(12) UK Patent Application (19) GB (11) 2 411 980 (13) A

(43) Date of A Publication 14.09.2005

(21) Application No: 0405410.2

(22) Date of Filing: 10.03.2004

(71) Applicant(s):
Giga-Byte Technology Co., Ltd
(Incorporated in Taiwan)
No 6 Bau Chiang Road, Hsin-Tien,
Taipei Hsien, Taiwan

(72) Inventor(s):
Yen Sheng Chang

(74) Agent and/or Address for Service:
Langner Parry
High Holborn House, 52-54 High Holborn,
LONDON, WC1V 6RR, United Kingdom

(51) INT CL^7:
G06F 1/00

(52) UK CL (Edition X):
G4A AAP A23C

(56) Documents Cited:
WO 1999/047989 A1 US 5838306 A
US 20030070079 A1 US 20010032319 A1
IBM Technical Disclosure Bulletin, Vol. 41, No. 1, January 1998, "Biometric Access Control in a Personal Computer System", pages 753-756.

(58) Field of Search:
UK CL (Edition W) G4A
INT CL^7 G06F
Other: Online: WPI, EPODOC, JAPIO

(54) Abstract Title: **Computer booting using biometrics**

(57) The booting of a computer is allowed to proceed only if a user biometric, e.g. fingerprint data, matches a pre-stored version. A fingerprint input process stored on a basic input/output system (BIOS) is performed during booting or resetting the computer. This causes an input module to perform a fingerprint scan and send a fingerprint signal to a recognition module 20 located on the motherboard 10 of the computer. The recognition module produces a recognition code in response to the fingerprint signal and compares it with at least one pre-stored recognition code. The comparison is used to determine if booting is permitted. Other biometric data may be used such as iris data. Also disclosed is a method of registering a user, wherein a username is provided, a fingerprint scan performed, and a recognition code is derived and stored. The scanner may be located on the computer housing, keyboard or mouse.

