



(12) **EUROPEAN PATENT APPLICATION**

(43) Date of publication:
12.01.2005 Bulletin 2005/02

(51) Int Cl.7: **G07C 9/00**

(21) Application number: **04103268.1**

(22) Date of filing: **09.07.2004**

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

(72) Inventors:
• **Villa, Massimiliano**
27025, GAMBOLO' (Pavia) (IT)
• **Cavaioni, Matteo**
27025, GAMBOLO' (Pavia) (IT)

(30) Priority: **11.07.2003 IT MI20031431**

(74) Representative: **Long, Giorgio et al**
Jacobacci & Partners S.p.A.
Via Senato, 8
20121 Milano (IT)

(71) Applicant: **Multimedia S.r.l.**
27025 GAMBOLO' (Pavia - Italy) (IT)

(54) **Fingerprint recognition security system**

(57) Security system with fingerprint recognition (100) comprising a local apparatus (50) provided with:

- a fingerprint acquisition unit (1) for generating, based on the finger of the main user placed near the unit, an electrical signal representative of the corresponding fingerprint,
- processing means (CPU, INT) coupled to the acquisition unit (1) for supplying reference digital data on

the basis of said electrical signal. Furthermore, the local apparatus comprises a memory (M) controlled by the processing means (CPU) for storing the reference digital data.

The system (100) is characterized in that it further comprises a remote managing apparatus (3) such as to generate an authorization signal by which said processing means (CPU, INT) can enable storage of the reference digital data in the memory (M).

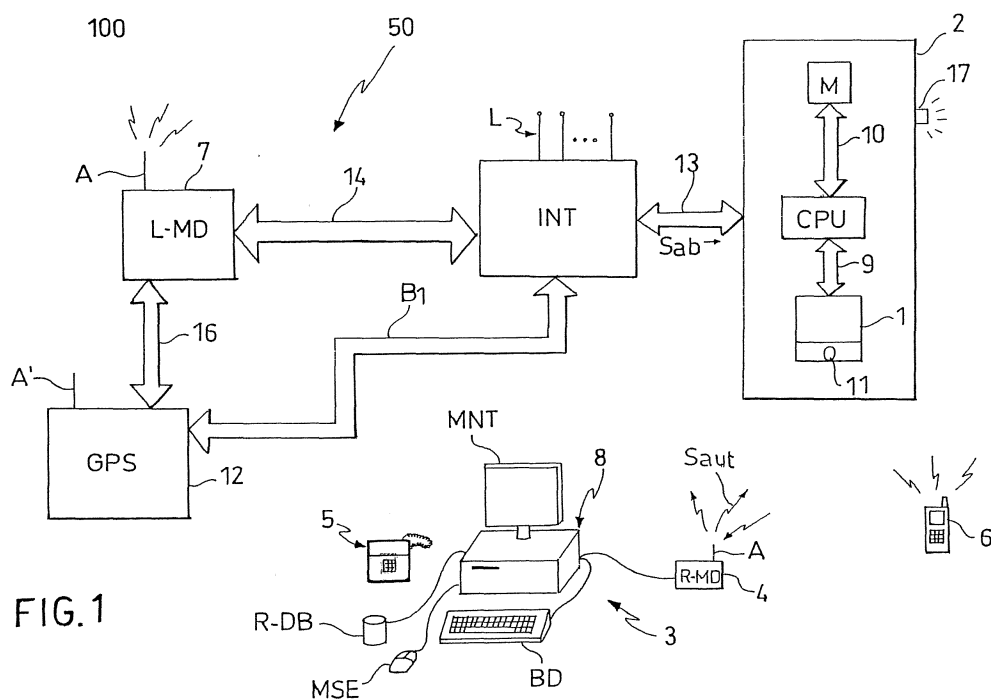


FIG.1

Description

[0001] The present invention refers to a security system provided for recognition of fingerprints. In particular, the present invention refers, but is not limited to a security system which can be used as an anti-theft device for vehicles such as cars, or places or premises such as houses.

