



(51) International Patent Classification:
G06K 9/00 (2006.01)

(21) International Application Number:
PCT/SE2018/050422

(22) International Filing Date:
25 April 2018 (25.04.2018)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
1750582-7 11 May 2017 (11.05.2017) SE

(71) Applicant: **FINGERPRINT CARDS AB** [SE/SE]; Box 2412, 403 16 Göteborg (SE).

(72) Inventors: **NILSSON, René**; Klippanvägen 37, 241 33 Es-löv (SE). **SETTERBERG, Eric**; Distansgatan 65, 421 70 Västra Frölunda (SE).

(74) Agent: **KRANSELL & WENNBORG KB**; Box 2096, 403 12 Göteborg (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).

Declarations under Rule 4.17:

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

Published:

— with international search report (Art. 21(3))
— 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: POST VERIFICATION FINGERPRINT IMAGE CAPTURE

(57) Abstract: The invention relates to a method of a fingerprint sensing system (101) arranged in an electronic device (100) of capturing fingerprint data of a user contacting a fingerprint sensor (102) of the fingerprint sensing system, and a fingerprint sensing system performing the method.

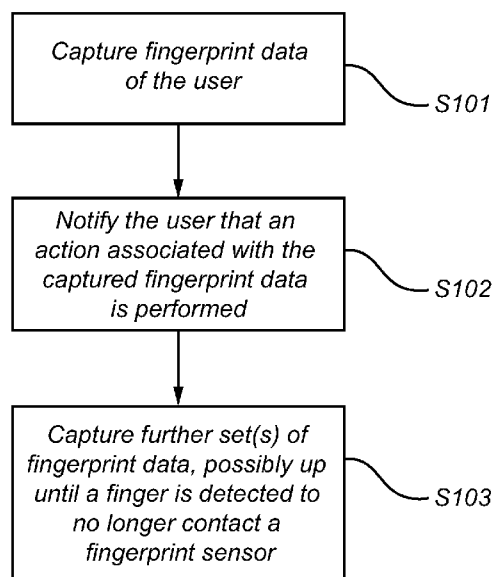


Fig. 4

POST VERIFICATION FINGERPRINT IMAGE CAPTURE

TECHNICAL FIELD

The invention relates to a method of a fingerprint sensing system arranged in an electronic device of capturing fingerprint data of a user contacting a fingerprint sensor of the fingerprint sensing system, and a fingerprint sensing system performing the method.

BACKGROUND

Electronic devices such as smart phones, laptops, remote controls, tablets, smart cards, etc., may use fingerprint recognition e.g. to allow a user to access the device, to authorize transactions carried out using the electronic device, or to authorize the user for accessing a service via the electronic device.

Hence, the electronic device, being for example a smart phone, is equipped with a fingerprint sensor on which the user places her finger in order for the sensor to capture an image of the fingerprint and compare the recorded fingerprint with a pre-stored, authenticated fingerprint template. If the recorded fingerprint matches the pre-stored template, the user is authenticated and the smart phone will perform an appropriate action, such as transitioning from locked mode to unlocked mode, in which the user is allowed access to the smart phone.

A problem in the art is that when capturing a fingerprint with the fingerprint sensor resulting in the electronic device performing an appropriate action based on the captured fingerprint, it is desirable that the time period from the capturing of the fingerprint to the action being performed is as short as possible, while at the same time ensuring capturing fingerprint data of sufficient quality. Generally, a short period of capturing fingerprint data results in poor-quality fingerprint data. Conversely, high-quality fingerprint data generally requires a longer period of capturing fingerprint data sets.

SUMMARY

An object of the present invention is to solve, or at least mitigate, this problem in the art and thus to provide an improved method of capturing fingerprint data of a user.

This object is attained in a first aspect of the invention by a method of a fingerprint sensing system arranged in an electronic device of capturing fingerprint data of a user contacting a fingerprint sensor of the fingerprint sensing system. The method comprises capturing initial fingerprint data of the user, controlling the electronic device to notify the user that an action associated with the captured initial fingerprint data is performed, and capturing further fingerprint data after the initial fingerprint data associated with the performed action has been captured but before the fingerprint sensor no longer detects a finger contacting the fingerprint sensor.

10 This object is attained in a second aspect of the invention by a fingerprint sensing system arranged in an electronic device, the system comprising a fingerprint sensor configured to capture fingerprint data of a user contacting the fingerprint sensor. The fingerprint sensor is configured to capture initial fingerprint data of the user, and a processing unit of the fingerprint sensing
15 system is configured to control the electronic device to notify the user that an action associated with the captured initial fingerprint data is performed. The fingerprint sensor is further configured to capture further fingerprint data after the initial fingerprint data associated with the performed action has been captured but before the fingerprint sensor no longer detects a finger
20 contacting the fingerprint sensor.

Hence, after the fingerprint sensor has captured initial fingerprint data of the user, the initial fingerprint data being used for instance for authenticating the user in order to unlock a smart phone in which the fingerprint sensing system is arranged by matching the captured initial fingerprint data to a previously
25 enrolled fingerprint template, the sensor will continue to capture further fingerprint data, possibly up until a moment where the sensor no longer detects a finger contacting the fingerprint sensor.

Hence, even though the initially captured fingerprint results in an appropriate action of which the user is notified, such as the smart phone
30 being unlocked after successful authentication of the user, the sensor will continue to capture further fingerprint data.

Since the user will not instantly remove her finger from the sensor, but will remain in contact with the sensor for a shorter (or longer) time period after the initial fingerprint data has been captured and the phone has been unlocked, the fingerprint system of the invention will advantageously use that
5 time period to capture further fingerprint data of the user.

Advantageously, the method of the invention provides for a short period of registering the users' fingerprint for the purpose of performing an action based on the registered fingerprint, and also facilitates capturing further fingerprint data which is required for ultimately obtaining a high-quality
10 representation of a fingerprint of the user from the further captured fingerprint data.

After the further fingerprint data has been captured, which typically is of a higher quality than the initially captured fingerprint data resulting in the user being notified of an action taken by the fingerprint sensing system, a number
15 of measures to be taken can be envisaged.

In an embodiment, the captured further fingerprint data is compared to the captured initial fingerprint data in order to ensure that the authentication based on the initial fingerprint data indeed was correct.

In an alternative embodiment, the captured further fingerprint data is
20 compared to the enrolled fingerprint template in order to ensure that the authentication based on the initial fingerprint data indeed was correct

If the matching is unsuccessful, the user will in an embodiment be requested to state her security credentials, for instance by entering her pin code via a display of the smart phone.

25 In a further embodiment a quality of the captured initial fingerprint data is determined, and if the determined quality exceeds a predetermined enrolment threshold value, the captured initial fingerprint data is enrolled as a new fingerprint data template.

In still another embodiment, a quality of the captured further fingerprint
30 data is determined, and if the determined quality exceeds a predetermined

quality threshold value, the enrolled fingerprint data template is updated based on the captured further fingerprint data.

Generally, all terms used in the claims are to be interpreted according to their ordinary meaning in the technical field, unless explicitly defined otherwise
5 herein. All references to "a/an/the element, apparatus, component, means, step, etc." are to be interpreted openly as referring to at least one instance of the element, apparatus, component, means, step, etc., unless explicitly stated otherwise. The steps of any method disclosed herein do not have to be performed in the exact order disclosed, unless explicitly stated.

