

(19)



(11)

EP 1 821 264 A2

(12)

EUROPEAN PATENT APPLICATION

(43) Date of publication:

22.08.2007 Bulletin 2007/34

(51) Int Cl.:

G07C 9/00 (2006.01)

(21) Application number: **07250333.7**

(22) Date of filing: **26.01.2007**

(84) Designated Contracting States:

**AT BE BG CH CY CZ DE DK EE ES FI FR GB GR
HU IE IS IT LI LT LU LV MC NL PL PT RO SE SI
SK TR**

Designated Extension States:

AL BA HR MK YU

(30) Priority: **01.02.2006 GB 0601990**

(71) Applicant: **Eja Limited**

**Hindley Green Industrial Estate,
Wigan WN2 4HR (GB)**

(72) Inventors:

- **Poyner, Julian**
Stockport, SK7 6JS (GB)

• **Jones, Derek**

**Clamhan Cottage
Dumfries & Galloway DG6 4SP
Scotland (GB)**

• **Nair, Suresh**

**Amherst
New Hampshire 03031 (US)**

• **Sawyer, Derek**

**Cadiar
Granada 18448 (ES)**

• **Parker, Gillian**

Wigan WN6 7BW (GB)

(74) Representative: **Roberts, Peter David et al**

**Marks & Clerk,
Sussex House,
83-85 Mosley Street
Manchester M2 3LG (GB)**

(54) **Safety switch**

(57) According to an aspect of the present invention there is provided a safety switch arranged to allow the control of power supplied to an apparatus, wherein the safety switch is provided with a biometric sensor module

arranged to obtain biological information from a user of the safety switch, such that activation of the safety switch is controlled via the biological information obtained.

EP 1 821 264 A2

Description

[0001] The present invention relates to safety switches.

[0002] A safety switch may be considered as an emergency electrical shut off switch, and either allows or prevents electricity from passing through it (i.e. it provides a closed circuit or an open circuit). If the safety switch is activated, such that it forms an open circuit, electricity will not pass to any apparatus to which the safety switch is connected.

[0003] Safety switches are often used in places where access to particular enclosures is to be restricted, such as enclosures enclosing electrically operated machinery. For example, safety switches are often found in factories that use kinetic machinery powered by electricity. The safety switch may be used to prevent access to an enclosure containing the machinery when the machinery is in operation. Specifically, power will only be supplied to the machinery when the switch is closed, and this is conveniently achieved by the closure of a gate incorporated in the enclosure. When the gate is opened, the safety switch is activated, the circuit is broken, and the electrical power supply to the machinery is interrupted (i.e. the machinery cannot run when the gate is opened and the safety switch is thereby activated). Safety switches are well known in the art, and come in a variety of different forms.

[0004] A safety switch will usually comprise a switch mechanism that is housed in a housing and attached to part of a structure forming the enclosure. A protruding actuator (i.e. a key) may be attached to a gate which is movable relative to the enclosure and the safety switch mechanism. When the gate is closed, the actuator engages with the switch mechanism to allow supply of electrical power to the machinery. Alternatively, the actuator may not be attached to the gate. Although access to the enclosure is still achieved by insertion of the actuator into the switch mechanism, the mechanism can be located at any suitable point, and the actuator may be carried around by a user and used as and when necessary (i.e. in the same manner as a house key).

[0005] While safety switches are intended to be beneficial to workers using and moving around dangerous machinery within a factory (for example), it is not uncommon for the safety features to be circumvented or abused. For example, it may be that workers wish to inspect dangerous machinery while it is in operation. In order to do this a worker may obtain a replacement key, or fabricate a makeshift one for him/herself to engage with the safety switch mechanism such that the machinery may be operable even when the gate remains open. Since the purpose of the safety switch is to prevent such access to the enclosure when machinery is in operation, thereby maintaining the safety of the workers, the use of a replacement or unauthorised key is not desirable.

[0006] It is thus an object of the present invention to obviate or mitigate at least one of the above-mentioned disadvantages.

