(19) Europäisches Patentamt
European Patent Office
Office européen des brevets

(11) EP 1 235 189 A1

(12) EUROPEAN PATENT APPLICATION

(43) Date of publication:
28.08.2002 Bulletin 2002/35

(51) Int Cl.[7]: **G07C 9/00**, G07F 7/00

(21) Application number: **01200723.3**

(22) Date of filing: **26.02.2001**

(84) Designated Contracting States:
AT BE CH CY DE DK ES FI FR GB GR IE IT LI LU MC NL PT SE TR
Designated Extension States:
AL LT LV MK RO SI

(71) Applicant: **Keyware Technologies**
8900 Ieper (BE)

(72) Inventor: **Hermand, Jean-Pierre,**
c/o Keyware Technologies
8900 Ieper (BE)

(74) Representative: **Quintelier, Claude et al**
Gevers & Vander Haeghen,
Livornostraat 7
1060 Brussels (BE)

(54) A biometric sensing device

(57) A biometric sensing device wherein the biometric data, collected by a biometric sensor, is combined into a data word with a time signal, indicating the time at which the biometric data was collected and/or a position signal indicating the position at which the biometric data was collected. The thus formed data word is stored during a predetermined time period in order to enable a verification with subsequently generated data words.

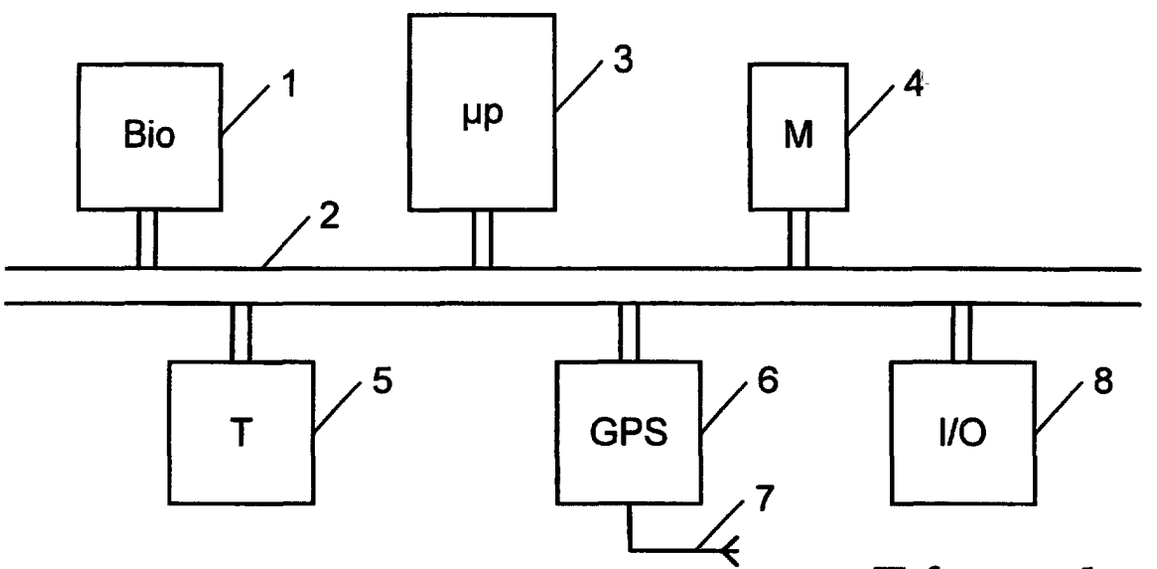

Fig. 1

EP 1 235 189 A1

Description

[0001] The invention relates to a biometric sensing device comprising a biometric sensor provided for collecting biometric data of a user and for forming a biometric data signal based on said collected biometric data.

[0002] Such a biometric sensing device is generally known and used for authentication purposes. Generally a fingerprint, a spoken word or an eye pattern of the user are recorded by the biometric sensor in order to form a biometric data signal. If the data signal is recognised by the system, the user will obtain access, if not, access will be refused.