10 **BRIEF DESCRIPTION OF THE DRAWINGS**

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

Figure 1 shows an electronic device in the form of a smart phone in which the present invention may be implemented;

15 Figure 2 shows a view of a fingerprint sensor onto which a user places the finger;

Figure 3 shows a fingerprint sensor being part of a fingerprint sensing system according to an embodiment;

20 Figure 4 illustrates a flowchart of the method of capturing fingerprint data of a user according to an embodiment of the present invention;

Figure 5 illustrates a flowchart of the method of capturing fingerprint data of a user according to a further embodiment of the present invention;

Figure 6a illustrates a sequence of fingerprint data captured at four different instances in time;

25 Figure 6b illustrates a flowchart of the method of capturing fingerprint data of a user according to still a further embodiment of the present invention;

Figure 7 illustrates a flowchart of the method of capturing fingerprint data of a user according to yet a further embodiment of the present invention;

Figure 8a illustrates another sequence of fingerprint data captured at four different instances in time; and

Figure 8b illustrates a flowchart of the method of capturing fingerprint data of a user according to yet a further embodiment of the present invention.

5 DETAILED DESCRIPTION

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

Figure 1 shows an electronic device in the form of a smart phone 100 in which
15 the present invention may be implemented. The smart phone 100 is equipped with a fingerprint sensor 102 and a display unit 104 with a touch screen interface 106. The fingerprint sensor 102 may, for example, be used for unlocking the mobile phone 100 and/or for authorizing transactions carried out using the mobile phone 100, etc. The fingerprint sensor 102 may
20 alternatively be placed on the backside of the mobile phone 100. It is noted that the fingerprint sensor 102 could be integrated in the display unit/touch screen or form part of a smart phone home button.

It is understood that the fingerprint sensor 102 according to embodiments of the invention may be implemented in other types of electronic devices, such
25 as laptops, remote controls, tablets, smart cards, smartwatches, etc., or any other type of present or future similarly configured device utilizing fingerprint sensing.

Figure 2 illustrates a somewhat enlarged view of the fingerprint sensor 102 onto which a user places her finger 201. In the case of employing a capacitive
30 sensing technology, the fingerprint sensor 102 is configured to comprise a

plurality of sensing elements. A single sensing element (also denoted as a pixel) is in Figure 2 indicated by reference numeral 202.

Figure 3 shows the fingerprint sensor 102 being part of a fingerprint sensing system 101. The fingerprint sensing system 101 comprises the fingerprint
5 sensor 102 and a processing unit 103, such as a microprocessor, for controlling the fingerprint sensor 102 and for analysing captured fingerprints. The fingerprint sensing system 101 further comprises a memory 105. The fingerprint sensing system 101 in turn, typically, forms part of the electronic device 100 as exemplified in Figure 1. A local memory 108 such as
10 a one-time programmable (OTP) memory, flash memory, or random access memory (RAM) may be embedded in the sensor die.

Now upon an object contacting the fingerprint sensor 102, the sensor 102 will capture an image of the object in order to have the processing unit 103 determine whether the object is a fingerprint of an authorised user or not by
15 comparing the captured fingerprint to one or more authorised fingerprint templates pre-stored in the memory 105.

The fingerprint sensor 102 may be implemented using any kind of current or future fingerprint sensing principle, including for example capacitive, optical, ultrasonic or thermal sensing technology. Currently, capacitive sensing is
20 most commonly used, in particular in applications where size and power consumption are important. Capacitive fingerprint sensors provide an indicative measure of the capacitance between (see Figure 2) several sensing elements 202 and a finger 201 placed on the surface of the fingerprint sensor 102. Acquisition of a fingerprint image is typically performed using a
25 fingerprint sensor 102 comprising a plurality of sensing elements 202 arranged in a two-dimensional manner.

In a general authorization process, the user places her finger 201 on the sensor 102 for the sensor to capture an image of the fingerprint of the user. The processing unit 103 evaluates the captured fingerprint and compares it to
30 one or more authenticated fingerprint templates stored in the memory 105. If the recorded fingerprint matches the pre-stored template, the user is

authenticated and the processing unit 103 will typically instruct the smart phone 100 to perform an appropriate action, such as transitioning from locked mode to unlocked mode, in which the user is allowed access to the smart phone 100.

5 With reference again to Figure 3, the steps of the method performed by the fingerprint sensing system 101 are in practice performed by the processing unit 103 embodied in the form of one or more microprocessors arranged to execute a computer program 107 downloaded to the storage medium 105 associated with the microprocessor, such as a Random Access Memory
10 (RAM), a Flash memory or a hard disk drive. The processing unit 103 is arranged to cause the fingerprint sensing system 101 to carry out the method according to embodiments when the appropriate computer program 107 comprising computer-executable instructions is downloaded to the storage medium 105 and executed by the processing unit 103. The storage medium
15 105 may also be a computer program product comprising the computer program 107. Alternatively, the computer program 107 may be transferred to the storage medium 105 by means of a suitable computer program product, such as a Digital Versatile Disc (DVD) or a memory stick. As a further alternative, the computer program 107 may be downloaded to the storage
20 medium 105 over a network. The processing unit 103 may alternatively be embodied in the form of a digital signal processor (DSP), an application specific integrated circuit (ASIC), a field-programmable gate array (FPGA), a complex programmable logic device (CPLD), etc. It should further be understood that all or some parts of the functionality provided by means of
25 the processing unit 103 may be at least partly integrated with the fingerprint sensor 102.

Now, when the user places her finger on the fingerprint sensor 102, either for initially enrolling the fingerprint template of the user in the fingerprint sensing system 101 or subsequently when comparing a captured fingerprint
30 of the user with the enrolled template for authentication purposes, the user is notified when the fingerprint sensing system 101 has enrolled and/or authenticated the user. Preferably, the period of time elapsing from the moment when the user places her finger on the sensor 102 up until the

moment when the fingerprint sensing system 101 has completed enrolment and/or authentication and thus notifies the user accordingly should be as short as possible to avoid that the enrolment/authentication process is perceived as slow and tedious by the user.

- 5 However, from a general point of view, the shorter the enrolment/authentication period, the poorer the quality of the captured fingerprint data; during the time period from the moment of the sensor 102 detecting a finger contact until the user is notified that the enrolment/authentication is completed and the user thus removes her finger
10 from the sensor 102, the sensor may have captured fingerprint data of a quality sufficient enough to complete the enrolment/authentication process but which is still far from being considered a top-quality representation of the fingerprint of the user.

- Figure 4 illustrates a flowchart of a method according to the invention of
15 capturing fingerprint data of a user.

- Hence, in a first step S101, the user places her finger on a surface of a sensing area of the fingerprint sensor 102, for instance by placing her thumb on a home button of the smart phone 100, under which the sensor 102 is arranged, whereupon the sensor 102 captures initial fingerprint data of the
20 user. It is noted that a number of sets of fingerprint data may be captured by the sensor.

In this exemplifying embodiment, it is assumed that the user desires to perform an authentication process for having her smart phone 100 transition from a locked to an unlocked state.

- 25 After the sensor 102 has captured one or more sets of initial fingerprint data of the user, the user is notified in step S102 that an action associated with the captured initial fingerprint data is completed, in this particular example the notification comes in the form of unlocking the mobile phone 100 and displaying the home screen of the phone to the user.

Now, the user will not instantly remove her finger from the sensor but will remain in contact with the sensor 102 for a shorter (or longer) time period after the phone 100 has been unlocked; even if the user would remove her finger, there will still be a period of time when further fingerprint data can be
5 captured.

Thus, after the initial fingerprint data has been captured that resulted in the issued notification in the form of the phone 100 being unlocked, the sensor 102 will continue to capture fingerprint data in step S103, possibly up until the moment where the fingerprint sensor 102 no longer detects a finger
10 contacting the fingerprint sensor.

Advantageously, the method of the invention provides for a short period of registering the users' fingerprint for the purpose of performing an action based on the registered fingerprint, and also facilitates capturing further fingerprint data which is required for ultimately obtaining a high-quality
15 representation of a fingerprint of the user from the further captured fingerprint data.

After the further fingerprint data has been captured, which oftentimes is of a higher quality than the initially captured fingerprint data resulting in the user being notified of an action taken by the fingerprint sensing system 100, a
20 number of measures to be taken can be envisaged.