[0007] According to a first aspect of the invention there is provided a safety switch arranged to allow the control of power supplied to an apparatus, wherein the safety switch is provided with a biometric sensor module arranged to obtain biological information from a user of the safety switch, such that activation of the safety switch is controlled via the biological information obtained

[0008] According to a second aspect of the invention there is provided a safety switch arranged to receive biological information from a biometric sensor module.

[0009] According to a third aspect of the invention there is provided a method of operating a safety switch, the safety switch being arranged to allow the control of power supplied to an apparatus, and wherein the safety switch is provided with a biometric sensor module arranged to obtain biological information from a user of the safety switch, such that activation of the safety switch is controlled via the biological information obtained, and wherein the method comprises: obtaining biological information from a user wishing to activate the safety switch via the biometric sensor module to; comparing the obtained biological information with authorised biological information from one or more users authorised to activate the safety switch; and activating the switch if the biological information obtained from the user matches the authorised biological information.

[0010] By incorporating a biometric sensor into the safety switch, access to an enclosure can be more readily controlled. This will help to prevent access by unauthorised users. For example, the safety switch may be provided with a fingerprint reader. The fingerprints read by the fingerprint reader may be compared with one or more stored (and authorised) fingerprints. Only users with authorised fingerprints can gain access to the enclosure.

[0011] Embodiments of the present invention will now be described, by way of example only, with reference to the accompanying drawings, in which:

Figure 1a depicts an enclosure incorporating a prior art safety switch;

Figure 1b depicts the prior art safety switch of Figure 1a;

Figure 2 depicts a safety switch according to an embodiment of the present invention;

Figures 3a and 3b illustrates operating principles of the embodiment of figure 2;

Figures 4a and 4b depict another embodiment of the present invention.

[0012] Figure 1 depicts a perspective view of an enclosure 1 enclosing electrically powered machinery 2. Access to the machinery 2 within the enclosure 1 is gained via a gate 3. The gate 3 is provided with a prior art safety switch 4. The gate 3 is opened by activation of the safety switch 4. When a safety switch 4 is activated, supply of electricity to the machinery 2 is interrupted such that when a user enters the enclosure 1 by opening the gate 3, the machinery 2 is not functioning. For example,

if the machinery 2 is electrically operated kinetic machinery, activation of the safety switch 4 will deactivate the machinery, and stop any movement thereof.

[0013] Figure 1b shows how the safety switch 4 is activated. The safety switch 4 is provided with an opening 5, which is arranged to receive an actuator (e.g. a key) 6. If the actuator 6 is of the correct shape, engagement of the actuator 6 with the safety switch 4 via the opening 5 will cause the safety switch 4 to activate. As described above, when activated, the safety switch 4 interrupts power supply to the machinery 2 enclosed in the enclosure 1.

[0014] It will be appreciated that the known safety switch 4 provides a useful safety feature, whereby it is not possible to enter the enclosure 1 without electrical supply to machinery 2 enclosed therein being interrupted. However, the safety switch 4 of figures 1a and 1b does not discriminate between different users. If the actuator 6 is of the correct shape, any user using that actuator 6 can gain access to the enclosure 1. It is therefore possible that unauthorised people may gain access to the enclosure 1 by obtaining copies of the actuator 6, or using the actuator 6 without authorisation. Such unauthorised use or copying circumvents the safety features provided by the safety switch 4, and this is undesirable.

[0015] Figure 2 depicts a perspective view of a safety switch 7 according to an embodiment of the present invention. The safety switch 7 is provided with a biometric sensor module. In this embodiment, the biometric sensor module is provided with a fingerprint reader 8. The fingerprint reader may be, for example, an EntréPad 4000 by AuthenTec, Melbourne USA, or an AT77C101B FingerChip™ by Atmel™ Corporation, San Jose, USA.

[0016] In use, a user wishing to enter an enclosure such as that described in relation to figure 1a places a finger 9 on the fingerprint reader 8. The fingerprint reader 8 reads the fingerprint of the finger 9 of the user in a known manner.