[0002] The most widespread conventional car anti-theft devices today are "code recognition" systems where the user, using a keyboard on the car computer (for example, the computer is associated to a Global Positioning System), has to enter an identification code with which he is recognized.

[0003] According to another type of conventional technology, each user is provided with a transponder (in particular, a transmitter which operates at a frequency of 433 MHz) which emits a signal which is recognized by a system installed in the vehicle when the engine is turned on.

[0004] In both techniques, failed recognition can prevent the vehicle from starting or can be followed by transmission of a silent alarm to a managing centre.

[0005] Nevertheless, these methods are not entirely satisfactory because they have proved to be vulnerable to fraud and coercive action taken against the authorized user.

[0006] With reference, for example, to anti-theft systems for houses, systems which make use of fingerprint recognition are well known.

[0007] These systems typically comprise a user fingerprint acquisition unit and a processing device capable of comparing each acquired fingerprint with a pre-stored reference fingerprint.

[0008] Normally, recognition of the authorized user's fingerprint enables opening of the entry door to the protected place.

[0009] It has been observed that conventional fingerprint recognition security systems have considerable limitations and do not ensure the necessary invulnerability against fraud.

[0010] Object of the present invention is to propose a security system with fingerprint recognition which overcomes the limitations of the above-mentioned conventional systems.

[0011] The object of the present invention is achieved by a security system as defined in the attached claim 1. Particular embodiments of the invention are defined in the attached claims 2-19. A device for fingerprint recognition as described in the attached claim 20 also forms part of this invention.

[0012] Methods to store data regarding fingerprints as defined in claims 21 and 23 also form part of the invention as well as a computer program as defined in claim 23.

[0013] For a better understanding of the characteristics and advantages of the present invention, some non-limiting embodiments thereof are described below, with

reference to the appended drawing, where:

figure 1 schematically shows an embodiment of the security system according to the present invention, figure 2 shows, by means of a flow diagram, a possible reference fingerprint registration procedure which can be implemented by said system.

[0014] Figure 1 shows a preferred embodiment of the security system 100 according to the invention which can be used as an anti-theft device, in particular, for vehicles, for example, cars or premises such as houses.

[0015] The security system 100 comprises a local apparatus 50 and a remote managing apparatus 3. The local apparatus 50 is intended to be installed on board the vehicle, preferably inside the driver and passenger compartment or inside the house. The remote managing apparatus 3 is located in an anti-theft security service management centre and can be placed in a single locality and ensure radio management, i.e. wireless management of a plurality of local apparatus 50 distributed throughout the territory of a single nation or various nations.

[0016] The local apparatus 50 comprises a fingerprint unit 2 for acquiring, reading and recognizing fingerprints, an interface processing device INT and a communication apparatus 7, L-MD.

[0017] In the case of vehicle application, the local apparatus 50 advantageously comprises a module 12 for localizing the position of the vehicle in the area.

[0018] The fingerprint unit 2 includes, for example, in a single housing, a fingerprint acquisition unit 1 connected by means of a bus 9 to a local processing device CPU connected, in turn, to a memory M by means of a bus 10.

[0019] The acquisition unit 1 is such as to acquire the fingerprint of the user's finger coupled to an input port 11 and transmit, on the bus 9, an electrical signal, for example of the digital type, corresponding to said fingerprint.

[0020] It should be noted that users of the system 100 use the acquisition unit both in the initial registration step, to store the fingerprint of the main user (for example, the owner of the vehicle), and every time it is necessary to recognize the user who wants to start the vehicle or enter the house.

[0021] The acquisition unit 1 can be produced with conventional technologies and, according to a particular embodiment of the invention, may comprise a video camera (for example, of the digital type) which acquires the image of the print of the finger placed on the support element 11 (for example, a transparent prism). Said camera comprises a sensor for image acquisition (for example, a matrix of integrated photodiodes) and, if necessary, suitable processing modules for the acquired image. Alternatively, others suitable types of acquisition units may be used, such as capacitive or pressure-static sensors, based on the variation of the electrical conduc-

tivity.