In a first exemplifying embodiment, with reference to Figure 5, first, initial fingerprint data F1 is captured by the sensor 102. In step S101a, the processing unit 103 compares the first fingerprint data F1 to a previously enrolled fingerprint template FT, and if there is a match, the user is
25 authenticated and the smart phone 101 is controlled by the processing unit 103 to transit to its unlocked state. If not, the user is not authenticated, and is typically requested to enter her pin code via the display of the phone 100.

It is noted that the process in practice may require further steps well known to a skilled person, such as for instance one or more feature extraction steps
30 where details pertaining to ridges of the captured fingerprint of the user, e.g.

ridge endings, bifurcations, and short ridges, are extracted and processed in order to represent the user's fingerprint.

- Now, after the first fingerprint data F1 - which resulted in the authentication of the user - has been captured by the sensor 102, the sensor continues to
- 5 capture one or more further sets of fingerprint data in step S103, in the following referred to as second fingerprint data F2. It is noted that the capturing of the further fingerprint data F2 typically commences directly after the capturing of the first fingerprint data, and is thus typically performed in parallel with the matching and notifying steps S101a and S102.
- 10 Advantageously, in order to have the fingerprint sensing system 101 provide a high level of security level, the processing unit 103 proceeds to Step S104 where it is verified that the second, higher-quality fingerprint data F2 and the first fingerprint data F.

- If the first fingerprint data F1 that was utilized to unlock the phone 100
- 15 differs from the subsequently captured second fingerprint F2 to such an extent that it is questionable whether the first fingerprint F1 is equal to the second "better" fingerprint F2, the user is not authenticated, the fingerprint sensing system 101 takes an appropriate security measure, such as e.g. instantly locking the phone 100 and requesting the user to enter her security
- 20 credentials in step 105, for instance her pin code, in order to unlock the smart phone 100.

- Alternatively in step S104, the second fingerprint F2 is compared to enrolled template FT, and if there is no match the user is not authenticated, wherein the fingerprint sensing system 101 takes an appropriate security measure and
- 25 requests the user to enter her security credentials in step 105.

Figure 6a illustrates a sequence of fingerprint data captured at four different instances in time. At a first instant of time t1, the fingerprint sensor 102 captures fingerprint data where the finger of the user has not been fully pressed against a surface of a sensing area of the fingerprint sensor 102.

At a second instant of time t_2 , the fingerprint sensor 102 captures fingerprint data where the finger of the user is slightly harder pressed against the surface of the sensing area of the fingerprint sensor 102, while a third instant of time t_3 , the finger of the user is further pressed against the surface of the sensing area of the fingerprint sensor 102.

At the fourth instant of time t_4 , the finger of the user is fully pressed against the surface of the sensing area of the fingerprint sensor 102, and high-quality fingerprint data is thus captured.

In a second exemplifying embodiment, with reference to Figure 6b, the fingerprint sensing system 101 will utilize captured second fingerprint data F2 to improve the enrolled template FT.

As in the embodiment of Figure 5, first fingerprint data F1 (illustrated on a left-hand side of the flowchart) is captured by the sensor 102 in step S101. In step S101a, the processing unit 103 compares the first fingerprint data F1 to a previously enrolled fingerprint template FT, and if there is a match, the user is authenticated and the smart phone 101 is controlled by the processing unit 103 to transit to its unlocked state. If not, the user is not authenticated, and is typically requested to enter her pin code via the display of the phone 100.

The sensor 102 also captures second fingerprint data F2 in step S103, and in step S104 the processing unit 103 verifies in step S104 that the second, higher-quality fingerprint data F2 matches the first fingerprint data F1.

Alternatively in step S104, the second fingerprint F2 is compared to the enrolled template FT, and if there is no match the user is not authenticated, wherein the fingerprint sensing system 101 takes an appropriate security measure and requests the user to enter her security credentials in step 105.

In this particular embodiment, the second fingerprint data F2 is indeed considered to match the first fingerprint data F1, and the processing unit 103 proceeds to step S106, in which the quality of the second fingerprint data F2 is assessed. In this example, the processing unit 103 determines whether the quality of the second fingerprint data exceeds a predetermined quality

threshold T_Q . If that is the case, the second fingerprint F_2 is considered to be of a higher quality than the enrolled template FT , and will be used in step S_{107} to either improve the enrolled template, or possibly even replace the enrolled template FT . As is illustrated on a left-hand side of the flowchart, the
5 second fingerprint data F_2 is of a higher quality than the enrolled template FT

As an example, the quality of the second fingerprint f_2 may be assessed by determining a sensor coverage area of the fingerprint, where a greater coverage area typically is better than a smaller area, or a matching value may
10 be associated with the second fingerprint data F_2 , where a better matching as compared to the first fingerprint data F_1 is given a higher matching value and the second fingerprint data F_2 is thus considered to be of a higher quality.

In a third exemplifying embodiment, with reference to Figure 7, an enrolment process will be described. Again, in a first step S_{101} , the user
15 places her finger on a surface of a sensing area of the fingerprint sensor 102, whereupon the sensor 102 captures first, initial fingerprint data F_1 of the user. It is noted that a number of sets of fingerprint data may be captured by the sensor.

In this exemplifying embodiment, it is assumed that the user is to be enrolled
20 by the fingerprint sensing system 101 arranged in the smart phone 100. Hence, fingerprint data to be subsequently used by the fingerprint sensing system 101 as a template for authenticating the user is registered at the phone 100.

In step S_{101b} , the processing unit 103 checks whether the quality of the
25 captured first fingerprint data F_1 is of sufficient quality to be enrolled in the system. For instance, this may be performed by determining the quality of the first fingerprint data F_1 and comparing the quality to a predetermined enrolment threshold value T_{EN} , and if the quality of F_1 exceeds the enrolment threshold value T_{EN} , the captured initial fingerprint data F_1 is
30 considered good enough to be enrolled with the system in step S_{101c} . If not,

further first fingerprint data is captured until fingerprint data can be enrolled.

After the sensor 102 has captured and enrolled the first fingerprint data F1 in the system, the user is notified in step S102 that an action associated with the
5 captured initial fingerprint data is completed, in this particular example by informing the user via the display of the phone 100 (and/or possibly even audibly) that the enrolment is complete.

However, as previously has been discussed, further, second fingerprint data is captured by the sensor 102 in step S103, possibly up until the moment
10 where the sensor 102 no longer detects contact with the user's finger.

The processing unit 103 then proceeds to step S106, in which the quality of the second fingerprint data F2 is assessed. In this example, the processing unit 103 determines whether the quality of the second fingerprint data exceeds a predetermined quality threshold T_Q . If that is the case, the second
15 fingerprint F2 is considered to be of a higher quality than the enrolled template FT, and will be used in step S107 to either improve the enrolled template, or possibly even replace the enrolled template FT.

Figure 8a illustrates a further sequence of fingerprint data captured at four different instances in time. At a first instant of time t_1 , the fingerprint sensor
20 102 captures fingerprint data where the finger of the user has not been fully pressed against a surface of a sensing area of the fingerprint sensor 102.

At a second instant of time t_2 , the fingerprint sensor 102 captures fingerprint data where the finger of the user is slightly harder pressed against the surface of the sensing area of the fingerprint sensor 102, while a third instant of time
25 t_3 , the finger of the user is further pressed against the surface of the sensing area of the fingerprint sensor 102.

At the fourth instant of time t_4 , the finger of the user is fully pressed against the surface of the sensing area of the fingerprint sensor 102, and high-quality fingerprint data is thus captured.

The appearance of the images captured in the sequence may be the result of sweat or moist on the user's finger, or alternatively the result of a malicious third party attempting to spoof the smart phone 100 with fake fingerprints.

In a further exemplifying embodiment, with reference to Figure 8b, a
5 sequence of images is captured and analysed, e.g. for determining if the mobile phone 100 is suspected to be subjected to a spoofing attempt.