[0017] Figure 3a schematically illustrates the operating principles of the safety switch of figure 2. A fingerprint 100 is taken from the fingerprint reader 8. The fingerprint 100 is then interpreted by two processors: a first processor 101 and a second processor 102. The two processors 101, 102 are independent, in that the first processor 101 interprets the fingerprint 100 independently from the second processor 102.

[0018] Each processor 101, 102 interprets the fingerprint 100, and references a store of authorised fingerprints 103. Each processor 101, 102 identifies if the obtained fingerprint 100 is an authorised (i.e. stored) fingerprint, and if so, which user it belongs to. Figure 3b shows how the fingerprint 100 may be compared with a stored fingerprint. Fingerprints may be compared in a known manner, for example by a known software or hardware comparator.

[0019] Referring back to figure 3a, the processors 101, 102 then pass fingerprint information 104, 105 to a comparator 106. If the fingerprint information 104, 105 sent

to the comparator 106 relates to the same authorised user, then the comparator 106 generates a positive signal that is sent to a safety switch control 107. If the comparator 106 does not receive the same fingerprint information 104, 105 from both processors 101, 102, then the fingerprint 100 has not been correctly interpreted by one or both of the processors and a positive signal is not sent to the safety switch control 107. A positive signal is not sent to the safety switch control 107 if either processor 101, 102 identifies the fingerprint 100 as belonging to an unauthorised user.

[0020] If the safety switch control 107 receives a positive signal from the comparator 106 the safety switch is activated, and the safety switch control 107 cuts the power to the machinery 2 while simultaneously (or after a short delay) unlocking a lock 108 incorporated in an access door to the enclosure, so that a user may gain access thereto.

[0021] By using more than one processor 101, 102 to interpret the fingerprint 100, a verification step is introduced. Only if all of the processors 101, 102 are able to identify the fingerprint 100 as an authorised fingerprint will access to the enclosure be allowed. This is a useful fail-safe if, for example, one of the processors has failed and always deems the obtained fingerprint to be an authorised fingerprint.

[0022] The operating principles illustrated in figure 3a are given by way of example only. It will be appreciated that any suitable hardware or process configuration may be employed. For example, more than one store of authorised fingerprints 103 may be provided. A fingerprint store 103 may be provided for and accessed by each processor 101, 102. Comparative logic could be provided in each of the processors 101, 102, as opposed to being provided in a comparator 106. If the processors 101, 102 are provided with the comparative logic, there may be no need for the use of a comparator 106. Instead, the processors 101, 102 could communicate directly with the safety switch control 107. The processors 101, 102 could be in communication with one another to ensure that the safety switch is only activated when each processor 101, 102 independently interprets the fingerprint 100 as being that of the same authorised user.

[0023] The safety switch 7 of figure 2 is provided with a fingerprint reader 8 that may be used by a plurality of users. In an alternative arrangement, each individual user may have an individual fingerprint reader which is connectable to a safety switch. This provides an additional level of security, whereby a user must not only have the correct fingerprint, but must also have access to a fingerprint reader that is connectable to the safety switch.

[0024] Figures 4a and 4b describe a safety switch 10 which is arranged to receive and electrically connect with a removable biometric sensor module 11 via an opening 12 in the safety switch 10.

[0025] The biometric sensor module 11 is provided with a fingerprint reader 13 and a connector 14 arranged to be received by the safety switch 10. The connector 14

may be, for example, a Universal Serial Bus (USB) connector, or any other suitable connector.

[0026] In use, an authorised user will have a biometric sensor module 11. The biometric sensor module 11 will be brought into engagement with the safety switch 10 such that the fingerprint reader 13 is in electrical connection with the switch 10. Thereafter, the safety switch 10 and the fingerprint reader 13 of figure 4b work in exactly the same way as described in relation to the safety switch 7 and the fingertip reader 8 of figure 2. After use, the biometric sensor module 11 may be removed from connection with the safety switch.