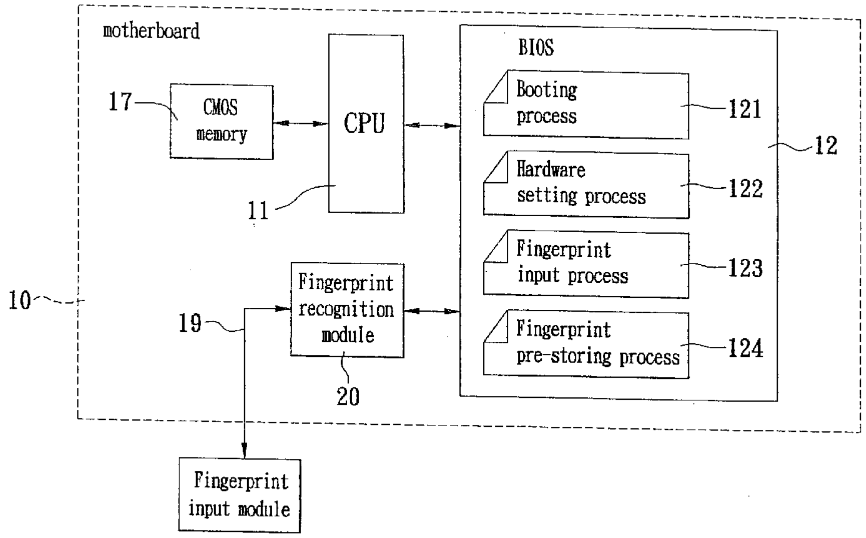

FIG. 2

GB 2 411 980 A

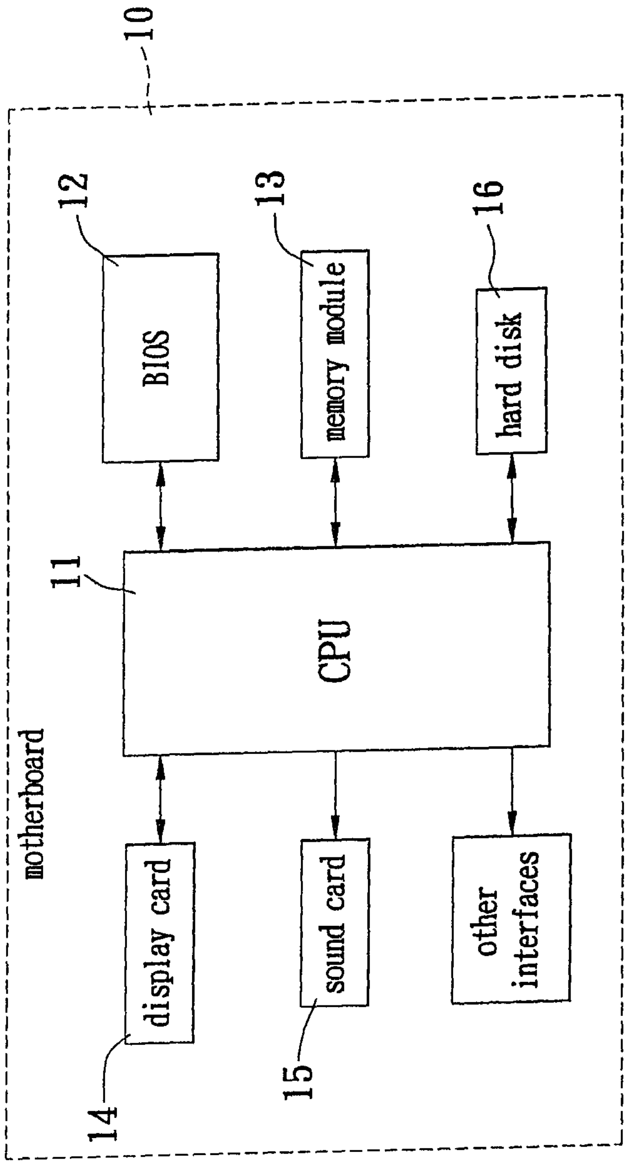

FIG. 1
PRIOR ART

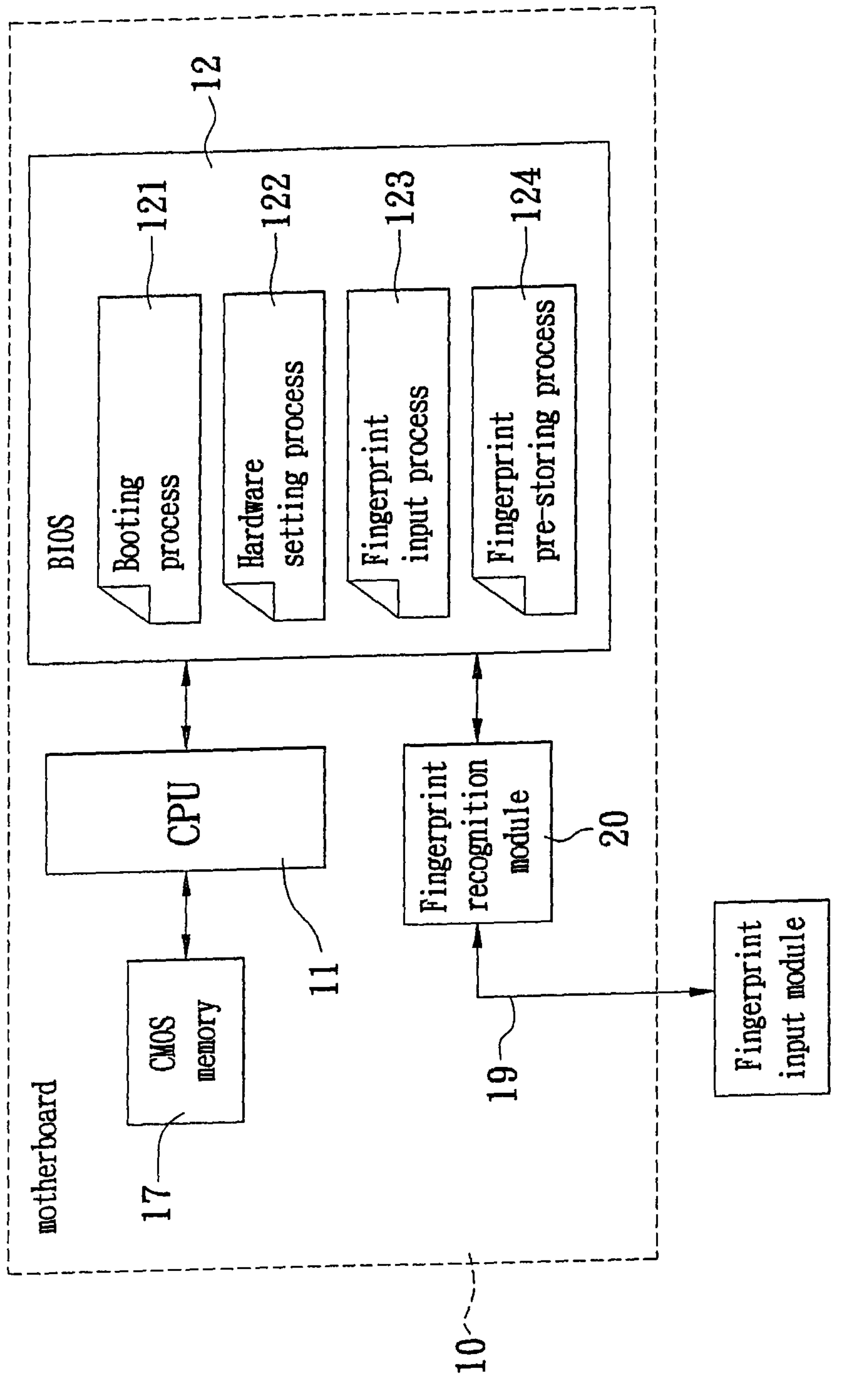
motherboard
BIOS
Booting process
Hardware setting process
Fingerprint input process
Fingerprint pre-storing process
CPU
CMOS memory
Fingerprint recognition module
Fingerprint input module
10
11
12
121
122
123
124
17
19
20