[0003] Although biometric sensors have substantially increased the reliability of authentication operations by making fraud more difficult, impostors have found ways to supply falsified data which can not easily be detected by the biometric sensing device. So, for example, when a spoken word has to be supplied to the biometric sensor, the latter could have been recorded on beforehand and played back in front of the biometric sensor. If the latter can not make the distinction between a "life" spoken word and a "played back" word, the impostor will get access.

[0004] It is an object of the present invention to realise a biometric sensing device having means that enable to detect fraudulent attempts.

[0005] A biometric sensing device according to the present invention is therefore characterised in that said biometric sensor is provided for generating a start pulse upon collecting biometric data of said user, said device further comprising at least a first signal generator having an input for receiving said start pulse and being provided for generating, under control of said start pulse and within a first predetermined time period, a time signal indicating a time at which said collecting of biometric data was performed and/or a position of said user, said device also comprises a data word generator provided for receiving said biometric data signal, said time signal and/or position signal and for forming a data word by combining those signals, said data word generator being linked to a verification element having a memory for storing said data word during a second predetermined time period, said verification element being provided for checking if a subsequent received data word, having a biometric data signal which corresponds with the biometric data signal of a stored data word, forms with that stored data word an admissible sequence and for generating a flag if said subsequent received data word does not form an admissible sequence. Since the time and/or position signal is determined under control of the start pulse and within a predetermined first time period, those signals indicate rather precisely the time at which the biometric data of the user was collected and/or where. By associating the time and/or the location to the biometric signal a unique data word is obtained which can be stored and used for further analysis. When a same biometric signal is subsequently formed, it will necessarily be associated with a different time and maybe with a different location. The time and/or location information can now be used to check if the subsequently formed data word is admissible. So, for example, if a same biometric data is collected first in Tokyo and one hour later in Houston (Texas), such a sequence is clearly considered as inadmissible as it is impossible to travel on earth within one hour from Tokyo to Houston. At least one of both attempts is clearly false.

[0006] A first preferred embodiment of a biometric sensing device according to the invention is characterised in that said first signal generator is provided for generating said time signal and wherein said device comprises a second signal generator, provided for generating under control of said start pulse and within said first predetermined time period, said position signal. Although either a time measurement or a location determination alone could be sufficient, the combination of both signals clearly enhances the possibility to detect a fraudulent attempt.

[0007] A second preferred embodiment of a biometric sensing device according to the invention is characterised in that said biometric sensor and said first and second generators are embedded in a same component. In such a manner the data word is generated within a same component and its falsification is not easy.

[0008] Preferably, said data word generator is provided for encrypting said data word. Encryption of the data word enhances the reliability.

[0009] The invention will now be described in more details with reference to the drawings, illustrating a preferred embodiment of a device according to the invention. In the drawings :

figure 1 shows a block diagram of the biometric sensor and the first and second generator;
figure 2 shows a block diagram of the verification element; and
figure 3 shows a time diagram.

[0010] Although the biometric sensing device according to the present invention is shown as split over the figures 1 and 2, the elements composing the device could either be formed by two physically separated parts or by a single part.

[0011] The biometric sensing device according to the present invention comprises a biometric sensor, having a sensing unit 1, connected via a bus 2 to a microprocessor 3. Depending on the biometric data to be collected, the sensing unit will either be formed by a single or a plurality of elements. So, for example, when only fingerprint data have to be collected, the unit 2 will be formed by a fingerprint scanner. A microphone for voice recording or a T.V.-camera for eye pattern or face recognition could be used either in combination with the fingerprint scanner or alone depending on the imposed level of security.

[0012] A memory 4 is also connected to the bus 2 for storing program data for operating the device. A first signal generator 5 and a second signal generator 6 as well as an I/O interface 8 are also connected to the bus 2. The first signal generator 5 is provided for generating a time signal whereas the second signal generator 6 is provided for generating a position signal. Although both the first and second signal generator are shown in figure 1, it is not necessary that both are present. The device could also operate with only one of both signal generators. The presence of one or both signal generators will depend on the application and required degree of security. The latter will also determine how the signal generators are implemented. For a low end device, the first signal generator could be formed by a clock which could even be the one of the microprocessor combined with a counter. For a high end device, the first signal generator could be formed by an atomic clock signal receiver provided to receive satellite signals. A low end second signal generator could simply be formed by a memory element wherein the position where the device is fixed is stored. A high end second signal generator could be formed by a GPS receiver provided with an antenna 7. It would also be possible to combine, for a device which should remain at a same position, a memory and a GPS receiver. In such a manner, it would be possible to detect that the sensor is removed from its fixed position since the received GPS signal would no longer match with the stored one.