[0022] The local processing device CPU and the memory M can be formed of a microcontroller of the conventional type provided on a single electronic board adequately connected to the acquisition unit 1.

[0023] The local processing device CPU, in accordance with procedures which will be explained hereinafter, can manage part of the operations necessary to store in the memory M the reference digital data corresponding to the main user's fingerprint.

[0024] Furthermore, according to a preferred embodiment, the processing device CPU is so as to carry out recognition of a current fingerprint placed on the input 11 of the acquisition unit 1, by means of a comparing (performed in execution of a suitable software) of the reference digital data with other digital data corresponding to the current fingerprint.

[0025] The fingerprint unit 2 is connected, by means of a bus 13, to the interface processing device INT coupled to the local communication apparatus 7, by means of a bus 14, as an example of the serial type.

[0026] The processing device INT comprises a suitable electronic board (for example, a microcontroller) such as to handle the exchange of information signals and control signals between the fingerprint unit 2 and the local communication apparatus 7.

[0027] Furthermore, the interface processing device INT is such as to generate, for example on the basis of recognition signals supplied by the fingerprint unit 2, alarm signals and/or signals which enable and disable particular vehicle functions (for example, engine start, seat position adjustment or mirror adjustment).

[0028] Said alarm and/or enabling signals are provided on output lines L of the interface device INT.

[0029] The local communication apparatus 7 is suitable for radio reception and transmission and, is preferably compliant with a conventional mobile telephone system. According to a preferred embodiment, the local communication apparatus 7 is a MODEM (provided with an aerial A) intended to communicate with the remote managing apparatus 3. For example, the local communication apparatus 7 is a GSM (Global System Mobile) type modem.

[0030] The position localization module 12 (provided with an aerial A') is, typically, a conventional apparatus which works within a GPS (Global Positioning System) satellite system. The position localization module 12 is connected by means of a data transmission line, such as a bus 16, to the local communication apparatus 7 to send data concerning the position of the vehicle to the remote managing apparatus. Advantageously, a further data bus B1, which allows the interchange of data between the interface device INT and the position localization module 12, can be provided.

[0031] The remote managing apparatus 3 comprises one or more central processors 8 which handle the data and the information received from the local apparatus 50 and which generate control signals to be sent to said

local apparatus.

[0032] The central processor 8 can be a conventional personal computer PC provided with a central processing unit working with mass storage and removable discs (hard disc, Compact Disk readers, floppy discs) and is provided with suitable peripheral units such as a monitor MNT, a keyboard BD and a mouse MSE.

[0033] Furthermore, a remote communication apparatus 4, R-MD, is associated with the central processor 8, in order to exchange data with the local communication apparatus 7 in a wireless mode. In accordance with the example given with reference to the local communication apparatus 7, the remote communication device 4 is also a GSM type MODEM.

[0034] In particular, the central processor 8, by means of the remote communication device 4, plays a primary role in the operation of registering the reference fingerprint of the main user. Advantageously, special software is stored in the memory of the central processor 8 to perform said reading procedure.

[0035] The remote managing apparatus 3 is, advantageously, further provided with a telephone 5 (mobile or landline) which makes it possible for the security system 100 operator to communicate with the main user provided with a respective telephone 6, preferably portable or mobile.

[0036] Furthermore, the central processor 8 or other processors having greater capacity, can collect data concerning the position of the vehicle and visualize this position on the monitor MNT. Advantageously, the remote managing apparatus 3 is in communication with a specialized Police centre so that data regarding a detected anomalous event can be transmitted to the police.

[0037] It should be observed that, advantageously, both the interface processing device INT and the local processing device CPU are produced in such a way as not to have further access ports which would make it possible to connect them to an external computer with which to pilot storage of fingerprints of non-authorized people.

[0038] Figure 2 shows a flow diagram which represents the steps of a method according to the invention for the registration of the reference fingerprint.