[0027] By providing a safety switch that is able to identify specific (authorised) users, additional benefits beyond the controlled activation of the switch may be realised. For example, once a specific user has activated the switch, control of the switch can be configured such that power cannot be supplied to the machinery until the same specific user has left the enclosure and placed his/her finger on the fingerprint reader, i.e. the biometric sensor module serves as an advanced off-on switch. In this way, another user cannot inadvertently activate the machinery after it has been turned off, even if the other user is an authorised user.

[0028] In situations where a high degree of security is required, the safety switch may be configured such that it may only be activated and/or deactivated when more than one fingerprint is used in succession. For example, the safety switch may require the fingerprints of two different authorised users to be activated and/or deactivated. Where a plurality of safety switches are used, for example to control access to one or more enclosures, each safety switch can be configured to allow access to a specific set of authorised users. For example, untrained employees may only be allowed into a first, peripheral enclosure, whereas trained employees may be allowed into a central enclosure, which is more dangerous due to the presence of machinery.

[0029] In the above-described embodiments, control circuitry used to obtain the fingerprint, a storage medium for storing authorised fingerprints and a comparator for comparing the obtained fingerprint with the stored fingerprints, may be located in the biometric sensor module, the safety switch or a computer system (e.g. a server) connected to the biometric sensor module and/or the safety switch. By locating the storage medium on a server, which may be remote from the safety switch and fingerprint reader, the store of authorised fingerprints may be centrally managed. This makes it easier to control who is authorised to access the enclosure.

[0030] The safety switch may be programmed with a unique identification number. To activate the safety switch the biometric sensor module or the server would have to match the fingerprint data with the switch identification number. This would restrict activation of individual safety switches to certain users. The safety switch could be programmed with the unique identification number and fingerprint data from one individual source

(e.g. the computer system or server). The source may be protected from unauthorised access in a conventional manner (e.g. password protection).

[0031] An access log may be provided which details authorised and attempted non-authorised use of the safety switch. The access log may be stored in the safety switch, the biometric sensor module or the computer system. Fingerprints of non-authorised users who attempt to activate the switch may be stored so that the non-authorised user can be identified (if necessary) at a later date.

[0032] In the case where the biometric sensor module is removable (for example the biometric sensor module 11 of figure 4a), the biometric sensor module 11 may be provided with a power source sufficient to activate the safety switch 10. Alternatively, the biometric sensor module 11 may be a passive device.

[0033] The embodiments described above have made reference to a fingerprint reader. However, it will be appreciated that any suitable biometric sensor may be used. For example, a retina scanner may be used, or any other biometric sensor that is able to uniquely identify a user by obtaining biological information therefrom. A fingerprint reader is preferable as these devices are cheaper and more reliable than many other biometric sensors. Any suitable fingerprint reader may be used. For example, a fingerprint reader requiring a single impression of a fingerprint may be used. Alternatively, a fingerprint reader requiring a fingerprint to be dragged across a sensor may be used.

[0034] Authorised and appropriate (i.e. corresponding to the type of sensor used) biological information may be stored in the biometric sensor module or the safety switch.

[0035] It will be appreciated that the present invention is applicable to any safety switch. The above described embodiments have made reference to activating the safety switch. It will be appreciated that the exact nature of the activation will depend on the mechanisms and operation of the safety switch concerned. For example, activation of a safety switch may involve an electrical signal being generated, which causes an electromagnet to be energised that in turn causes a pair of contacts within the safety switch to open. Opening of these contacts may cause a break in a circuit which interrupts the power supplied to machinery within the enclosure. It is to be appreciated, however, that any suitable switch mechanism may be employed.

[0036] The above described embodiments have described the biometric sensor module as being in electrical connection with the safety switch or connectable to the safety switch. The connection however may be wireless. For example, the obtained biological information (e.g. a fingerprint) may be transmitted to the safety switch by pressure waves or electromagnetic waves. The electromagnetic waves may be radio waves. In this way, the safety switch may be operated remotely, or may not require an opening that could become contaminated with

dirt.

