Internal distribution code:

(A) [-] Publication in OJ
(B) [-] To Chairmen and Members
(C) [-] To Chairmen
(D) [X] No distribution

Datasheet for the decision of 25 July 2019

Case Number: T 1241/13 - 3.5.06

Application Number: 05252731.4

Publication Number: 1653320

IPC: G06F1/00

Language of the proceedings: EN

Title of invention:
Data processing apparatus

Applicant:
Fujitsu Frontech Limited

Headword:
Continuous biometric authentication/FUJITSU

Relevant legal provisions:
EPC 1973 Art. 56

Keyword:
Inventive step - (no)

Decisions cited:

Catchword:

Europäisches Patentamt
European Patent Office
Office européen des brevets

Beschwerdekammern

Boards of Appeal

Chambres de recours

Boards of Appeal of the
European Patent Office
Richard-Reitzner-Allee 8
85540 Haar
GERMANY
Tel. +49 (0)89 2399-0
Fax +49 (0)89 2399-4465

Case Number: T 1241/13 - 3.5.06

D E C I S I O N
of Technical Board of Appeal 3.5.06
# of 25.07.2019

Appellant: (Applicant)	Fujitsu Frontech Limited 1776, Yanokuchi Inagi-shi, Tokyo 206-8555 (JP)
Representative:	Haseltine Lake Kempner LLP Lincoln House, 5th Floor 300 High Holborn London WC1V 7JH (GB)
Decision under appeal:	**Decision of the Examining Division of the European Patent Office posted on 21 December 2012 refusing European patent application No. 05252731.4 pursuant to Article 97(2) EPC.**

Composition of the Board:

Chairman	W. Sekretaruk
Members:	G. Zucka
	M. Müller

Summary of Facts and Submissions

I. The appeal is against the decision by the examining division, dispatched with reasons on 21 December 2012, to refuse European patent application 05252731.4, on the basis that claims 1 and 8 were not clear (Article 84 EPC 1973) and the subject-matter of those claims was not inventive (Article 56 EPC 1973). The following documents were cited during the first instance procedure:

D1 = WO 02/05478 A
D2 = EP 1 396 779 A
D3 = US 5 229 764 A
D4 = U. Geiger: "Generationswechel bei Bildschirmschreibern", SPS Magazin, Technik-Dokumentations Verlag, Marburg, vol. 2002, no. 8, August 2002, pages 1-2, XP002302406, ISSN: 0935-0187
D5 = US 5 629 981 A

Only D1 was relied upon in the reasons for the decision.

II. A notice of appeal was received on 20 February 2013, the appeal fee being paid on the same day. A statement of grounds of appeal was received on 17 April 2013.

III. The appellant requested that the decision under appeal be set aside and a patent granted on the basis of claims 1 to 8 filed with the grounds of appeal. The appellant made a conditional request for oral proceedings.

IV. The board issued a summons to oral proceedings. In an annex to the summons, the board set out its preliminary, negative opinion on the appeal.

V. On 16 August 2018, the appellant filed claims 1 to 8 of an auxiliary request.

VI. On 31 August 2018, the appellant announced that he would not attend the oral proceedings. The oral proceedings were subsequently cancelled.

VII. The appellant requests that the decision under appeal be set aside and a patent be granted on the basis of claims 1 to 8 of the main request filed with the grounds of appeal or claims 1 to 8 of the auxiliary request filed with his reply to the summons, and on the basis of description pages 1 to 45 and drawing sheets 1 to 16, both as originally filed.

VIII. Independent claim 1 of the main request reads as follows:

"A data-processing apparatus (1, 10, 13), comprising:
a data input unit (7-1, 7-2, 7-3, 7-4, 9-1, 9-2) for inputting data according to an operation of an operator;
a biological information input unit (8) for inputting biological information of the operator;
a biological information storage unit (4) for storing biological information of each of one or more operators beforehand in association with identification (41) of each of the one or more operators;
a data storage unit (6) for storing registration data;
a biological authentication unit (3); and
a data processing unit (5);

wherein the data-processing unit (5) issues (A3), on login of the operator to the data-processing apparatus, a first authenticate request;

in response to the first authenticate request, the biological authentication unit (3) authenticates (A3) the operator by comparing (B5) first biological information obtained (Bl) by the biological information input unit (8) with the stored biological information,

when authentication of the operator on the basis of the first biological information succeeds, the data-processing unit (5) registers (A5) the identification (41) stored in the biological information storage unit (4) in association with the first biological information,