[0039] At the moment of purchasing the local apparatus 50, the user is given, preferably by the same service centre which runs the entire system 100, a secret code (typically a password) which unequivocally identifies both the user and the particular local apparatus 50 purchased by him.

[0040] Subsequently, the main user will install the local apparatus in his vehicle or at his home and will start (START step) the procedure to read his fingerprint.

[0041] In a first step called COMM, the main user contacts, by means of his telephone 6, the telephone 5 of the remote managing apparatus 3 and refers the password to the operator of the system 100.

[0042] Subsequently, the operator proceeds with

identification of the main user, initially entering the password into the central processor 8, for example, by means of the keyboard BD (INSERT-COD step).

[0043] The software of the central processor 8 makes a comparison (CFR-IDENT) between the password and all the passwords stored in a remote database R-DB (for example, located in the said central processor) and regarding all the users of the system 100.

[0044] The registration procedure can continue only if this identification step is successful.

[0045] It should be observed that the procedure which envisages the presence of an operator at the remote managing apparatus 3 is certainly preferable in terms of security and functionality. However, it is possible to carry out the call (COMM) and identification (CFR-ID) steps not by means of a telephone direct conversation between two persons, but in a completely automatic mode, that is to say with a vocal recognising system of the IVR (Interactive Voice Response) type.

[0046] For example, the vehicle or house can be equipped with a local processor (a PC) which is connected to a data communication network (for example, the Internet) of which the central processor 8 forms part. In this case, the local processor can send non-vocal signals to the central processor 8 carrying the user's identification code. For example, the password can be entered in a special box on the web page of the Internet site of the security system 100.

[0047] In the case the comparison procedure CFR-IDENT leads to identification of an authorized user, the central processor 8 generates a first authorization signal S_{aut} (AUT-SIG step) and sends it to the remote communication device 4. Said authorization signal is necessary to enable memorization of the digital data corresponding to the reference fingerprint in the memory M of the local apparatus 50.

[0048] It should be observed that, advantageously, the software installed in the central processor 8 is such as to generate the authorization signal S_{aut} in such a way that it carries a further code exclusively associated to that specific local apparatus 50 purchased by the identified main user.

[0049] The authorization signal S_{aut} is processed by the communication device 4 which, according to the embodiment, processes it in accordance with the GSM mobile communication system and sends it by means of the aerial A (IRRD irradiation step).

[0050] The transmitted authorization signal S_{aut} is received (RECEIV step) by the local communication apparatus 7 which, after processing it according to GSM demodulation procedures, delivers it on one or more lines of the bus 14.

[0051] The interface processing device INT receives, in its turn, the demodulated authorization signal S_{aut} and carries out the recognition of this code to evaluate the suitability of the authorization signal (COD-RECOGN step).

[0052] In this code recognition step, the interface de-

vice INT carries out the operation of comparing with a corresponding code (as well as any decoding and/or decrypting operations).

[0053] The registration procedure continues only if the interface processing device INT recognizes that the authorization signal S_{aut} is the one unequivocally intended for that specific local apparatus 50.

[0054] In this case, the interface processing device INT generates an enabling signal S_{ab} and sends it to the local processing device CPU associated to the fingerprint unit 2 by means of one or more lines of the bus 13.

[0055] Furthermore, advantageously, once the suitability of the code associated to the authorization signal S_{aut} has been recognized, the interface processing device INT begins the countdown of a registration time interval within which registration of the fingerprint can take place.

[0056] Start of the registration time interval is indicated, for example, by a signal which, from the interface processing device INT and through the bus 13 and the local processing device CPU, causes activation of a luminous source 17 (for example a LED, Light Emitting Diode) provided on the fingerprint unit 2.

[0057] From the moment in which the luminous source 17 lights up, the main user can place his fingertip on the transparent prism 11, or an other suitable sensor.

[0058] The enabling signal S_{ab} allows the local processing device CPU to command the acquisition unit 1 in order to perform acquisition of the image of the fingerprint (ACQ step), its processing (ELAB step) for obtaining corresponding digital data (performed according suitable mathematical models known to the skilled person), and storage of said data in the memory M (STOR step).