First fingerprint data F1 is captured by the sensor 102. In step S101a, the processing unit 103 compares the first fingerprint data F1 to a previously enrolled fingerprint template FT, and if there is a match, the user is
10 authenticated and the smart phone 101 is controlled by the processing unit 103 to transit to its unlocked state. If not, the user is not authenticated, and is typically requested to enter her pin code via the display of the phone 100.

Now, after the first fingerprint data F1 - which resulted in the authentication of the user - has been captured by the sensor 102, the sensor continues to
15 capture second fingerprint data F2 in step S103. Again, it should be noted that the capturing of the further fingerprint data F2 typically commences directly after the capturing of the first fingerprint data, and is thus typically performed in parallel with the matching and notifying steps S101a and S102.

Further, third fingerprint data F3 is captured in step S103a and fourth
20 fingerprint data F4 is captured in step S103b. The captured sets of fingerprint data F1-F4 are illustrated on the left-hand side of the flowchart.

Advantageously, in order to have the fingerprint sensing system 101 provide a high level of security level, the processing unit 103 proceeds to Step S104 where it is verified that the second, higher-quality fingerprint data F2 and the
25 first fingerprint data F.

In this embodiment, the sequence of captured fingerprint data F1-F4 are analysed in step S104a, and if the sets of captured fingerprint data F1-F4 indicates a (sufficient) gradual change in the captured fingerprint print data, the processing unit 103 controls the smart phone 100 to perform a safety

measure, such as for instance requesting the user to enter her PIN code in step S105.

Alternatively, the processing unit 103 may analyse the sequence for finding artefacts indicating spoof. For instance, the second fingerprint data F2
5 presents a higher degree of sensing area coverage than the first fingerprint data F1. Known algorithms of spoof detection may be employed to find any artefacts. If a spoofing attempt has occurred, the method proceeds to step S105 where the user typically is requested to enter her PIN code.

To determine the gradual change, the processing unit 103 may compare each
10 set of captured fingerprint data with the immediately preceding captured set, and compute one or more change metrics for each comparison. If a value of a change metric exceeds a predetermined change threshold value, the change is considered to be sufficiently substantial to motivate a safety measure being taken in step S105. Further, a value of a change metric may be determined to
15 lie within a predetermined range delimited by a lower threshold value and an upper threshold in order for the object touching the sensor be considered to constitute a live finger. The predetermined range would typically be defined as a range which would comply with live fingers.

Change metric examples are for instance measures of sweat and degree of
20 deformation of a captured fingerprint.

Hence, F2 is compared to F1, F3 is compared to F2, and so on, and if one or more of the comparisons result in a change metric value exceeding the threshold value, the processing unit 103 makes the assessment that a spoofing attempt may have been undertaken, and an appropriate safety
25 measure is taken in step 105. The invention has mainly been described above with reference to a few embodiments. However, as is readily appreciated by a person skilled in the art, other embodiments than the ones disclosed above are equally possible within the scope of the invention, as defined by the appended patent claims.

CLAIMS

1. A method of a fingerprint sensing system (101) arranged in an electronic device (100) of capturing fingerprint data of a user contacting a fingerprint sensor (102) of the fingerprint sensing system (101), comprising:
 - 5 capturing (S101) initial fingerprint data of the user;
 - controlling (S102) the electronic device (100) to notify the user that the user has been successfully authenticated or enrolled using the captured initial fingerprint data; and
 - capturing (S103) further fingerprint data after the initial fingerprint data used for the successful authentication or enrolment has been captured but before the fingerprint sensor (102) no longer detects a finger contacting the fingerprint sensor (102).
2. The method of claim 1, further comprising:
 - 15 comparing (S101a) the captured initial fingerprint data to an enrolled fingerprint data template, and if there is a match the user is authenticated.
3. The method of claims 1 or 2, further comprising:
 - comparing (S104) the captured further fingerprint data to the captured initial fingerprint data, and if there is a match the user is authenticated.
4. The method of claims 1 or 2, further comprising:
 - 20 comparing (S104) the captured further fingerprint data to an enrolled fingerprint data template, and if there is a match the user is authenticated.
5. The method of claims 3 or 4, further comprising:
 - requesting (105) the user to enter her security credentials via the electronic device (100) if the captured further fingerprint data does not match the captured initial fingerprint data, or if the captured further fingerprint data does not match the enrolled fingerprint data template.
6. The method of anyone of the preceding claims, further comprising:
 - determining (S101b) a quality of the captured initial fingerprint data; and if the determined quality exceeds a predetermined enrolment threshold value;

enrolling (S101c) the captured initial fingerprint data as a fingerprint data template.

7. The method of any one of the preceding claims, further comprising:
determining (S106) a quality of the captured further fingerprint data;
5 and if the determined quality exceeds a predetermined quality threshold value;
updating (S107) an enrolled fingerprint data template based on the captured further fingerprint data.
8. The method of any one of the preceding claims, wherein the capturing
10 (S103) of further fingerprint data comprises:
capturing (S103a, s103b) a sequence of fingerprint data sets; and
determining (S104a), for said sequence, if a change in the captured fingerprint data has occurred, and if so
controlling (S105) the electronic device (100) to perform a safety
15 measure.
9. The method of claim 8, wherein the determining (S104a) if a change in the fingerprint data has occurred for captured sequence further comprises:
determining if for at least two of the captured fingerprint data sets in the sequence a change has occurred exceeding a predetermined change
20 threshold value, or being outside a predetermined allowed change range, in which case the electronic device (100) is controlled to perform a safety measure.
10. A fingerprint sensing system (101) arranged in an electronic device (100), the system comprising a fingerprint sensor (102) configured to
25 capture fingerprint data of a user contacting the fingerprint sensor (102),
the fingerprint sensor (102) being configured to:
capture initial fingerprint data of the user; the fingerprint sensing system (101) further comprising:
a processing unit (103) being configured to:
30 control the electronic device (100) to notify the user that the user has been successfully authenticated or enrolled using the captured initial

fingerprint data; the fingerprint sensor (102) further being configured to:
capture further fingerprint data after the initial fingerprint data
used for the successful authentication or enrolment has been captured but
before the fingerprint sensor (102) no longer detects a finger contacting the
5 fingerprint sensor (102).

11. The fingerprint sensing system (101) of claim 10, the processing unit
(103) further being configured to:

compare the captured initial fingerprint data to an enrolled fingerprint
data template, and if there is a match the user is authenticated.

10 12. The fingerprint sensing system (101) of claims 10 or 11, the processing
unit (103) further being configured to:

compare the captured further fingerprint data to the captured initial
fingerprint data, and if there is a match the user is authenticated.

13. The fingerprint sensing system (101) of claims 10 or 11, the processing
15 unit (103) further being configured to:

compare the captured further fingerprint data to an enrolled fingerprint
data template, and if there is a match the user is authenticated.

14. The fingerprint sensing system (101) of claims 12 or 13, the processing
unit (103) further being configured to:

20 request the user to enter her security credentials via the electronic
device (100) if the captured further fingerprint data does not match the
captured initial fingerprint data, or if the captured further fingerprint data
does not match the enrolled fingerprint data template.

15. The fingerprint sensing system (101) of any one of claims 10-14, the
25 processing unit (103) further being configured to, when controlling the
electronic device (100) to notify the user that an action associated with the
captured initial fingerprint data is performed:

control the electronic device (100) to notify the user that the user has
been successfully enrolled.

16. The fingerprint sensing system (101) of claim 15, the processing unit (103) further being configured to:

determine a quality of the captured initial fingerprint data; and if the determined quality exceeds a predetermined enrolment threshold value;

5 enrol the captured initial fingerprint data as a fingerprint data template.

17. The fingerprint sensing system (101) of any one of claims 10-16, the processing unit (103) further being configured to:

determine a quality of the captured further fingerprint data; and if the determined quality exceeds a predetermined quality threshold value;

10 update an enrolled fingerprint data template based on the captured further fingerprint data.

