/2011
				US	7809651	B2	05/10/2010
				US	20140096216	A1	03/04/2014
				US	20130024374	A1	24/01/2013
				US	20110258120	A1	20/10/2011
				US	20070289000	A1	13/12/2007
				US	20070288758	A1	13/12/2007
				US	9100826	B2	04/08/2015
				WO	2007145687	A1	21/12/2007
KR	20030086527	A	10/11/2003	NONE			
KR	20020011577	A	09/02/2002	KR	100377522	B1	26/03/2003