[0037] The biometric sensor module may be provided with a radio-wave emitter that is arranged to emit a specific signal (i.e. a signal specific to and therefore identifying an individual biometric sensor module). Only if the fingerprint and radio signal are deemed to be authorised will the switch be activated, i.e. the radio signal acts as a further security check. Alternatively or additionally, the detection by the switch of such a specific radio signal may allow the switch to prepare for an expected user. For example, rather than having to compare the fingerprint with a store of fingerprints, the received radio signal can be used to identify and retrieve a specific fingerprint. When the user tries to access the enclosure using the fingerprint reader, the safety switch need only check that the fingerprint is the one that it is expecting. This may improve the efficiency of checking whether a user is authorised, i.e. make access or denial quicker.

[0038] It will be appreciated that an enclosure may be anything which encloses powered apparatus (e.g. machinery), the power supply to which is controlled by a safety switch. An enclosure may be, for example, a room, a cage or a fully or partially fenced off area. The apparatus may be powered electrically, and the supply of electrical power to the machinery may cause activation of a pneumatic or hydraulic system. These systems will also be shutdown when the supply of electrical power to the machinery is interrupted.

[0039] It will be appreciated that the above embodiments of the invention have been described by way of example only, and that various modifications may be made to these embodiments without detracting from the invention, which is defined by the claims that follow.

Claims

1. A safety switch arranged to allow the control of power supplied to an apparatus, wherein the safety switch is provided with a biometric sensor module arranged to obtain biological information from a user of the safety switch, such that activation of the safety switch is controlled via the biological information obtained.
2. A safety switch as claimed in claim 1, wherein the biometric sensor module comprises a fingerprint reader.
3. A safety switch as claimed in claim 1 or claim 2, wherein the safety switch comprises a first processor arranged to interpret the biological information.
4. A safety switch as claimed in claim 3, wherein the biometric sensor module is provided with the first processor.
5. A safety switch as claimed in any preceding claim, wherein the safety switch comprises a second processor arranged to interpret the biological information.
6. A safety switch as claimed in claim 5, wherein the biometric sensor module is provided with the second processor.
7. A safety switch as claimed in any preceding claim, wherein the safety switch comprises a comparator for comparing the obtained biological information with authorised biological information from one or more users authorised to activate the safety switch.
8. A safety switch as claimed in claim 7, wherein the biometric sensor module is provided with the comparator.
9. A safety switch as claimed in claim 7 or claim 8, wherein the safety switch comprises a database or other storage medium arranged to store the authorised biological information.
10. A safety switch as claimed in claim 9, wherein the biometric sensor module is provided with the database or other storage medium.
11. A safety switch as claimed in claim 7 or claim 8, wherein a database or other storage medium arranged to store the authorised biological information is provided on a server.
12. A safety switch as claimed in any preceding claim, wherein the biometric sensor module is removable from the safety switch.
13. A safety switch as claimed in any preceding claim, wherein the biometric sensor module is arranged to provide a signal in the form of one of a group comprising: an electrical signal, a pressure wave and an electromagnetic wave.
14. A safety switch as claimed in 13, wherein the signal comprises the biological information.
15. A safety switch as claimed in any preceding claim, wherein the biometric sensor module is provided with a power source.
16. A safety switch as claimed in any preceding claim, wherein the safety switch is arranged to allow the control of electrical power supplied to an apparatus.
17. A safety switch arranged to receive biological information from a biometric sensor module.
18. A safety switch as claimed in claim 17, wherein the safety switch is arranged to receive the biometric sensor module.

19. A method of operating a safety switch, the safety switch being arranged to allow the control of power supplied to an apparatus, and wherein the safety switch is provided with a biometric sensor module arranged to obtain biological information from a user of the safety switch, such that activation of the safety switch is controlled via the biological information obtained, and wherein the method comprises:
- obtaining biological information from a user wishing to activate the safety switch via the biometric sensor module to;
- comparing the obtained biological information with authorised biological information from one or more users authorised to activate the safety switch; and
- activating the switch if the biological information obtained from the user matches the authorised biological information.
20. A method of operating a safety switch as claimed in claim 19, wherein the switch may only be deactivated if the user who activated the switch provides biological information to the biometric sensor module.
21. A safety switch substantially as hereinbefore described with reference to the accompanying drawings.
22. A method of operating a safety switch substantially as hereinbefore described with reference to the accompanying drawings.