18. The fingerprint sensing system (101) of any one of claims 10-17, the processing unit (103) further being configured to, when capturing the further fingerprint data:

15 capture a sequence of fingerprint data sets; and

determine, for said sequence, if a change in the captured fingerprint print data has occurred, and if so

control the electronic device (100) to perform a safety measure.

19. The fingerprint sensing system (101) of claim 18, the processing unit (103) further being configured to, when determining if a change in the fingerprint data has occurred for captured sequence:

20 determine if for at least one of the captured fingerprint data sets in the sequence a change has occurred exceeding a predetermined change threshold value, or being outside a predetermined allowed change range, in which case
25 the electronic device (100) is controlled to perform a safety measure.

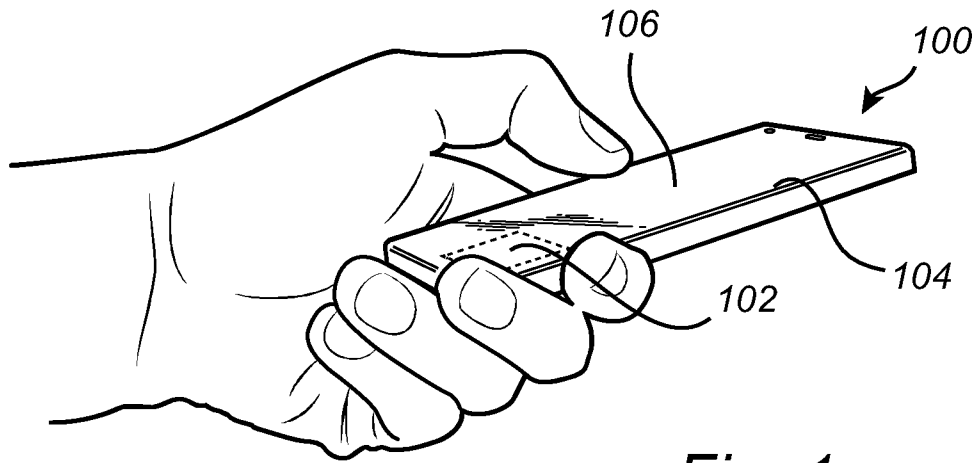
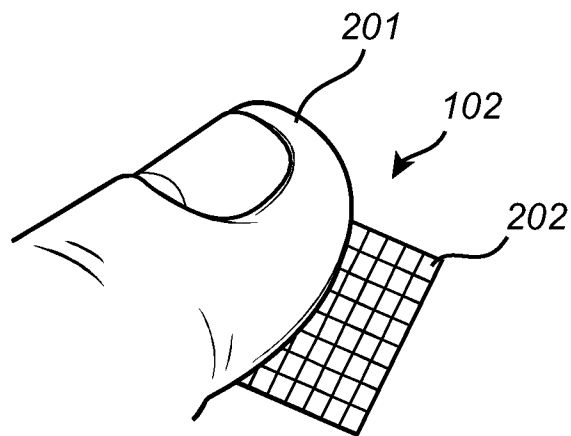
20. An electronic device (100) comprising the fingerprint sensing system (101) of any one of claims 10-19.

21. A computer program (107) comprising computer-executable instructions for causing the fingerprint sensing system (101) to perform steps
30 recited in any one of claims 1-9 when the computer-executable instructions

are executed on a processing unit (103) included in the fingerprint sensing system (101).

22. A computer program product comprising a computer readable medium (105), the computer readable medium having the computer program (107)
5 according to claim 21 embodied thereon.

1/9

*Fig. 1**Fig. 2*

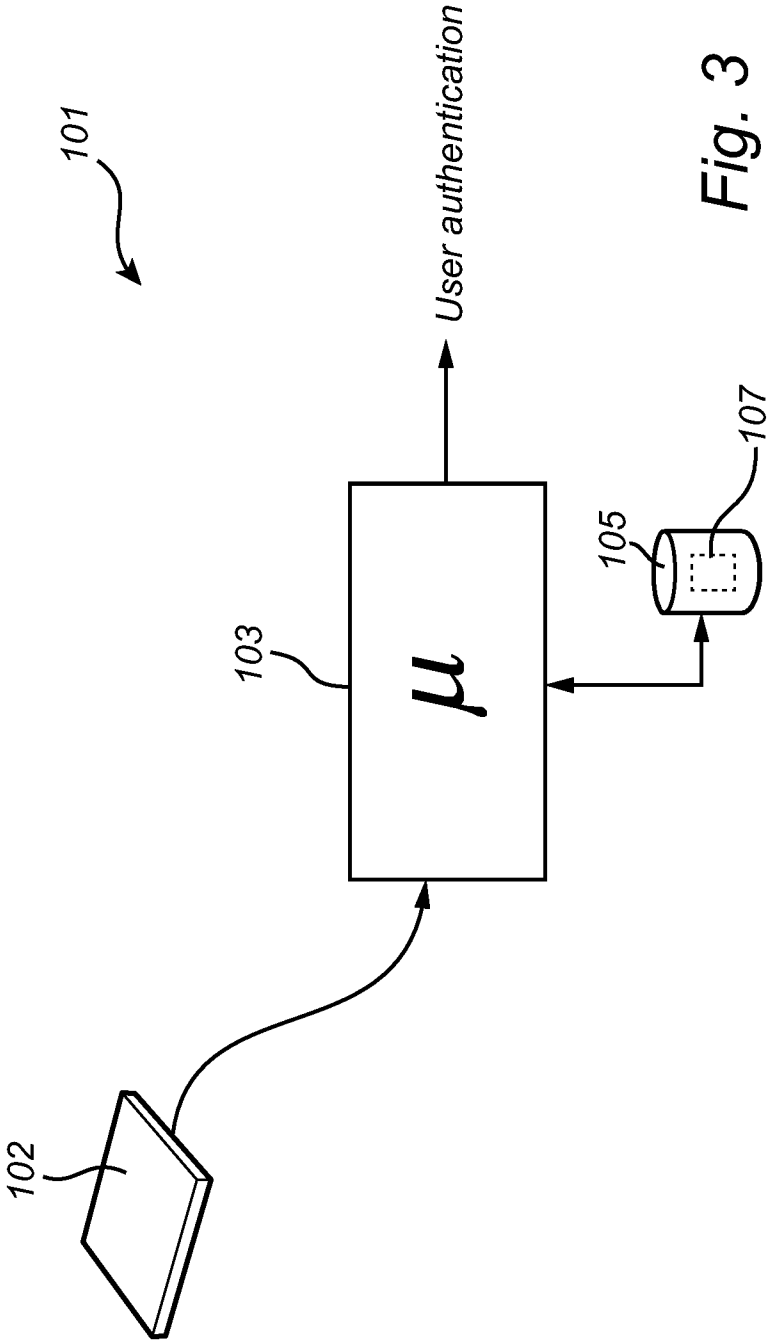
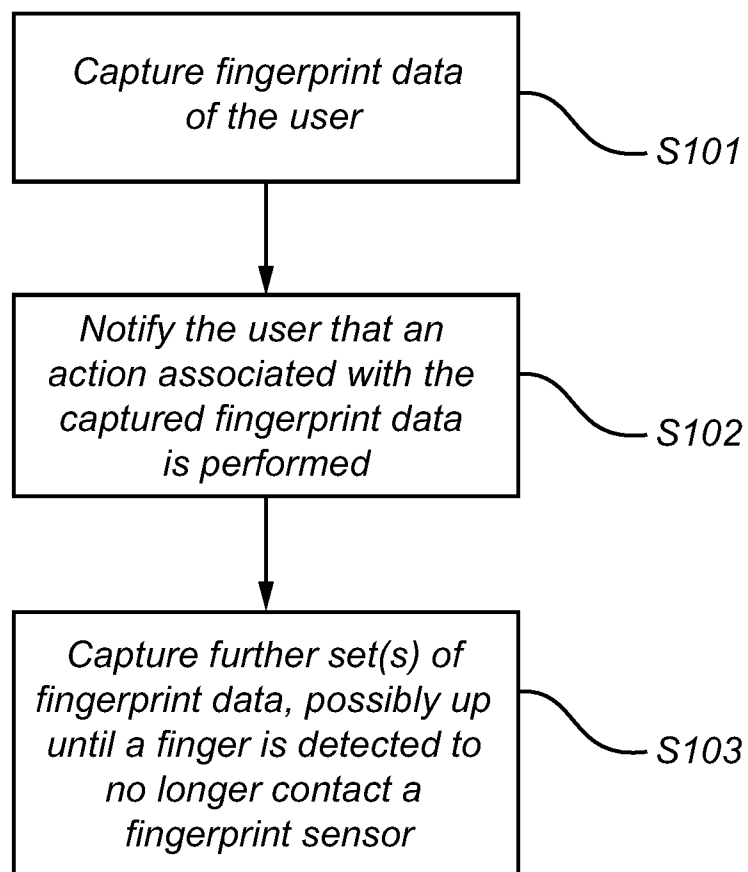