FIG. 2

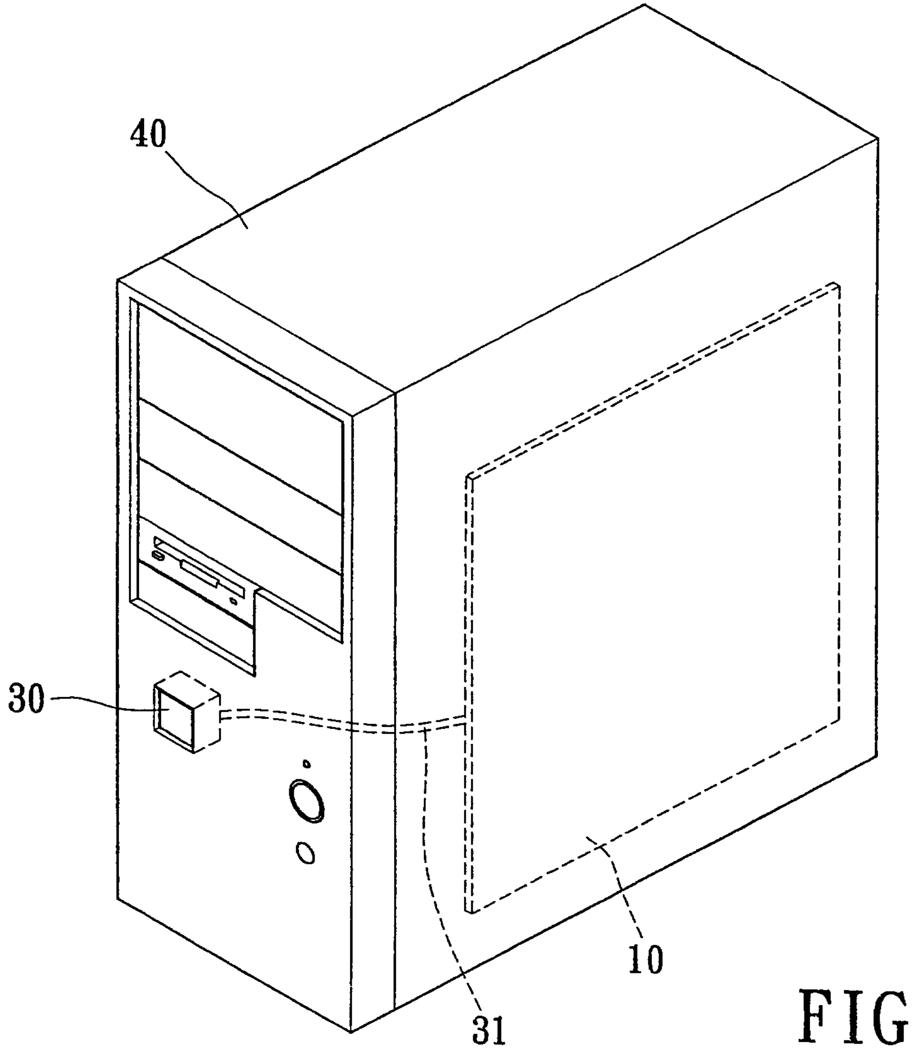

FIG. 3

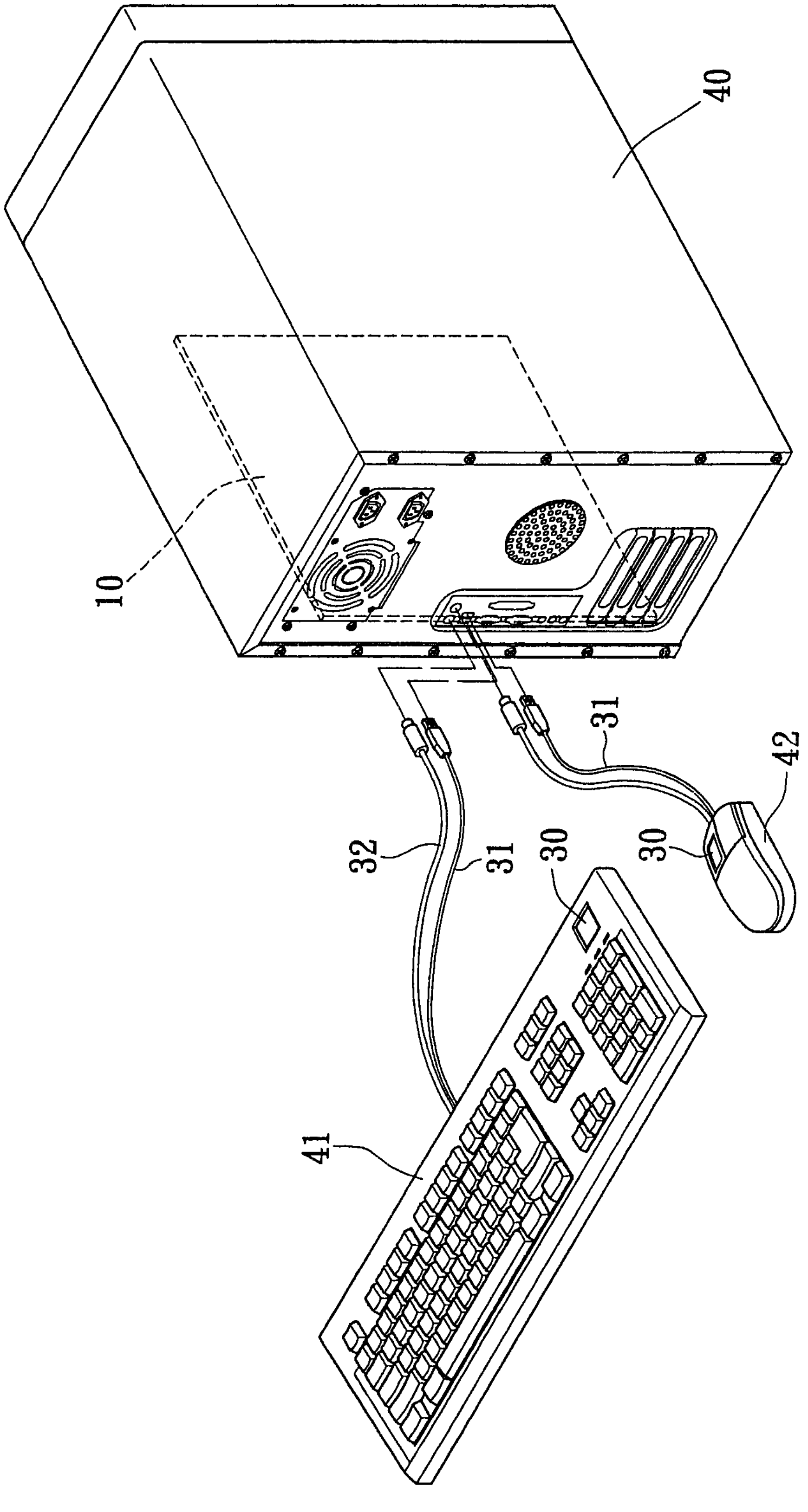

FIG. 4

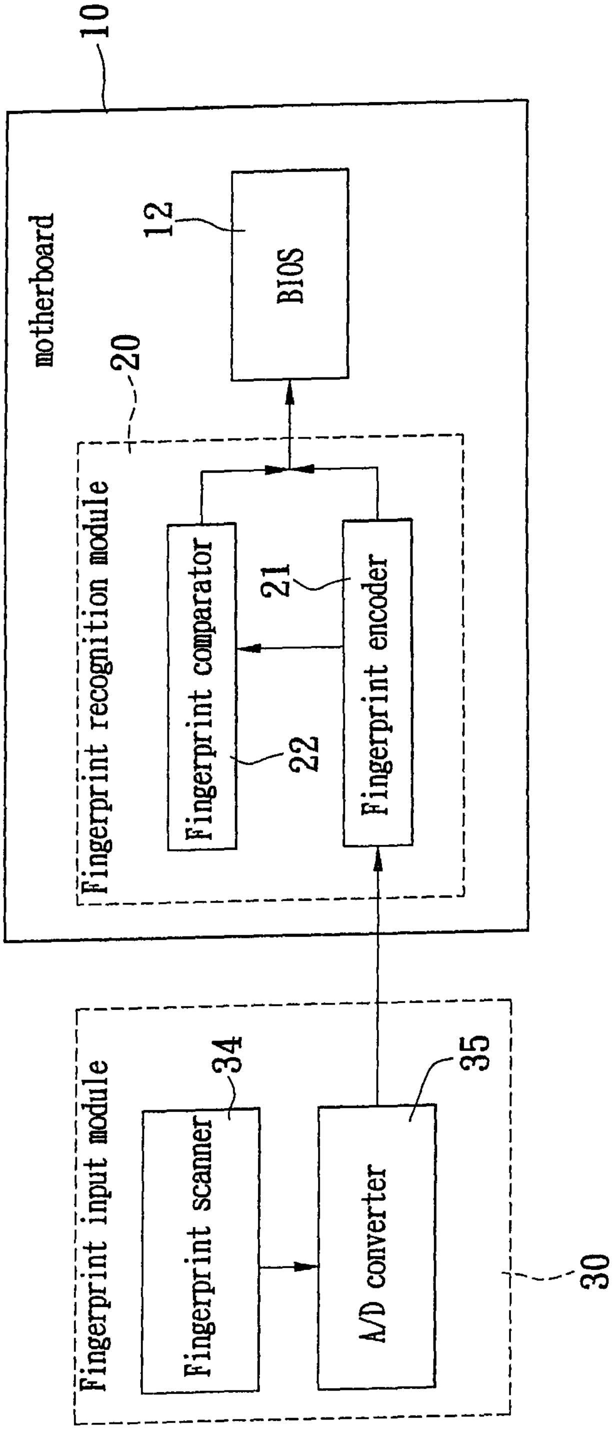
10
motherboard
12
BIOS
20
Fingerprint recognition module
Fingerprint comparator
22
21
Fingerprint encoder
Fingerprint input module
Fingerprint scanner
34
A/D converter
35
30

FIG. 5

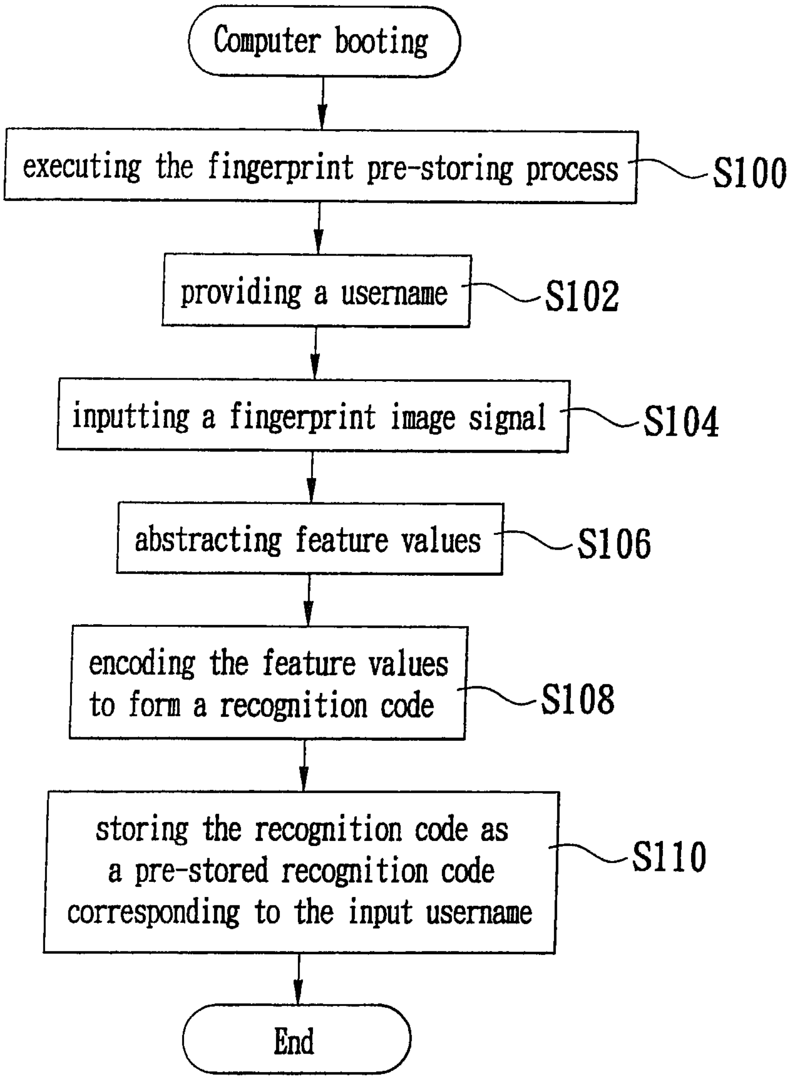
Computer booting
executing the fingerprint pre-storing process
S100
providing a username
S102
inputting a fingerprint image signal
S104
abstracting feature values
S106
encoding the feature values to form a recognition code
S108
storing the recognition code as a pre-stored recognition code corresponding to the input username
S110
End