[0059] The same luminous source 17 can, as it switches off, signal the end of the time interval available for registration.

[0060] Furthermore, after registration is complete, it is possible for the local processing device CPU to generate a confirmation signal which, through the interface device INT and the local communication apparatus 7, reaches the remote managing apparatus 3. The confirmation signal, received by the remote communication device 4 causes, by means of the software of the central processor 8, visualization of a corresponding message of completed registration on the monitor MNT. The operator of the remote managing apparatus can inform the user, by means of the phones 5 and 6, that the registration procedure has been completed.

[0061] Registration of the digital image is thus concluded (END step).

[0062] Using a procedure substantially identical to that described, it is possible for the user to read several reference fingerprints, for example of other people who he intends giving authorization to use the vehicle or enter the house.

[0063] Furthermore, the user can register the print of another finger which will be used exclusively to signal

an anomalous situation, for example, a situation where he is under duress.

[0064] In the step following registration of the fingerprint/s, each time the user intends starting the vehicle or opening the house door he will carry out his own fingerprint recognition. In fact, after switching on the fingerprint unit 2 by means of the special key, he places his finger on the transparent prism 11 and waits for acquisition of the corresponding fingerprint image. Said acquisition involves generation of the current digital data corresponding to the fingerprint read by the acquisition unit 1.

[0065] The local processing device CPU compares the acquired current digital data with the reference digital data stored in the memory M.

[0066] If, following this comparison procedure, the main user is recognized, the local processing device CPU sends a user recognition signal to the interface processing device INT which can, for example, by means of a special relay (not shown), command ignition of the vehicle engine or, by means of another conventional actuator, opening of the front door of the house.

[0067] Should the main user not be recognized, ignition of the vehicle engine or opening of the front door is inhibited and all attempts to start the engine or open the door can cause activation of a sound alarm (for example, a siren on board the vehicle) and/or transmission of an alarm signal from the local apparatus 50 to the remote managing apparatus 3.

[0068] Advantageously, together with said alarm signal, the position of the vehicle is sent to the remote managing apparatus 3, obtained by means of the GPS module 12.

[0069] Should the user wish to signal a state of duress, he will place the corresponding finger on the acquisition unit 1. The fingerprint unit 2 will recognize this other fingerprint stored and will send, similarly to that described above, an alarm signal to the remote managing apparatus 3. In this case, it is possible to design the system 100 in such a way that the vehicle doors could be opened and the activation of the car motor could be allowed.

[0070] The system 100 of the present invention offers considerable advantages compared to conventional systems.

[0071] In fact, the teachings of this invention make it possible to adopt a fingerprint registration procedure which makes fraud particularly difficult if not totally impossible. In particular, the registration operations are controlled by the same centre which controls the security system and not, as happens in the state of the art, by car dealers or security system installers who can register fingerprints of people not authorized by the main user.

[0072] Furthermore, the registration procedure made possible by the security system according to the invention, can be considered user-friendly since the owner is not obliged to go in person to the system control centre

to carry out said registration.

[0073] It should be observed that the digital data regarding the fingerprints are stored in the local apparatus 50 and comparison procedures are carried out in the same apparatus. This makes fingerprint recognition procedures faster and safer since transmission of the most sensitive data to remote processors is avoided. Furthermore, said reference fingerprints are not made available even to the operator of the remote managing apparatus 3, so fully respecting the user's privacy.

[0074] The possibility of signalling situations of duress is also particularly useful and advantageous for the users.

Claims

1. Security system with fingerprint recognition (100) comprising a local apparatus (50) provided with:

- a fingerprint acquisition unit (1) for generating, based on a main user's finger placed near the unit, an electrical signal representing the corresponding fingerprint,
- processing means (CPU, INT) coupled to the acquisition unit (1) for supplying reference digital data on the basis of said electrical signal,
- a memory (M) controlled by the processing means (CPU) for storing the reference digital data,

characterized in that it further comprises a radio operated remote managing apparatus (3) so as to generate an authorization signal by which said processing means (CPU, INT) can enable storage of the reference digital data in the memory (M).