[0013] The verification element shown in figure 2 comprises a bus 10 to which I/O interface 9, a microprocessor 11 and a memory 12, are connected. The I/O interface 9 is provided to communicate with the I/O interface 8 in a usual manner for computer systems.

[0014] Suppose now that a user presents himself to the device in order to get access to for example a building, a file or a bank account. The sensing unit 1 will collect its biometric data and form a biometric signal with the collected data in a well known manner. The fact that the biometric sensing unit 1 has detected the presence of the user and starts to collect data at a time t1 (see figure 3) will cause the latter to generate a start pulse S1. In order to avoid malfunctioning, it is important that the start pulse is only generated if indeed biometric data are collected and not upon collecting noise. Therefore, it could even be possible that the start pulse is only generated immediately after the biometric data of the user is collected and recognised as being biometric data.

[0015] The first 5 and second 6 signal generator each have an input for receiving the start pulse which starts a first predetermined time period T1 of for example 1 second or less. Under control of the start pulse, the first and second generator will generate during the first time period a time signal and a position signal respectively. The time signal will indicate the time at which the user's biometric data have been collected and the position signal will indicate the actual geographic position of the user when his biometric data are collected i.e. the actual position of the sensing device. As the time and position signal reflects an actual information of the user, it is important that the first time period is short and linked to the start pulse. The time signal can express the time either in hours, minutes, seconds or as a number, whereas the position can be expressed in degrees or by indicating the place, street etc..

[0016] The biometric data signal, the time and/or position signal, depending on the embodiment, are then supplied to a data word generator which is part of the microprocessor 3. The data word generator is provided for combining the biometric signal with the first and/or second signal in order to form a data word. That data word can be formed either by a juxtaposition of the signal values or by interleaving the time and/or position values with the biometric data signal values. When using several biometric units, the time and position values could be added once or to each of the biometric values. When using a sample and hold technology for determining the value of the different signals, the time and/or position values could be inserted for each sample value thus enabling to compensate for drift.

[0017] Once the data word is generated, the latter could also be encrypted which is preferred if the data word has to be sent via a public communication medium to the verification unit. The quality of the encryption algorithm will of course be determined by the required degree of security. In this way, data confidentiality and integrity are ensured as possible data tampering in uncontrolled environments is substantially reduced. The encryption is performed by providing the data word generator with encryption means.

[0018] The data word or the encrypted data word if available is thereafter transmitted via the I/O interfaces 8 and 9 to the memory 12 of the verification unit 14 where it will be stored during a second predetermined time period T2 which is substantially longer than the first time period T1. Depending on the required security level, the second time period will be, for example, one day, one week, one month, one or several years. The second time period is either started by the down going edge of the clock signal determining the first period as illustrated in figure 3 or by an internal clock of the verification unit. The end of the second period is determined either by annexing a time period to the stored data word or by the internal clock of the verification unit. Once the second predetermined period has lapsed, the stored data word can be retrieved or at least is no longer considered as valid and can be overruled.

[0019] Suppose now that the same user presents himself one day later before the same sensing unit 1. The same operation as described here before will be performed leading to the generation of a subsequent data word. Since the same user is concerned, the biometric data signal will most probably be the same or at least corresponding. The position signal included in the data word will also be the same, since the same sensor is used but the time signal will be different. The verification

element is now provided for establishing, by comparing the biometric data signal part in the subsequent data word with the stored data words, that a same user is concerned since the biometric data signal parts match. The verification element will then compare the position and time signal of the received subsequent data word with the one that has been identified among the stored one as belonging to a same user. The verification element will, in the present example, establish that the position signals match and that only the time signals are different. The verification element will now check if both time signals form an admissible sequence. This signifies that the verification unit will apply predetermined criteria to establish whether the sequence is admissible or not. So, for example, the verification unit could have a criteria that for this sensing device one day time difference with a same location is admissible since the sensor controls the access to his office. In this case, the user is identified as the correct one and access is provided. In order to update the memory, the subsequent data word could overrule the actual stored data word.