FIG. 6

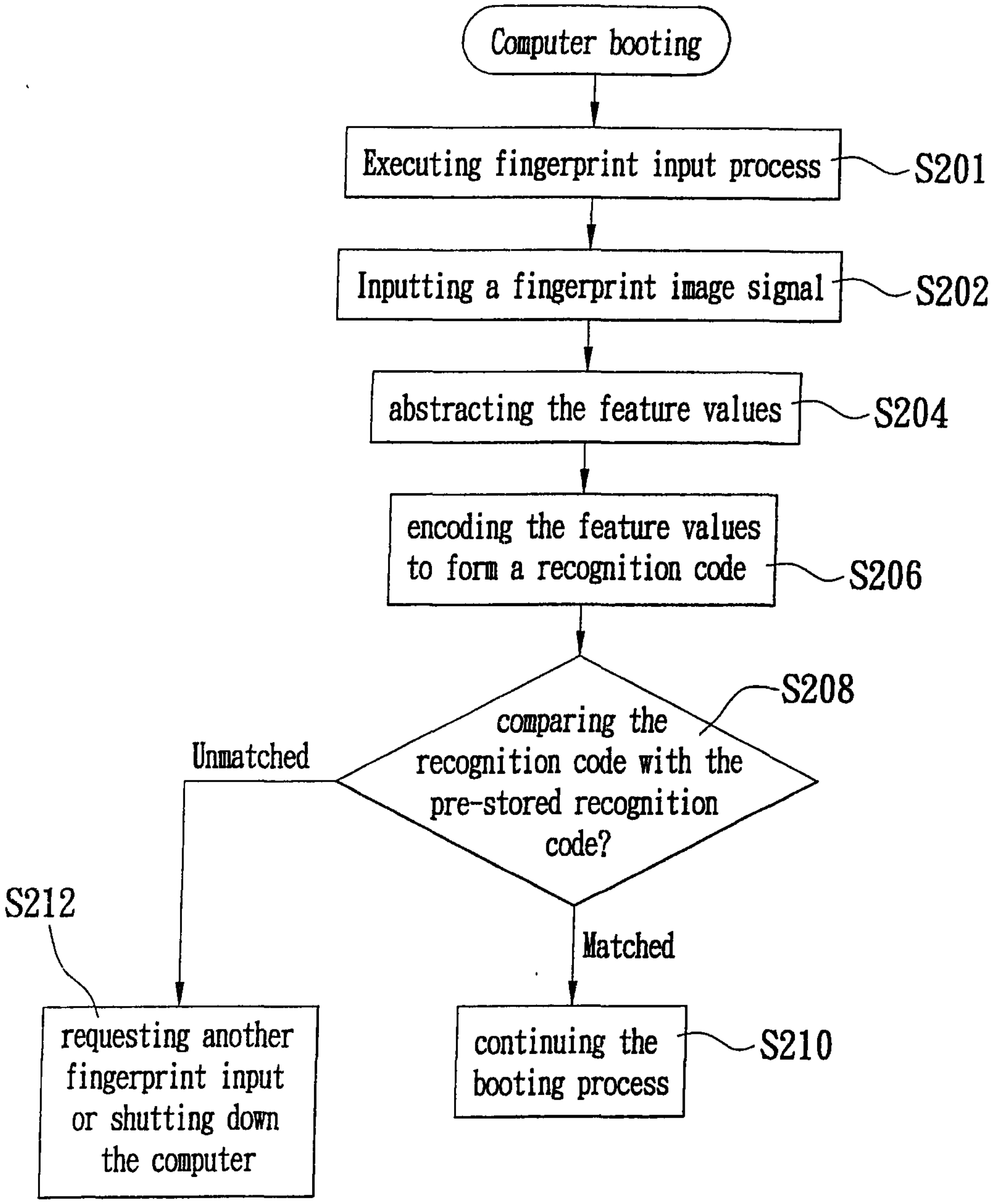
Computer booting
Executing fingerprint input process
S201
Inputting a fingerprint image signal
S202
abstracting the feature values
S204
encoding the feature values to form a recognition code
S206
comparing the recognition code with the pre-stored recognition code?
S208
Unmatched
Matched
S212
requesting another fingerprint input or shutting down the computer
continuing the booting process
S210

FIG. 7

METHOD FOR COMPUTER BOOTING

The present invention is directed to a method for computer booting e.g. using a motherboard combined with a fingerprint recognition module and an apparatus thereof, and more particularly, to a method and apparatus that combines the motherboard with the fingerprint recognition module, which is used to scan the fingerprint, for the security of the computer during booting.

Since each human fingerprint is unique and permanent the fingerprint identification is extensively used in many security systems. With the progress of science and technology, the hardware for fingerprint input has standardised as a module or a single chip. Hence, it has gradually been applied to many computer products or business transaction products, such as, for example, card-reading machines or automatic transfer machines.

As to the application of the computer products, fingerprint readers have been combined with the computer keyboards, computer mice or computer access devices, such hard disks or portable disks. The objective is to secure the computer software or hardware to prevent access to the computer by other persons. However, all of the recent fingerprint readers are connected with the computer externally and need additional software or drivers during connection or actuation. This is quite inconvenient.

In the prior art, computers all have a basic input/output system (BIOS), which has setting values of the computer hardware and a computer booting process used for booting the computer. In general, in order to prevent the computer from unauthorized access, a user usually sets a password in the BIOS. However, other people may steal the password and the programs for removing the password of the BIOS exist as well. Hence, the password cannot provide high security. It is inconvenient for the user if he forgets the password of the BIOS.

An object of the present invention is to overcome or alleviate at least some of the above problems.

In one aspect the present invention combines the fingerprint recognition module with the computer motherboard and uses the BIOS to drive the fingerprint recognition module directly to provide the security of the computer. Accordingly, the present invention can improve the drawbacks mentioned above.