2. System (100) according to claim 1, wherein said authorization signal carries a first code and the processing means (INT) are provided for recognizing the first code and enabling storing of the reference digital data in the memory.

3. System according to claim 1 or 2, wherein said processing means comprise:

- a processing device (CPU) associated to said memory and to said acquisition unit,
- an interface processing device (INT) connected to said processing device (CPU).

4. System according to claim 1, wherein the remote managing apparatus (3) comprises a remote radio transmission device (4) for sending said authorization signal, and said local apparatus (50) includes a local radio receiving apparatus (7) for said authorization signal.

5. System according to claims 3 and 4, wherein the local radio receiving apparatus (7) is connected to the interface processing device (INT) in order to supply a demodulated authorization signal based on said authorization signal, the interface processing device (INT) being provided for performing recognition of the first code associated to the authorization signal and for generating the enabling signal to be fed to the processing device (CPU) associated to said memory (M). 5
6. System (100) according to claim 1, wherein said remote managing apparatus comprises a remote receiving device (5) for receiving a main user identification signal carrying a second code and which can be generated from a user's transmission device (6), intended for use by the main user, the authorization signal being sent from the remote managing apparatus (3) after identification of the main user on the basis of said second code. 10
7. System (100) according to claim 6, wherein the remote receiving device (5) is included in a phone usable by an operator of the remote managing apparatus (3) and the user's transmission device (6) is a mobile phone, preferably a cell phone; the main user being able to supply to said operator, by means of a voice signal, a password corresponding to the second code. 15
8. System (100) according to claim 4, wherein the remote radio transmission device is included in a remote communication apparatus (4) and the local radio receiving device is included in a local communication apparatus (7), the local and remote communication apparatuses being suitable for transmission and reception of radio signals carrying data/information according to a system, preferably, of the cellular type. 20
9. System according to claims 6 or 7, wherein the remote managing apparatus (3) comprises a central electronic processor (8) coupled to a corresponding database, the central processor (8) being provided for carrying out recognition of said second code supplied by the main user by comparing the second code with codes stored in said database. 25
10. System according to claim 9, wherein, in the case of recognition of the main user, the central processor (8) is provided for generating an intermediate authorization signal carrying said first code, the first code being associated exclusively to the local apparatus. 30
11. System according to claims 8 and 10, wherein said intermediate authorization signal is sent to the remote communication apparatus (4) to generate said radio authorization signal. 35
12. System according to claim 2, wherein said acquisition unit (1) is such as to acquire a current fingerprint and said processing device (CPU) associated to the memory (M) is such as to supply corresponding current digital data, the processing device (CPU) being such as to perform a comparison between said current digital data and said reference digital data in order to generate an identification signal for the main user to be supplied to said interface processing device (INT). 40
13. System (100) according to claim 12, wherein said interface processing device, in the case of recognition of the main user, is provided for driving the activation of an actuator intended to enable/disable operation of a device associated to the object to be protected by the security system. 45
14. System (100) according to claim 13, wherein said object to be protected by the security system is a motor vehicle and said actuator is such as to activate/deactivate engine start on the vehicle, the local apparatus (50) being installed on board said vehicle. 50
15. System (100) according to claim 13, wherein said object is a place or premises and the actuator controls an entry door into the place or premises. 55
16. System (100) according to claim 1, wherein the acquisition unit (1) and the processing means provides acquisition of digital data relative to a plurality of reference fingerprints.
17. System (100) according to claim 14, wherein said local apparatus (50) further comprises a vehicle position localization module (12), said module (12) being able to send data regarding the position of the vehicle to the remote managing apparatus (3) by means of the local communication apparatus (7).
18. System (100) according to at least one of the previous claims, wherein the acquisition unit (1) and the processing means (CPU, INT) provide the storing in the memory (M) of further digital data corresponding to a further reference fingerprint, in the case wherein the comparison between the current digital data and the further digital data leads to recognition, the processing means (CPU, INT) provide generation of an alarm signal to be sent to the remote managing apparatus.
19. System (100) according to claim 1, wherein said acquisition unit comprises a video camera for capturing an image corresponding to the fingerprint.