Fig. 3

3/9

*Fig. 4*

4/9

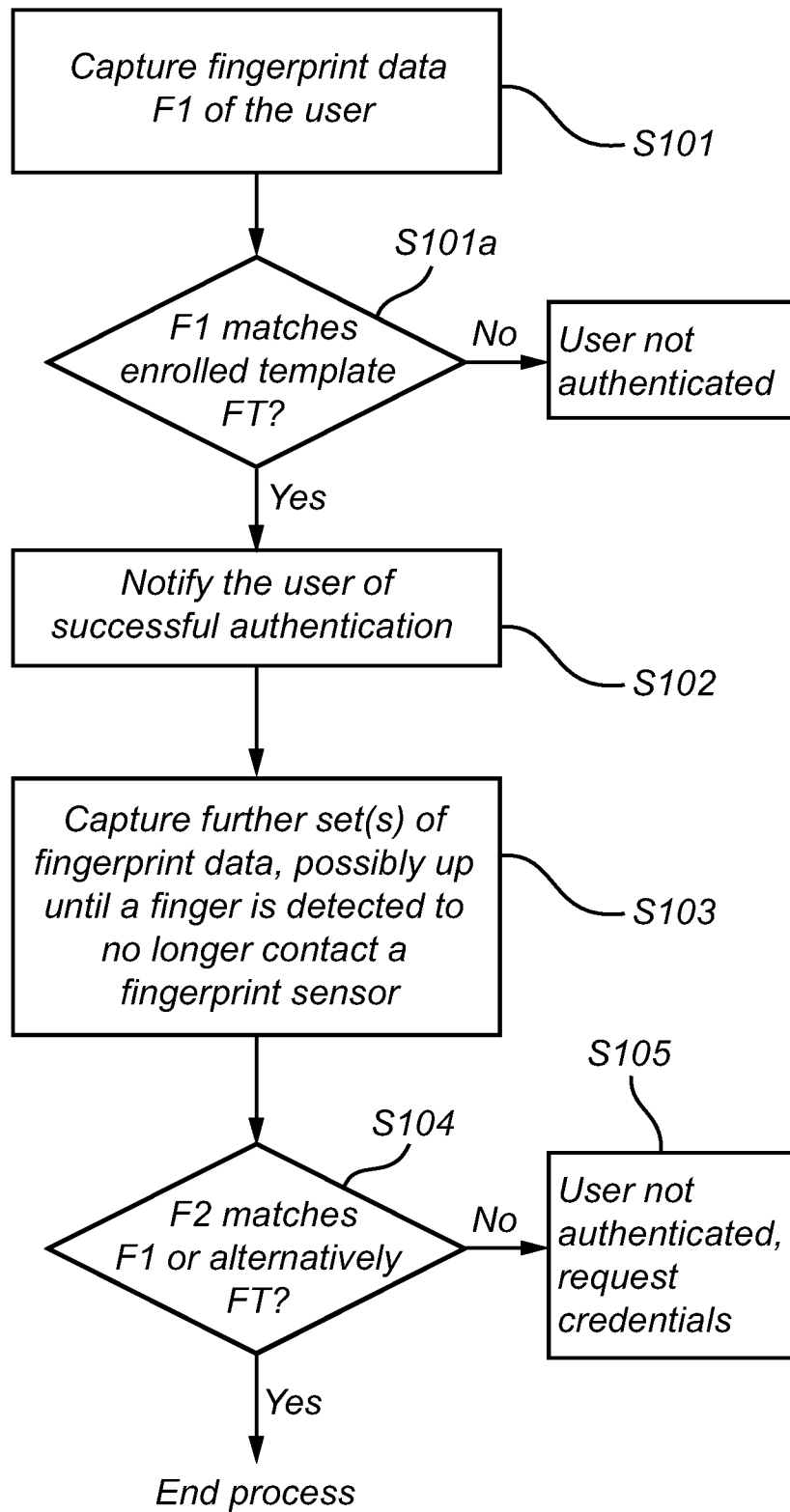


Fig. 5

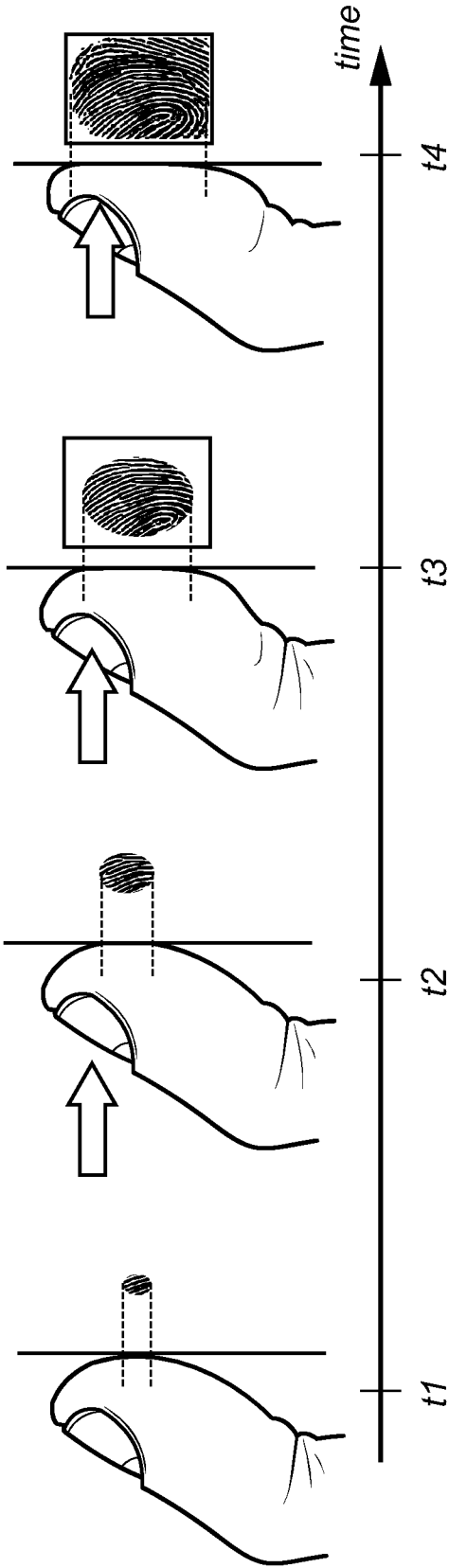