One embodiment of the present invention combines a fingerprint recognition module with the computer motherboard and disposes a fingerprint input module on the computer housing or peripherals to acquire a user's fingerprints for identification during computer booting. Hence, it can be used to secure hardware or software of computers.

In one embodiment the present invention provides a method for computer booting, which disposes a fingerprint recognition module connected with a fingerprint input module on a motherboard of a computer and executes a fingerprint input process stored in a basic input/output system (BIOS) during booting or resetting the computer. First, it inputs a fingerprint image signal via the fingerprint input module and sends the fingerprint image signal to the fingerprint recognition module to produce a recognition code. Then, it compares the recognition code with at least a pre-stored recognition code to produce a comparison result, which is used to determine if booting the computer is permitted.

Preferably, the present invention further provides a method for computer booting, which utilises a fingerprint recognition module connected with a fingerprint input module on a motherboard of a computer and executes a fingerprint pre-storing process stored in a basic input/output system (BIOS) during booting or resetting the computer. First, it inputs a username, employs the fingerprint input module to provide a fingerprint image signal and sends the fingerprint image signal to the fingerprint recognition module to produce a recognition code. Then, it stores the recognition code as a pre-stored recognition code corresponding to the username and resets the computer in the end.

In a preferred embodiment there is provided a computer motherboard including a BIOS having a booting process, a fingerprint input module used to input at least a first fingerprint image, and a fingerprint recognition module electrically connected with the fingerprint input module and the BIOS for abstracting a feature value of the first fingerprint image and encoding the feature value to form a recognition code. When booting the computer, the booting process is able to control the fingerprint recognition module to compare the recognition code with at least a pre-stored recognition code to produce a comparison result used to determine if computer booting is permitted to continue.

Numerous additional features, benefits and details are described in the detailed description, which follows:

Preferred embodiments are described below by way of example only with reference to the following detailed description, when taken in conjunction with the accompanying drawings, wherein:

Fig. 1 is a block diagram of a conventional motherboard;

Fig. 2 is a block diagram of a motherboard having a fingerprint recognition module in accordance with the present invention;

Fig. 3 is a schematic diagram of the first embodiment in accordance with the present invention;

Fig. 4 is a schematic diagram of the second embodiment in accordance with the present invention;

Fig. 5 is a block diagram of a fingerprint module in accordance with the present invention;

Fig. 6 is a flowchart of a fingerprint pre-storing process in accordance with the present invention; and

Fig. 7 is a flowchart of a fingerprint input process in accordance with the present invention.

Reference is made to Fig. 1, which is a block diagram of a conventional motherboard. In general, a motherboard 10 is connected with a central processing unit (CPU) 11, a basic input/output system (BIOS) 12, a memory module 13, a display card 14, a sound card 15, at least a hard disk 16, multiple interfaces and so on for constituting a computer.

The BIOS 12 has a booting process 121 and a hardware setting process 122 as shown in Fig. 2. The booting process 121 is used to control the basic input/output devices during computer booting, whereas the hardware setting process 122 is used to initially set the basic hardware and store the initial setting values to a complementary metal-oxide semiconductor (CMOS) memory 17.

A conventional method for security of the computer is to employ the hardware setting process 122 to set a password and then store it in the CMOS memory 17. The password can be easily removed via resetting the CMOS memory 17. Hence, this security method is ineffectual.

Reference is made to Fig. 2, which is a block diagram of a motherboard having a fingerprint recognition module in accordance with the present invention. Motherboard 10 of the present invention has a fingerprint recognition module 20, which electrically connects with a fingerprint input module 30 and a BIOS 12. The present embodiment further includes a fingerprint input process 123 added to the BIOS 12 and a fingerprint pre-storing process 124 added to the BIOS 12. Hence, during computer booting, the BIOS 12 will identify the user by recognizing his fingerprint to provide security.

The fingerprint input module 30 is used to input at least a user's fingerprint image. The fingerprint recognition module 20 is used to recognize the fingerprint signal and convert it into a recognition code. The fingerprint input process 123 is used to control the fingerprint recognition module 20 to compare the recognition code with at least a pre-stored recognition code to produce a comparison result. Then, the BIOS 12 will determine whether or not to boot the computer according to the result.

In general, the BIOS 12 is an electrically erasable programmable read-only memory (EEPROM), which has the booting process and so on as mentioned above. A preferred embodiment of the present invention uses an EEPROM with larger storage capacity as the BIOS 12, which has a storage region to store user's pre-stored recognition code. Hence, when the CMOS memory 17 is reset, the user's pre-stored recognition code in the EEPROM will not be removed so as to provide security.

In other embodiments another storage device can be used to store the pre-stored recognition code. The storage device can be a non-volatile memory, such as a flash memory or the hard disk 16. The storage device is electrically connected with the fingerprint recognition module 20 and also used to store temporarily the fingerprint image input from the fingerprint input module 30.

For convenience, the fingerprint input module 30 is disposed on the housing 40 of the computer as shown in Fig. 3, which is a schematic diagram of the first embodiment. The fingerprint input module 30 is electrically connected with the fingerprint recognition module 20 of the motherboard 10 via a fingerprint transmission line 31.

Fig. 4 is a schematic diagram of a second embodiment. The fingerprint input module 30 can also be disposed on a keyboard 41 or a mouse 42 and is electrically connected with the fingerprint recognition module 20 via the fingerprint transmission line 31, which is combined with the keyboard transmission line 32 or mouse transmission line 33.

Although the fingerprint recognition module 20 is disposed on the motherboard 10, in practice, the fingerprint input module 30 still needs to use a transmission interface as the fingerprint transmission line 31 to electrically connect with the fingerprint recognition module 20. The transmission interface can be a universal serial bus (USB), an IEEE1394 interface, a RS-232 interface, a PS2 interface or a parallel port interface.