[0020] Suppose now that the legally entitled user presents himself at a time T to a bank terminal in Tokyo equipped with a microphone wherein a spoken word has to be used as biometric data. Suppose also that an impostor has recorded the voice of the correct user on tape and presents himself one hour later (T+1) at a bank terminal in Houston (Texas). The device will generate and store a first data word for the correct user including his voice biometric data with Tokyo as position signal and time T as time signal. One hour later the verification element will receive a second subsequent data word having a same biometric data since the recorded voice was used, but with T + 1 as time signal and Houston as position signal. Since both biometric data signals match, the verification unit will compare the time and position signal of the second subsequent data word with the one of the first data word retrieved from the memory. The verification unit will have as predetermined criteria a distance between the position signals which related to the time difference between the time signal may not exceed a threshold value. The verification element will calculate the difference in position between Tokyo and Houston and will establish that this distance exceeds the threshold value as it is impossible to travel from Tokyo to Houston in one hour time. The verification will thus consider the sequence between the first and second data word as being inadmissible and will generate a flag.

[0021] That flag can then be used to prevent the storage of the second data word and to generate an alarm signal that could lead to prevent the impostor in Texas to get access to that bank account.

[0022] The biometric sensing device according to the present invention is applicable everywhere where access control is realised by means of biometric authentication. The present device can however also be used in combination with other devices such as mobile phones, cars, trucks or in the transaction of documents. So for example, the device according to the invention could be embedded in a mobile phone using the operator antenna identifier as input data for the position of the user. The time data can be supplied either from the internal phone clock or from the operator. The antenna identifier indeed enables to locate where the phone is used and can therefore be used as position data. Since the time and position data are known and combined with the biometric data, it will provide evidence to prove that a user indeed used that telephone at that place at that time. Such an information would be useful when the debit note for the phone would be contested.

[0023] The device according to the present invention could also be mounted in a truck or other vehicle equipped with a GPS navigation system. The device would then be used for identifying the driver and/or tracking the vehicle. The driver would have to introduce his biometric data within certain time periods. Since the position data is added to the biometric data, it would be possible, based on the stored data to monitor where the vehicle was and at what time.

[0024] The device according to the present invention could further be used for authentication of the transaction of official documents. So, for example, when a document has to be signed by different persons who are not necessarily at the same place, the device could be used to establish that the concerned persons where at a well defined place, for example with a notary public, at a well defined time.

[0025] When use is made of several biometric sensors for authentication purpose, those sensors need not to be necessarily combined in a same apparatus for application of the present invention. So, for example a camera, which is used for monitoring a public place could be used for face recognition and output biometric face data. A fingerprint sensor and/or voice sensor could also be used for fingerprint and/or voice biometric data. To each biometric data, a position and time signal could be added as described here before in order to form a set. That set could then be used to furnish evidence that a person indeed was present at a certain time at a certain place since the data had been collected by two sensors operating independently from each other.

Claims

1. A biometric sensing device comprising a biometric sensor provided for collecting biometric data of a user and for forming a biometric data signal based on said collected biometric data, **characterised in that** said biometric sensor is provided for generating a start pulse upon collecting biometric data of said user, said device further comprising at least a first signal generator having an input for receiving said start pulse and being provided for generating under control of said start pulse and within a first predetermined time period a time signal indicating

a time at which said collecting of biometric data was performed and/or a position of said user, said device also comprises a data word generator provided for receiving said biometric data signal, said time signal and/or position signal and for forming a data word by combining those signals, said data word generator being linked to a verification element having a memory for storing said data word during a second predetermined time period, said verification element being provided for checking if a subsequent received data word, having a biometric data signal which corresponds with the biometric data signal of a stored data word, forms with that stored data word an admissible sequence and for generating a flag if said subsequent received data word does not form an admissible sequence.

2. A biometric sensing device as claimed in claim 1, **characterised in that** said first signal generator is provided for generating said time signal and wherein said device comprises a second signal generator provided for generating under control of said start pulse and within said first predetermined time period said position signal.