when the data-processing unit (5) receives (A6; A5 ... A10), from the data input unit (7, 9),

first data that indicates an intention to register, into the data storage unit (6), input data that is input from the data input unit, or

second data that indicates an intention to access the registration data stored in the data storage unit (6),

the biological authentication unit (3) authenticates (A7; D3) the operator on the basis of second biological information obtained (C2) from the biological information input unit (8) by comparing (C4) the second biological information with the biological information stored in the biological information storage unit (4) in association with the registered identification of the operator currently using the apparatus, and

when authentication of the second biological information succeeds (C6), the data-processing unit (5) performs (A8; D4-D8) data processing based on the first or the second data;

and wherein the data-processing apparatus (1, 10, 13) further comprises:

a display unit (12) for displaying the registration data; and

a display control unit (11) for controlling the display unit (12) to display the registration data when receiving a display request (All) of the registration data from the data-processing unit (5),

wherein the data-processing unit (5) is adapted to repeatedly issue a second authenticate request,

for each time the data-processing unit (5) issues the second authenticate request, the biological authentication unit (3) authenticates the operator by way of the second biological information, with the second biological information being obtained anew from the biological information input unit (8), and

as long as the authentication based on the second biological information succeeds,

the data-processing unit (5) transmits the display request and the registration data stored in the data storage unit (6) to the display control unit (11), and

according to the display request, the display control unit (11) controls the display unit (12) to continue to display the registration data on the display unit (12)."

IX. Independent claim 1 of the auxiliary request additionally contains the following wording at the end:

", wherein

even after the authentication based on the second biological information has failed, the authentication based on the second biological information is repeatedly performed by the biological authentication unit (3), and

when the authentication based on the second biological information succeeds after the authentication based on the second biological information has failed, the display control unit (11) controls the display unit (12) to display the registration data".

Reasons for the Decision

1. *The admissibility of the appeal*

The appeal is admissible.

2. *The invention*

The invention relates to a data processing apparatus with a biometric authentication unit. Authentication takes place repeatedly and registration data will only be displayed as long as the operator can be successfully authenticated (see last part of claim 1), thereby preventing other parties to see said data (see grounds of appeal, page 2, lines 6 to 10).

3. *Main request - inventive step; Article 56 EPC 1973*

3.1 It is common ground that D1 is a suitable starting point for an inventive step analysis. The board considers that this document discloses a data processing apparatus, comprising:

a data input unit (see D1, page 6, last line: "handheld computer") for inputting data according to an operation of an operator;

a biological information input unit (see page 7, line 3: "biometric sensor") for inputting biological information of the operator;

a biological information storage unit for storing biological information of each of one or more operators beforehand in association with identification of each of the one or more operators (page 8, paragraph 2, second sentence: reference prints are stored in the host computer);

a data storage unit for storing registration data (in D1 these are stored in "user records"; see for instance page 9, last paragraph);

a biological authentication unit (host computer); and

a data processing unit (host computer);

wherein the data-processing unit issues, on login of the operator to the data-processing apparatus, a first authenticate request (see process described in figure 9A);

in response to the first authenticate request, the biological authentication unit authenticates the operator by comparing first biological information obtained by the biological information input unit with the stored biological information (matching of sensed print #1 with reference print #1; see figure 9B),

when authentication of the operator on the basis of the first biological information succeeds, the data-processing unit registers (the identification stored in the biological information storage unit in association with the first biological information (the application documents are not specific as to what "registers" means at this stage; the board holds that, in order to "enable user access" as shown in figure 9B of D1, the user should be identified, which means that the identification stored in the biological information storage unit should be matched with the first

biological information, i.e. the association between both should be "registered" at least in a broad sense of the word),

when the data-processing unit receives, from the data input unit,

first data that indicates an intention to register, into the data storage unit, input data that is input from the data input unit, or

second data that indicates an intention to access the registration data stored in the data storage unit (network access request to high security data; see figure 9A),

the biological authentication unit authenticates the operator on the basis of second biological information ("sensed print #2 in figure 9B) obtained from the biological information input unit by comparing the second biological information with the biological information stored in the biological information storage unit in association with the registered identification of the operator currently using the apparatus (figure 9B: matching sensed print #2 with reference print #2), and

when authentication of the second biological information succeeds, the data-processing unit performs data processing based on the first or the second data; and wherein the data-processing apparatus further comprises:

a display unit (handheld computer) for displaying the registration data; and

a display control unit for controlling the display unit to display the registration data when receiving a display request of the registration data from the data-processing unit (corresponds to granting the network access request in figure 9B).