Reference is made to Fig. 5, which is a block diagram of a fingerprint input module. The fingerprint input module 30 is preferably a fingerprint input integrated circuit (IC) and the fingerprint recognition module 20 can also be a fingerprint recognition IC. The fingerprint input module 30 has a fingerprint scanner 34 (optical type or IC type) and an analog/digital (A/D) converter 35. The fingerprint recognition module 20 has a fingerprint encoder 21 and a fingerprint comparator 22.

The fingerprint scanner 34 is used to input a user's fingerprint image and the A/D converter 35 is used to convert the fingerprint image into a digital fingerprint image signal. The fingerprint encoder 21 is used to abstract the fingerprint features from the digital fingerprint image signal and encode it as a recognition code, whereas the fingerprint comparator 22 is used to compare the recognition code and a pre-stored recognition code to produce a compared recognition.

Reference is made to Fig. 6, which is a flowchart of a fingerprint pre-storing process useful in the method of the present invention. Since the user is identified before computer booting, it is necessary to pre-store the user's fingerprint to form the pre-stored recognition code. Hence, executing the fingerprint pre-storing process 124 is necessary during computer booting. A user can choose an item of the menu of the hardware setting process 122 or press a corresponding hot-key of the keyboard 41 to execute the fingerprint pre-storing process 124 during computer booting (S100).

First, the user needs to provide a username to the fingerprint pre-storing process 124 (S102). Then, the user needs to use the fingerprint input module 30 to produce a fingerprint image signal (S104). The fingerprint image signal will be sent to the fingerprint recognition module 20, which will abstract feature values from the fingerprint image signal (S106), encode the feature values as a recognition code (S108) and then store the recognition code as a pre-stored recognition code corresponded to the input username (S110). After finishing the fingerprint pre-storing process, the user can reset the computer.

Reference is made to Fig. 7, which is a flowchart of a fingerprint input process useful in the above embodiment. After finishing the fingerprint pre-storing process and re-starting the computer, the computer will execute the booting process 121 and the fingerprint input process 123 (S201). The user can input his fingerprint image via the fingerprint input module 30 to produce the fingerprint image signal (S202). Subsequently, the fingerprint image signal will be sent to the fingerprint recognition module 20 to abstract the feature values (S204) and then encode them to form a recognition code (S206). Finally, the fingerprint recognition module 20 will compare the recognition code with the pre-stored recognition code (S208) to produce a comparison result. If the comparison result shows that the recognition code matches the pre-stored one, the booting process will be continued (S210). Otherwise, the system will require the user to input his fingerprint again or shut down the computer.

Although the present invention has been described with reference to the preferred embodiment thereof, it will be understood that the invention is not limited to the details thereof. Various substitutions and modifications have been suggested in the foregoing description, and other will occur to those of ordinary skill in the art. Therefore, all such substitutions and modifications are embraced within the scope of the invention as defined in the appended claims.

In one variant, biometric data other than fingerprint data, e.g. data acquired by an iris scanner can be used to control booting.

CLAIMS:

1. A method for computer booting, wherein a fingerprint recognition module connected with a fingerprint input module on a motherboard of a computer executes a fingerprint input process stored in a basic input/output system (BIOS) during booting or resetting the computer, the method comprising:

inputting a fingerprint image signal via the fingerprint input module;

sending the fingerprint image signal to the fingerprint recognition module to produce a recognition code; and

comparing the recognition code with at least a pre-stored recognition code to produce a comparison result, wherein the comparison result is used to determine if booting the computer is permitted.

2. The method as claimed in claim 1, wherein, in the step of inputting the fingerprint image signal, the fingerprint image signal is stored in the BIOS, a non-volatile memory or a hard disk.

3. The method as claimed in claim 1 or claim 2, wherein the step of sending the fingerprint image signal to the fingerprint recognition module to produce the recognition code further comprises:

abstracting at least a feature value from the fingerprint image signal; and

encoding the feature value to form the recognition code.

4. The method as claimed in any preceding claim, wherein the step of comparing the recognition code with the pre-stored recognition code employs the fingerprint recognition module to compare the recognition code with the pre-stored recognition code.

5. The method as claimed in any preceding claim, wherein the step of comparing the recognition code with the pre-stored recognition code to produce

the comparison result used to determine if booting the computer is permitted further comprises:

continuing a booting process if the comparison result shows that the recognition code matches the pre-stored recognition code; and

requesting another fingerprint input or shutting down the computer if the comparison result shows that the recognition code doesn't match the pre-stored recognition code.

6. A method for computer booting, wherein a fingerprint recognition module connected with a fingerprint input module on a motherboard of a computer executes a fingerprint pre-storing process stored in a basic input/output system (BIOS) during booting or resetting the computer, the method comprising:

providing a username;

employing the fingerprint input module to provide a fingerprint image signal;

sending the fingerprint image signal to the fingerprint recognition module to produce a recognition code;

storing the recognition code as a pre-stored recognition code corresponding to the username; and resetting the computer.

7. The method as claimed in claim 6, wherein the BIOS is an electrically erasable programmable read-only memory (EEPROM) having a storage region for storing the pre-stored recognition code.

8. The method as claimed in claim 6, wherein the BIOS is a flash memory having a storage region for storing the pre-stored recognition code.

9. The method as claimed in claim 6, wherein, in the step of storing the recognition code, the pre-stored recognition code is stored in a non-volatile memory or a hard disk.

10. The method as claimed in claim 6, wherein, in the step of sending the fingerprint image signal, the fingerprint image signal is stored in the BIOS, a non-volatile memory or a hard disk.

11. The method as claimed in any of claims 6 to 10, wherein the step of sending the fingerprint image signal to the fingerprint recognition module to produce the recognition code further comprises:

abstracting at least a feature value from the fingerprint image signal; and encoding the feature value to form the recognition code.

12. The method as claimed in any of claims 6 to 11, comprising:

choosing an item of a menu of the BIOS to execute the fingerprint pre-storing process.