3. A biometric sensing device as claimed in claim 2, **characterised in that** said biometric sensor and said first and second generator are embedded in a same component.

4. A biometric sensing device as claimed in claim 1 or 2, **characterised in that** said data word generator is provided for encrypting said data word.

5. A biometric sensing device as claimed in any one of the claims 1 to 4, **characterised in that** said biometric sensor is provided for performing data collection on different biometric characteristics.

6. A biometric sensing device as claimed in claim 2, **characterised in that** said second signal generator comprises an input for receiving a GPS signal.

7. A biometric sensing device as claimed in claim 2, **characterised in that** said second signal generator comprises a further memory for storing a geographic position indicating the position at which said second signal generator is placed.

8. A biometric sensing device as claimed in any one of the claims 1 - 7, **characterised in that** it comprises a plurality of biometric sensors provided for supplying biometric data signals independently from each other.

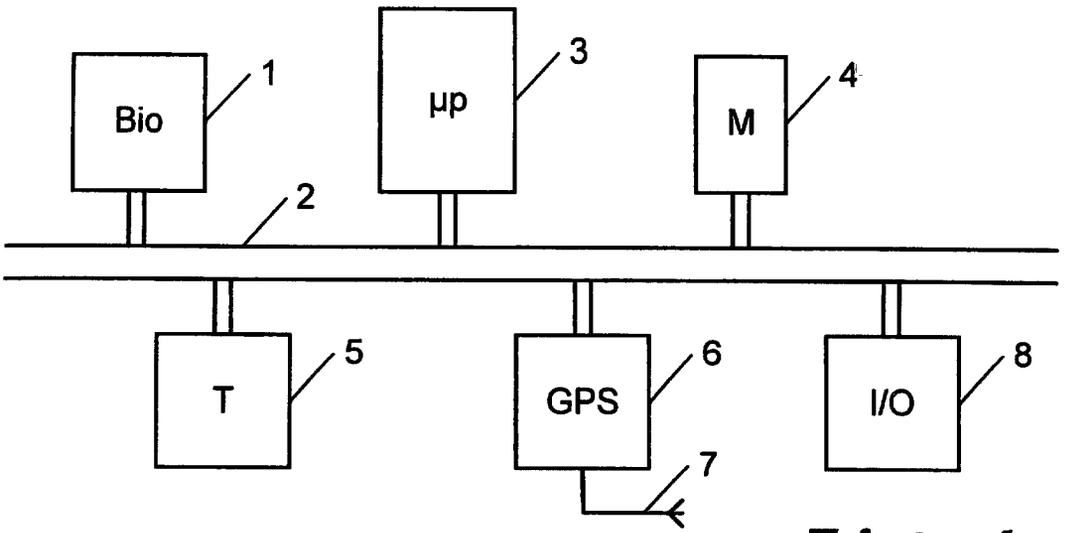

Fig. 1

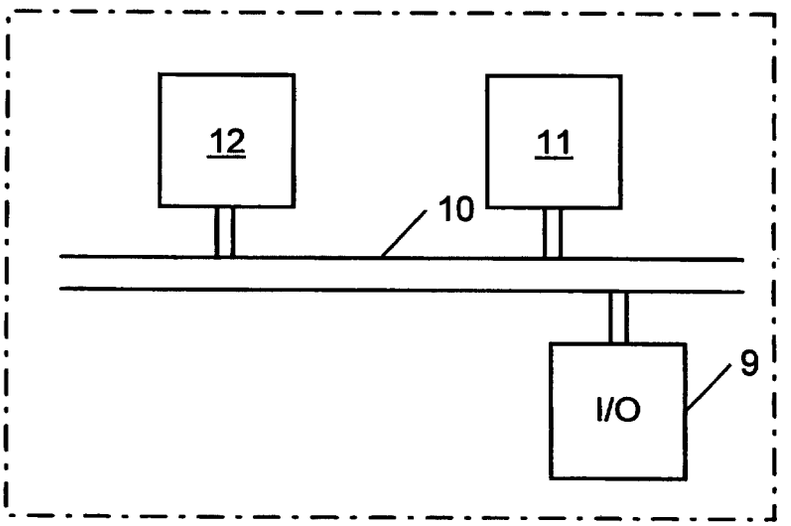

Fig. 2

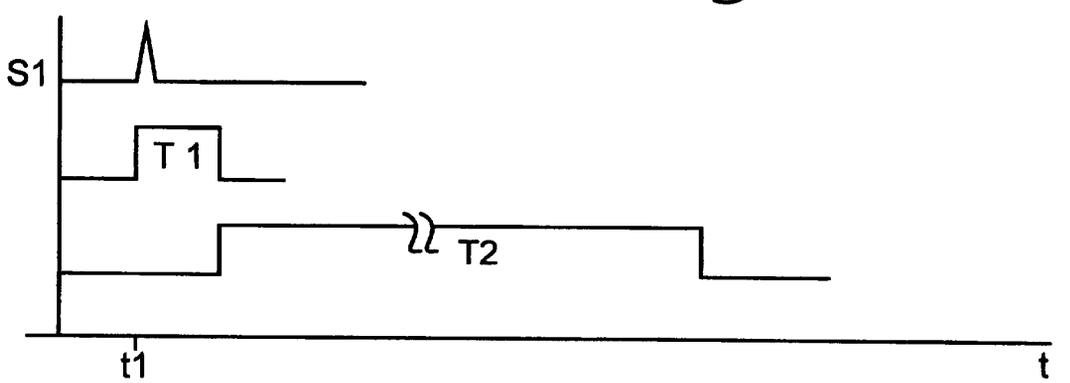

Fig. 3

European Patent Office

EUROPEAN SEARCH REPORT

Application Number
EP 01 20 0723

DOCUMENTS CONSIDERED TO BE RELEVANT

Category	Citation of document with indication, where appropriate, of relevant passages	Relevant to claim	CLASSIFICATION OF THE APPLICATION (Int.Cl.7)
X Y	DE 198 09 043 A (DEUTSCHE TELEKOM AG) 9 September 1999 (1999-09-09) * abstract * * column 2, line 8 - column 4, line 25 * ---	1-3,5,7, 8 4	G07C9/00 G07F7/00
Y	US 5 280 527 A (FAST NORMAN ET AL) 18 January 1994 (1994-01-18) * abstract * * column 4, line 39 - column 5, line 33 * ---	4	