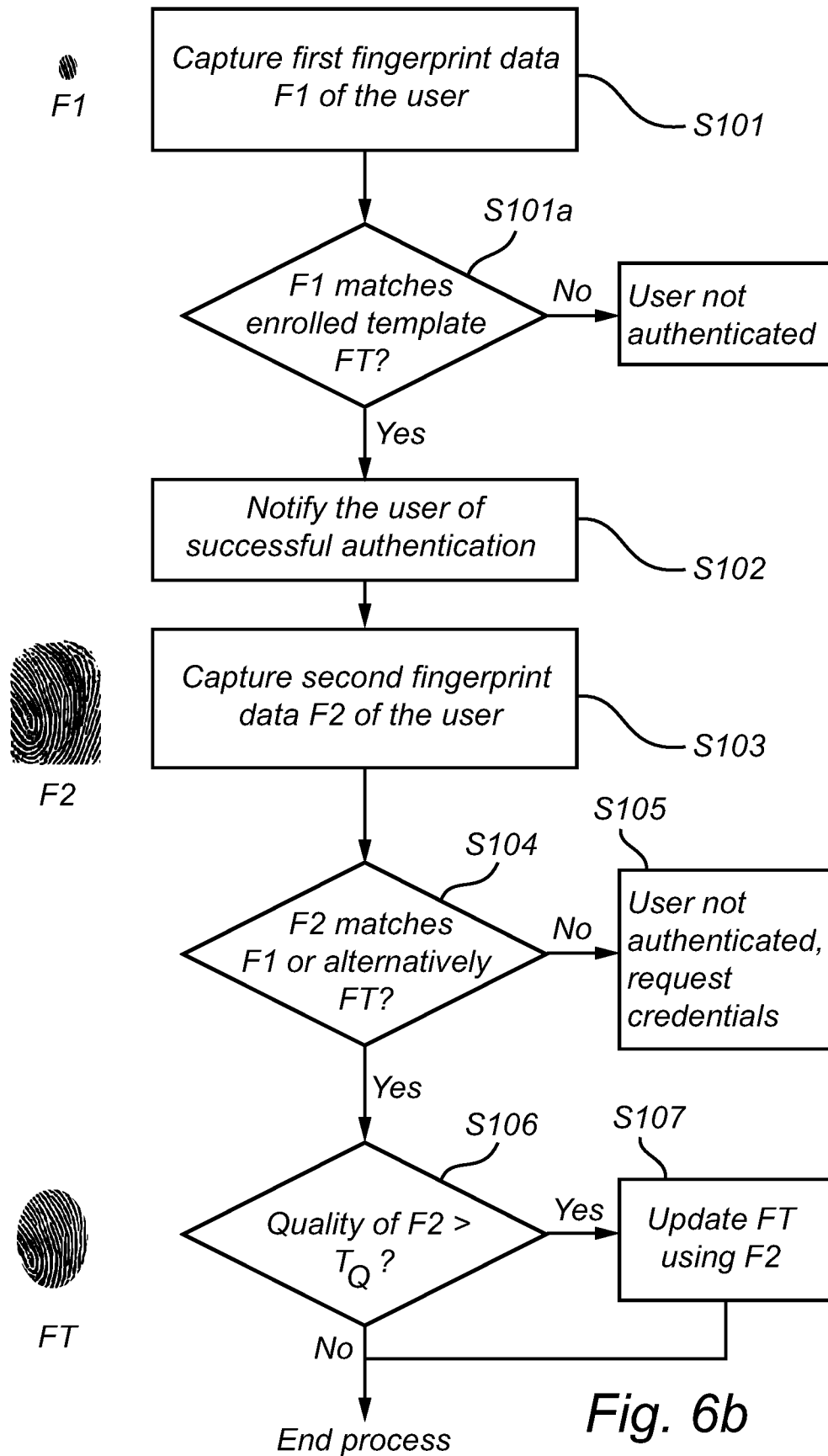


Fig. 6a

6/9



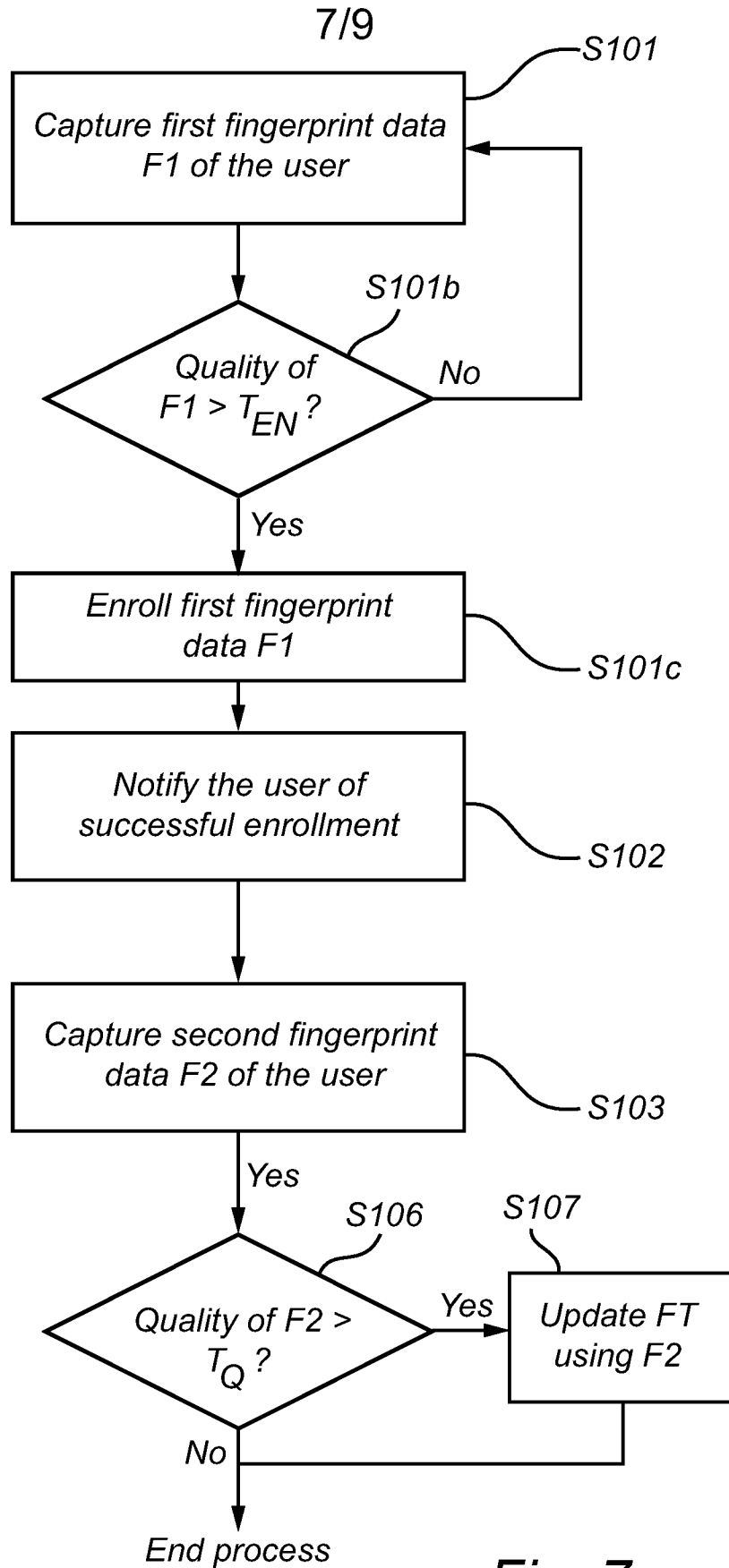
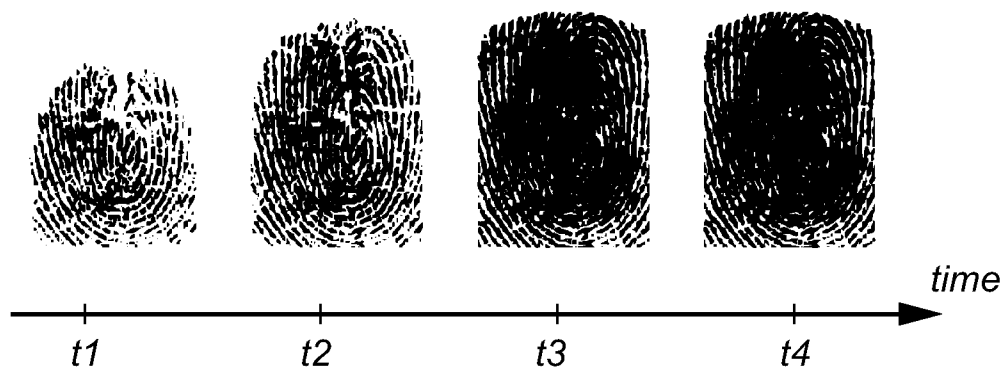