13. The method as claimed in any of claims 6 to 12, comprising:

pressing a hot key of a keyboard to execute the fingerprint pre-storing process.

14. A computer motherboard, comprising:

a BIOS having a booting process;

a fingerprint input module used to input at least a first fingerprint image; and

a fingerprint recognition module electrically connected with the fingerprint input module and the BIOS for abstracting a feature value of the first fingerprint image and encoding the feature value to form a recognition code;

wherein, during computer booting, the booting process is arranged to control the fingerprint recognition module to compare the recognition code with at least a pre-stored recognition code to produce a comparison result used to determine if computer booting is permitted to continue.

15. The computer motherboard as claimed in claim 14, wherein the BIOS is an EEPROM having a storage region for storing the pre-stored recognition code.

16. The computer motherboard as claimed in claim 14, wherein the BIOS is a flash memory having a storage region for storing the pre-stored recognition code.

17. The computer motherboard as claimed in any of claims 14 to 16, wherein the BIOS further has a fingerprint pre-storing process used to input at least a second fingerprint to provide the pre-stored recognition code, and wherein the pre-stored recognition code is stored in a non-volatile memory, via the fingerprint input module and the fingerprint recognition module.

18. The computer motherboard as claimed in any of claims 14 to 17, wherein the fingerprint input module is disposed on a computer housing and connected with the fingerprint recognition module of the computer motherboard via a fingerprint transmission line.

19. The computer motherboard as claimed in any of claims 14 to 17, wherein the fingerprint input module is disposed on a computer keyboard and connected with the fingerprint recognition module of the computer motherboard via a fingerprint transmission line combined with a transmission line of the keyboard.

20. The computer motherboard as claimed in any of claims 14 to 17, wherein the fingerprint input module is disposed on a mouse and connected with the fingerprint recognition module of the computer motherboard via a fingerprint transmission line combined with a transmission line of the mouse.

21. The computer motherboard as claimed in any of claims 14 to 20, wherein the fingerprint input module further comprises:

a fingerprint scanner 34 used to input the first fingerprint image; and an analog/digital (A/D) converter used to convert the first fingerprint image into a digital fingerprint image signal.

22. The computer motherboard as claimed in any of claims 14 to 21, wherein the fingerprint recognition module is a fingerprint recognition integrated circuit (IC).

23. The computer motherboard as claimed in any of claims 14 to 22, wherein the fingerprint recognition module further comprises:

a fingerprint encoder used to abstract the feature value of the first fingerprint image and encode the feature value to form the recognition code; and

a fingerprint comparator used to compare the recognition code with the pre-stored recognition code to produce the comparison result.

24. The computer motherboard as claimed in any of claims 14 to 23, further comprising:

a storage device electrically connected with the fingerprint recognition module to store the first fingerprint image and the pre-stored recognition code.

25. The computer motherboard as claimed in claim 24, wherein the storage device is a non-volatile memory or a hard disk.

26. 26. The computer motherboard as claimed in claim 25, wherein the non-volatile memory is a flash memory.

27. The computer motherboard as claimed in any of claims 14 to 26, further comprising:

a transmission interface disposed on the computer motherboard to electrically connect the fingerprint recognition module with the fingerprint input module.

28. The computer motherboard as claimed in claim 27, wherein the transmission interface is a universal serial bus (USB), an IEEE1394 interface, a RS-232 interface, a PS2 interface or a parallel port interface.

29. A method of controlling booting of a computer wherein the BIOS of the computer is responsive to a comparison between stored biometric data of an authorised user and newly acquired biometric data from a biometric scanner to permit or prevent booting.

30. A computer motherboard comprising a BIOS module arranged to compare stored biometric data of an authorised user with newly acquired biometric input data and to prevent booting in the event of a discrepancy.

31. A computer motherboard substantially as described hereinabove with reference to Figs.2, 3 and 5 or 2, 4 and 5 of the accompanying drawings.

32. A method of booting a computer substantially as described hereinabove with reference to Figs. 6 and 7 of the accompanying drawings.

PATENTS • DESIGNS
The Patent Office
COPYRIGHT • TRADE MARKS

INVESTOR IN PEOPLE

Application No:	GB0405410.2	**Examiner:**	Matthew Nelson
Claims searched:	1-5, 14-30	**Date of search:**	7 July 2004

Patents Act 1977: Search Report under Section 17

Documents considered to be relevant:

Category	Relevant to claims	Identity of document and passage or figure of particular reference
X	1-5, 15-18, 21-30	WO 99/47989 A1 (VERIDICOM) See whole document in particular figures 1, 4B and 5.
X	1-5, 14, 17-30	US 2003/0070079 A1 (CROMER et al) See e.g. paragraphs [0017], [0018], [0025] and figure 1.
X	1-5, 14, 17-30	US 2001/0032319 A1 (SETLAK) See paragraphs [0022]-[0026] and figures 2 and 3.
X	1-5, 14-17, 20-30	US 5838306 A (O'Connor et al) See in particular col. 3, lines 23-41; col. 4, lines 16-62; col. 5, lines 18-40 and col. 7, lines 5-10.
X	1-5, 14, 17-19, 21-30	IBM Technical Disclosure Bulletin, Vol. 41, No. 1, January 1998, "Biometric Access Control in a Personal Computer System", pages 753-756.

Categories:

X	Document indicating lack of novelty or inventive step	A	Document indicating technological background and/or state of the art.
Y	Document indicating lack of inventive step if combined with one or more other documents of same category.	P	Document published on or after the declared priority date but before the filing date of this invention.
&	Member of the same patent family	E	Patent document published on or after, but with priority date earlier than, the filing date of this application.

Field of Search:

Search of GB, EP, WO & US patent documents classified in the following areas of the UKC^{W} :

G4A

Worldwide search of patent documents classified in the following areas of the IPC^{07}

G06F

The following online and other databases have been used in the preparation of this search report

Online: WPI, EPODOC, JAPIO