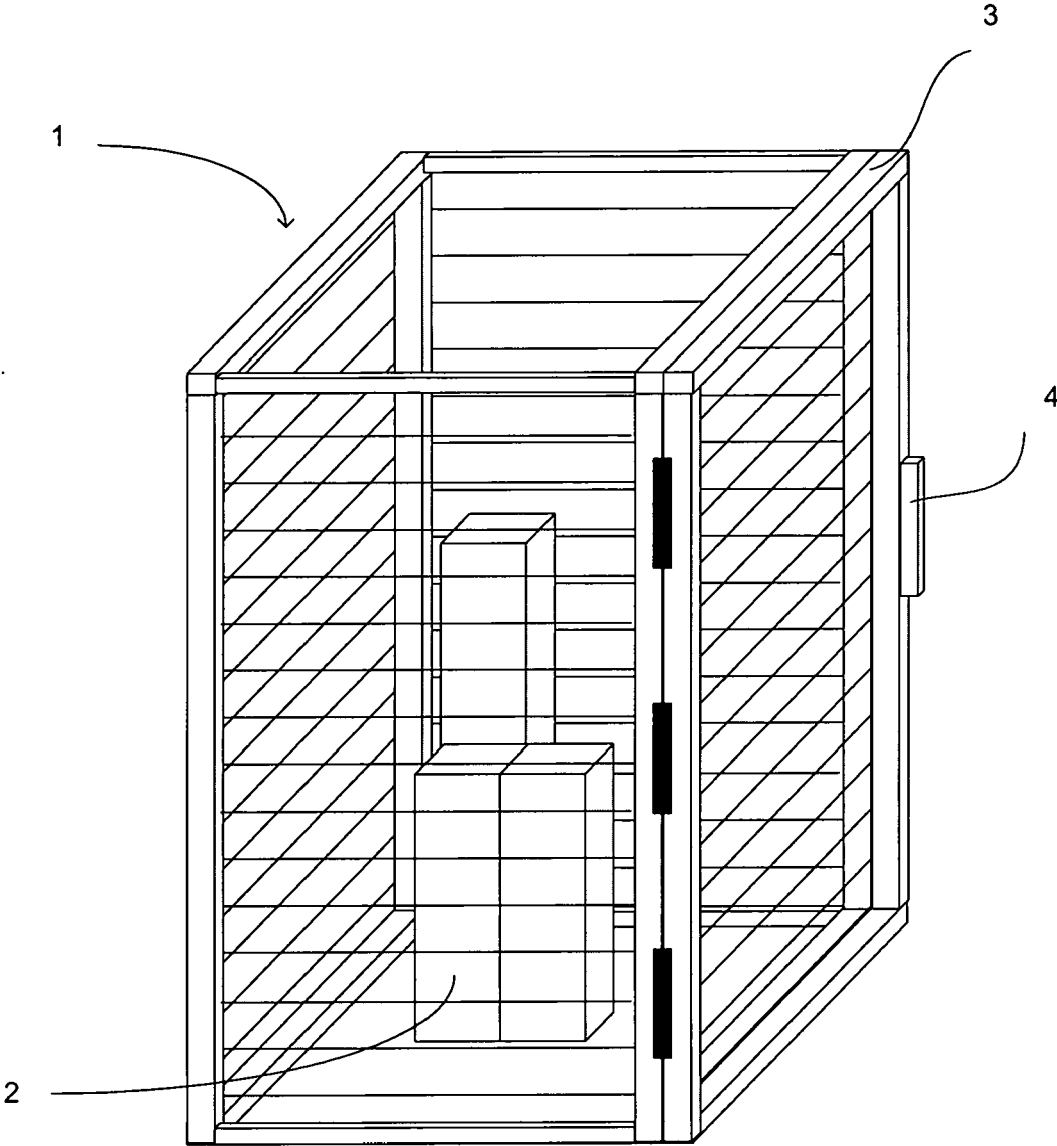


FIGURE 1a