20. Apparatus (50) for recognizing fingerprints (100) comprising a local apparatus (50) provided with:

- an fingerprint acquisition unit (1) for generating, based on a main user's finger placed near the unit, an electrical signal representing the corresponding fingerprint, 5
- processing means (CPU,INT) coupled to the acquisition unit (1) to supply reference digital data on the basis of said electrical signal, 10
- a memory (M) controlled by the processing means (CPU) to store the reference digital data, 15

characterized in that it further comprises a receiving apparatus (7) for receiving an authorization radio signal, which can be generated by a remote control apparatus, through which said processing means (CPU, INT) can enable storage of the reference digital data in the memory (M). 20

21. Method for storing digital data corresponding to fingerprints, the method comprising the steps of:

- a) transmitting (COMM) a signal carrying a code identifying the main user to a receiving device (5) of a remote managing apparatus (3), 25
- b) identifying (CFR-IDENT) the remote managing apparatus (3) of the main user according to said code, by means of a central processor (8), 30
- c) in the case of user recognition, generating (AUT-SIG) a first authorization signal by means of said central processor (8),
- d) transmitting the authorization signal (IRRD) by wireless means and by means of a remote transmission device (4) of said remote managing apparatus (3), 35
- e) receiving (RECEIV) said authorization signal by means of a receiving apparatus (7) of a local apparatus (50), 40
- f) generating an enabling signal according to said received authorization signal, by means of the processing means (INT, CPU) of the local apparatus (50)
- g) controlling the acquisition (ACQ) of a reference fingerprint by means of said processing means and storing (STOR) the digital data corresponding to said reference fingerprint, in a memory (M), the fingerprint being acquired by placing a finger of the main user on the acquisition unit situated in the local apparatus. 45 50

22. Method according to claim 21, wherein said enabling signal generating step comprises a recognizing step of the second code carried by said authorization signal and uniquely associated to said local apparatus. 55

23. Computer program to be loaded in the memory of a central processor (8) in order to perform, in the central processor, steps b), c) and d) of the method according to claim 21.