Fig. 7

8/9

*Fig. 8a*

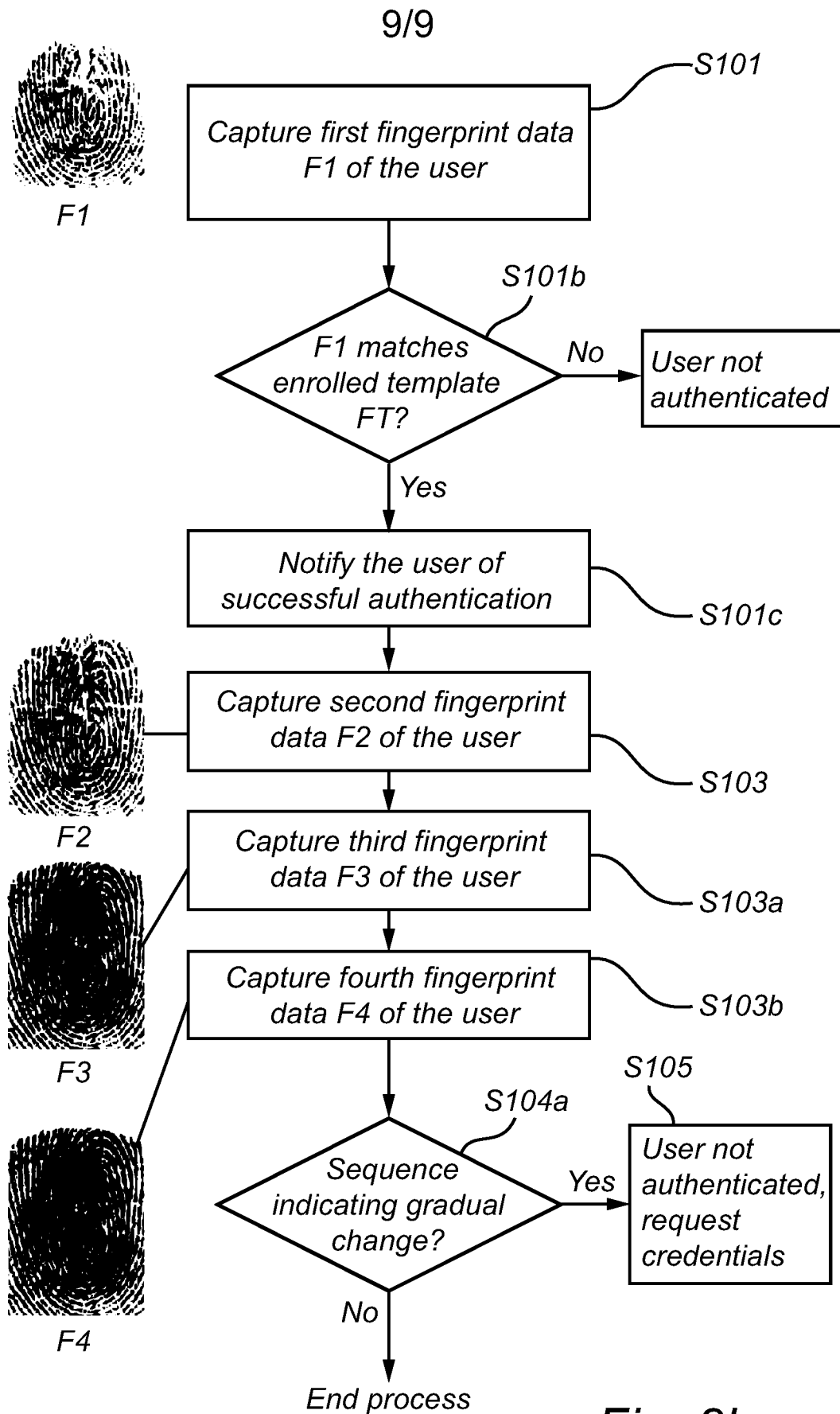


Fig. 8b

INTERNATIONAL SEARCH REPORT

International application No.
PCT/SE2018/050422

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: G06K

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, BIOSIS, COMPENDEX, EMBASE, INSPEC, MEDLINE, PUBCHEM, IBM-TDB

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	US 20150347816 A1 (BOSHRA MICHAEL), 3 December 2015 (2015-12-03); paragraphs [0004]-[0005], [0009], [0031]-[0032], [0036]; figures 3,7-8 --	1-22
A	US 20140003679 A1 (HAN BYRON B ET AL), 2 January 2014 (2014-01-02); paragraphs [0020], [0024], [0040]-[0046]; figure 4B --	1-22
A	US 20150350202 A1 (WEI JINPING), 3 December 2015 (2015-12-03); paragraphs [0070], [0072]-[0073], [0078]; figures 1,2 --	1-22



Further documents are listed in the continuation of Box C.



See patent family annex.

* Special categories of cited documents:	"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
"A" document defining the general state of the art which is not considered to be of particular relevance	"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
"E" earlier application or patent but published on or after the international filing date	"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
"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)	"&" document member of the same patent family
"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	

Date of the actual completion of the international search

03-09-2018

Date of mailing of the international search report

03-09-2018

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

Alexander Lakic

Telephone No. + 46 8 782 28 00

INTERNATIONAL SEARCH REPORT

International application No.
PCT/SE2018/050422

C (Continuation). DOCUMENTS CONSIDERED TO BE RELEVANT		
Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	US 20150349959 A1 (MARCINIAK CRAIG A), 3 December 2015 (2015-12-03); paragraphs [0054]-[0055]; figure 3 --	1-22
A	US 20160180146 A1 (SETTERBERG ERIC ET AL), 23 June 2016 (2016-06-23); paragraphs [0104]-[0105]; figures 12a,12b -- -----	1-22

INTERNATIONAL SEARCH REPORT

Information on patent family members

International application No.

PCT/SE2018/050422

US	20150347816 A1	03/12/2015	US	9858491 B2	02/01/2018
			US	20160086013 A1	24/03/2016
			US	9230152 B2	05/01/2016
US	20140003679 A1	02/01/2014	CN	104321786 A	28/01/2015
			DE	112013003258 T5	02/04/2015
			US	20170262688 A1	14/09/2017
			US	9665785 B2	30/05/2017
			US	20150139512 A1	21/05/2015
			US	20140301614 A1	09/10/2014
			US	8913802 B2	16/12/2014
			US	8913801 B2	16/12/2014
			WO	2014004642 A1	03/01/2014
US	20150350202 A1	03/12/2015	CN	103780736 A	07/05/2014
			EP	3096507 A4	13/09/2017
			US	9432367 B2	30/08/2016
			WO	2015106521 A1	23/07/2015
US	20150349959 A1	03/12/2015	CN	105279410 A	27/01/2016
			WO	2015183974 A1	03/12/2015
US	20160180146 A1	23/06/2016	CN	105981045 B	30/03/2018
			EP	3234864 A1	25/10/2017
			JP	2017538225 A	21/12/2017
			KR	20170080617 A	10/07/2017
			TW	201636806 A	16/10/2016
			TW	I592854 B	21/07/2017
			US	9646193 B2	09/05/2017
			WO	2016099382 A1	23/06/2016

Continuation of: second sheet
International Patent Classification (IPC)
G06K 9/00 (2006.01)