3.2 In line with the appellant's statements in the grounds of appeal (page 1, line 27 to page 2, line 10), the salient difference between the subject-matter of claim 1 and the disclosure of D1 is therefore that:

the data-processing unit is adapted to repeatedly issue a second authenticate request,

for each time the data-processing unit issues the second authenticate request, the biological authentication unit authenticates the operator by way of the second biological information, with the second biological information being obtained anew from the biological information input unit, and

as long as the authentication based on the second biological information succeeds,

the data-processing unit transmits the display request and the registration data stored in the data storage unit to the display control unit, and

according to the display request, the display control unit controls the display unit to continue to display the registration data on the display unit.

3.3 From the grounds of appeal (page 2, lines 3 to 5), it is apparent that those distinguishing features intend to solve the problem of "eavesdropping", i.e. that of a third party being able to see the data, e.g. when the operator temporarily leaves the remote device.

3.4 In this respect, the board firstly notes that, although in claim 1 the registration data will presumably no longer display the registration data once authentication fails, these data will still be visible to a third party for a period of time between the last successful authentication and the unsuccessful authentication. The claim's wording does not specify

how frequently the second authentication request is repeated. Said period of time may therefore be long enough to allow an eavesdropper to be successful.

3.5 More importantly, the board considers that the problem of an unauthorised user getting access to the system after an authorised user has been authenticated is obvious. Contrary to what the appellant states (*ibid.*, page 2, lines 13 to 14), the problem is particularly acute also for handheld devices, e.g. because they could be stolen after their legitimate user has been authenticated.

The skilled person will be aware that the problem of eavesdropping concerns not only access to secure records (which is solved in D1 by the need to re-authenticate when such access takes place) but is more general, as any kind of access whilst posing as an authenticated user is obviously a potential security threat.

3.6 The skilled person will recognise that D3 addresses this problem (see D3, column 2, line 41 to column 3, line 7) and solves it by continuous biometric authentication, i.e. in the same manner as in claim 1. In D3, any use of the system, which would include the display of registration data, is blocked once authentication fails.

It is further noted that the apparatus of D1 would only require minimal adaptation to incorporate the teaching of D3, since the means for ensuring an easy continuous authentication are already present in that apparatus; see D1, page 11, last paragraph: it takes less than 1/10 of a second to capture a high-resolution image of a fingerprint.

3.7 The skilled person would thus combine the teaching of D1 and D3 and thereby arrive at the subject-matter of claim 1, which is consequently considered not inventive (Article 56 EPC 1973).

4. *Auxiliary request*

4.1 Independent claim 1 of the auxiliary request distinguishes itself from that of the main request in that it additionally contains the following wording at the end:

", wherein
even after the authentication based on the second biological information has failed, the authentication based on the second biological information is repeatedly performed by the biological authentication unit (3), and
when the authentication based on the second biological information succeeds after the authentication based on the second biological information has failed, the display control unit (11) controls the display unit (12) to display the registration data".

4.2 The appellant submits (reply to summons, page 2, first paragraph) and the board agrees that neither D1 nor D3 disclose or suggest these features.

4.3 However, when applying the teaching of D3 to the apparatus of D1 to solve the problem mentioned under 3.3 above, the skilled person will take into account that, when continuously scanning a fingerprint as in D1, it is not realistic to expect that the operator will be able to hold his or her finger constantly and

correctly on the sensor for any extended period of time. It would be considered rather user-unfriendly to block any use of the system simply because, at some moment, the fingerprint authentication fails. Instead of completely blocking the access, the skilled person would therefore ensure that the system waits some time, i.e. blocks the access only temporarily, and restores full access immediately when the operator again holds his or her finger correctly on the sensor.

4.4 In other words, even if the authentication based on the second information has failed (the finger was momentarily not placed correctly on the sensor), the authentication based on the second biological information would still be repeatedly performed by the biological authentication unit, and when the authentication based on the second biological information succeeds again after it has failed (the finger is now again placed correctly on the sensor), the display control unit will again control the display unit to display the registration data.

4.5 The skilled person would thus arrive at the subject-matter of claim 1 of the auxiliary request without the need for an inventive step.

The auxiliary request therefore also does not satisfy the requirement of Article 56 EPC 1973.

Order

For these reasons it is decided that:

The appeal is dismissed.

The Registrar: The Chairman:

L. Stridde W. Sekretaruk

Decision electronically authenticated