A	WO 96 41488 A (DICE COMPANY) 19 December 1996 (1996-12-19) * abstract * * page 5, line 1 - page 7, line 2 * ---	1,6	
A	WO 00 42577 A (SENSAR INC) 20 July 2000 (2000-07-20) * abstract * * page 8, last paragraph - page 15, paragraph 2 * -----	1	

TECHNICAL FIELDS SEARCHED (Int.Cl.7)
G07C G07F

The present search report has been drawn up for all claims

Place of search	Date of completion of the search	Examiner
THE HAGUE	16 July 2001	Teutloff, H

CATEGORY OF CITED DOCUMENTS

X : particularly relevant if taken alone
Y : particularly relevant if combined with another document of the same category
A : technological background
O : non-written disclosure
P : intermediate document

T : theory or principle underlying the invention
E : earlier patent document, but published on, or after the filing date
D : document cited in the application
L : document cited for other reasons

& : member of the same patent family, corresponding document

EPO FORM 1503 03.82 (P04C01)

ANNEX TO THE EUROPEAN SEARCH REPORT ON EUROPEAN PATENT APPLICATION NO. EP 01 20 0723

This annex lists the patent family membersrelating to the patent documents cited in the above-mentioned European search report. The members are as contained in the European Patent Office EDP file on
The European Patent Office is in no way liable for these particulars which are merely given for the purpose of information.

16-07-2001

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
DE 19809043 A	09-09-1999	WO 9945690 A EP 1060607 A	10-09-1999 20-12-2000
US 5280527 A	18-01-1994	CA 2105404 A	03-03-1995
WO 9641488 A	19-12-1996	NONE	
WO 0042577 A	20-07-2000	AU 2615400 A	01-08-2000

EPO FORM P0459

For more details about this annex : see Official Journal of the European Patent Office, No. 12/82