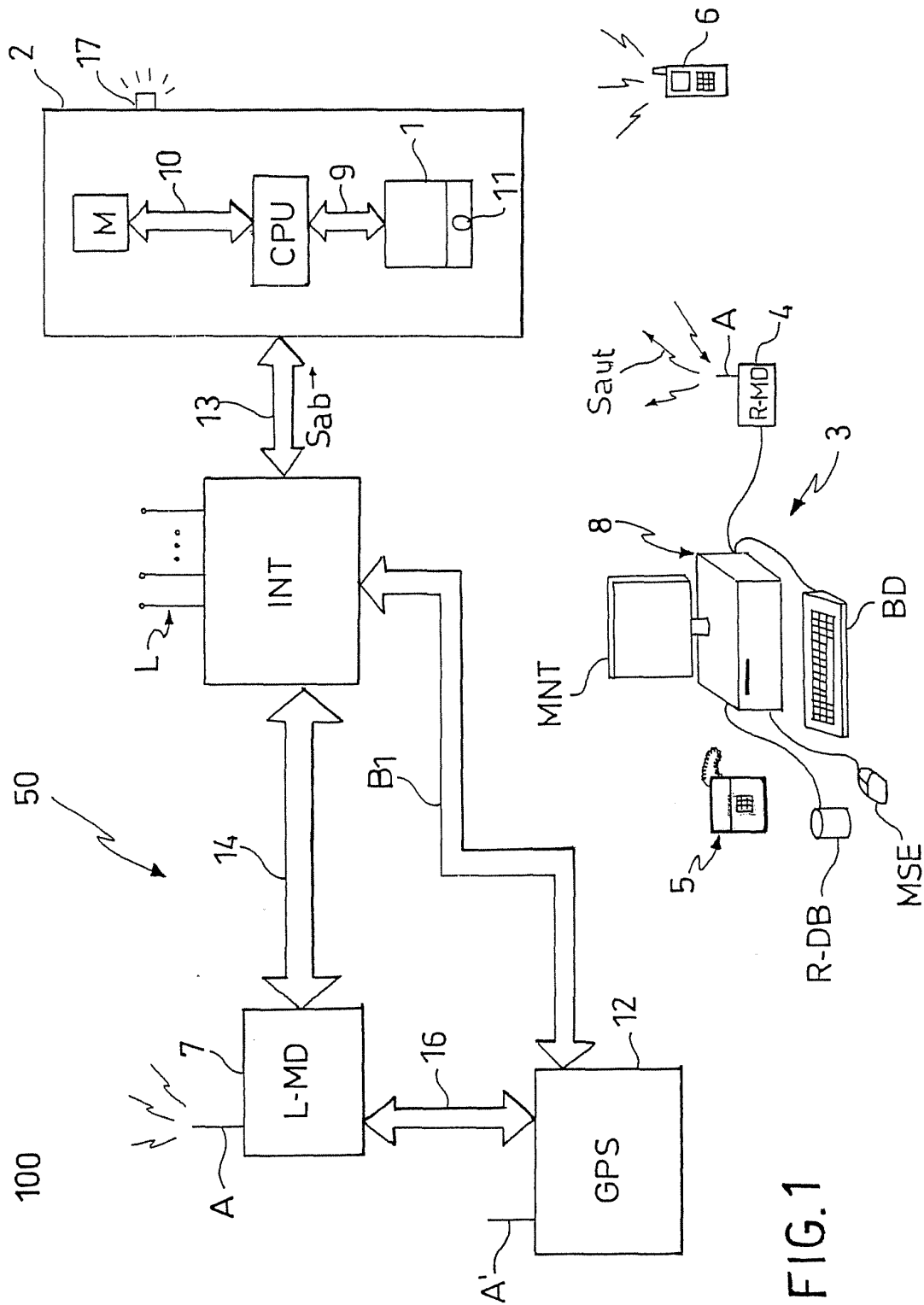


FIG.1

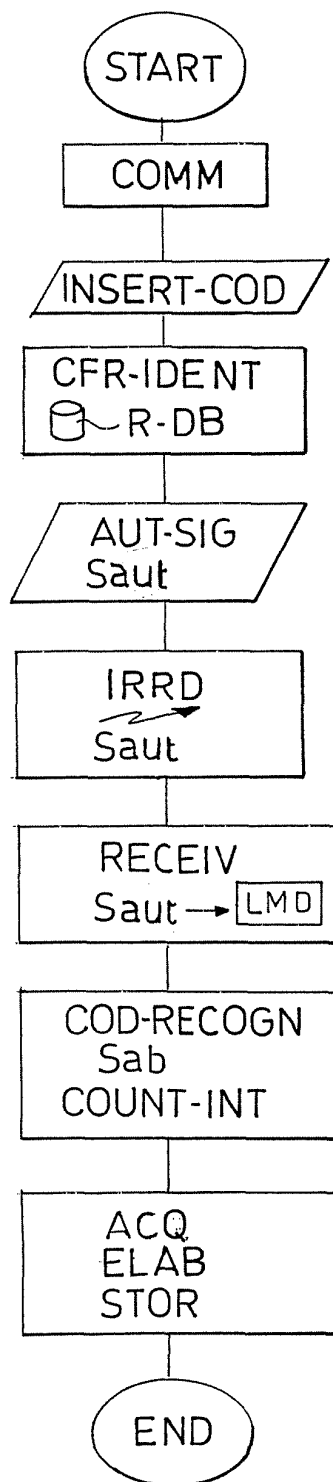


FIG. 2