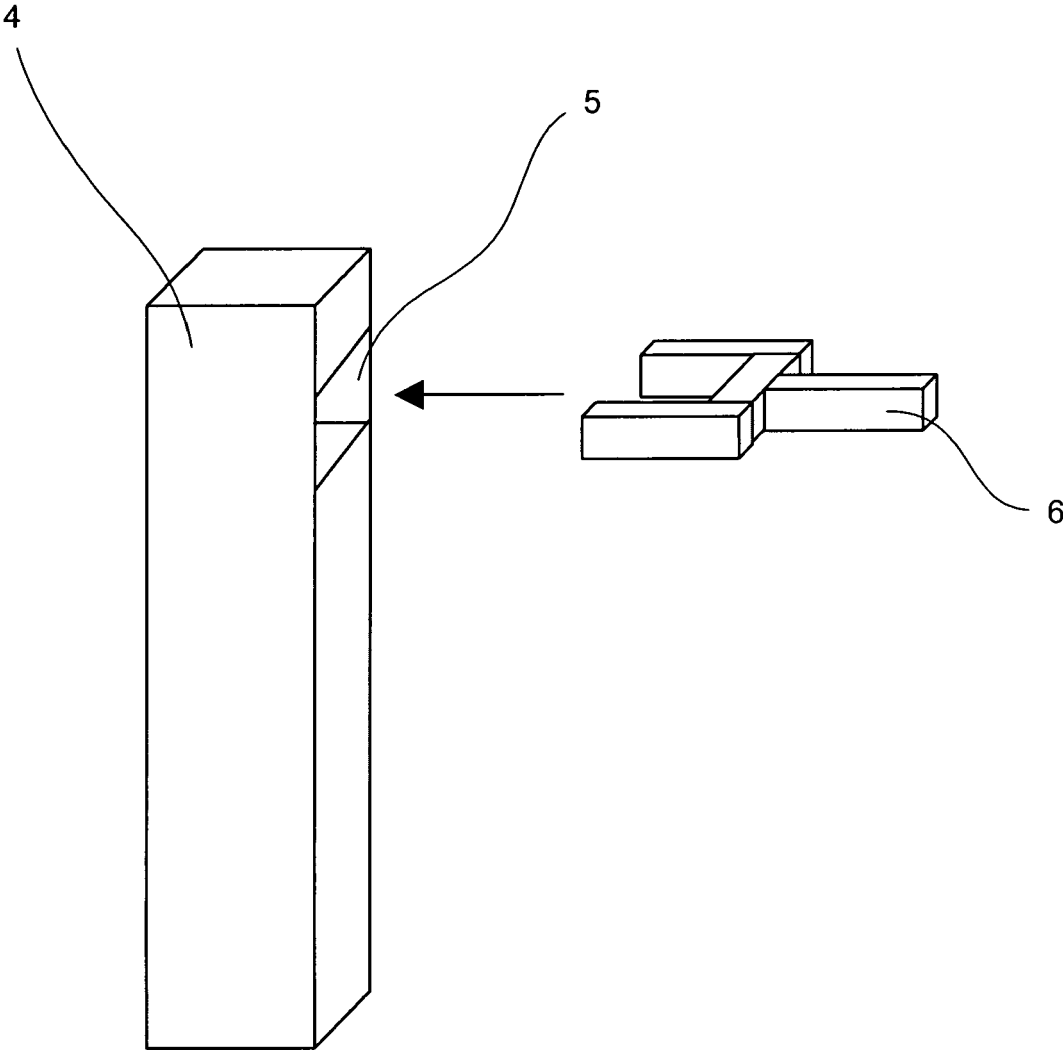


FIGURE 1b

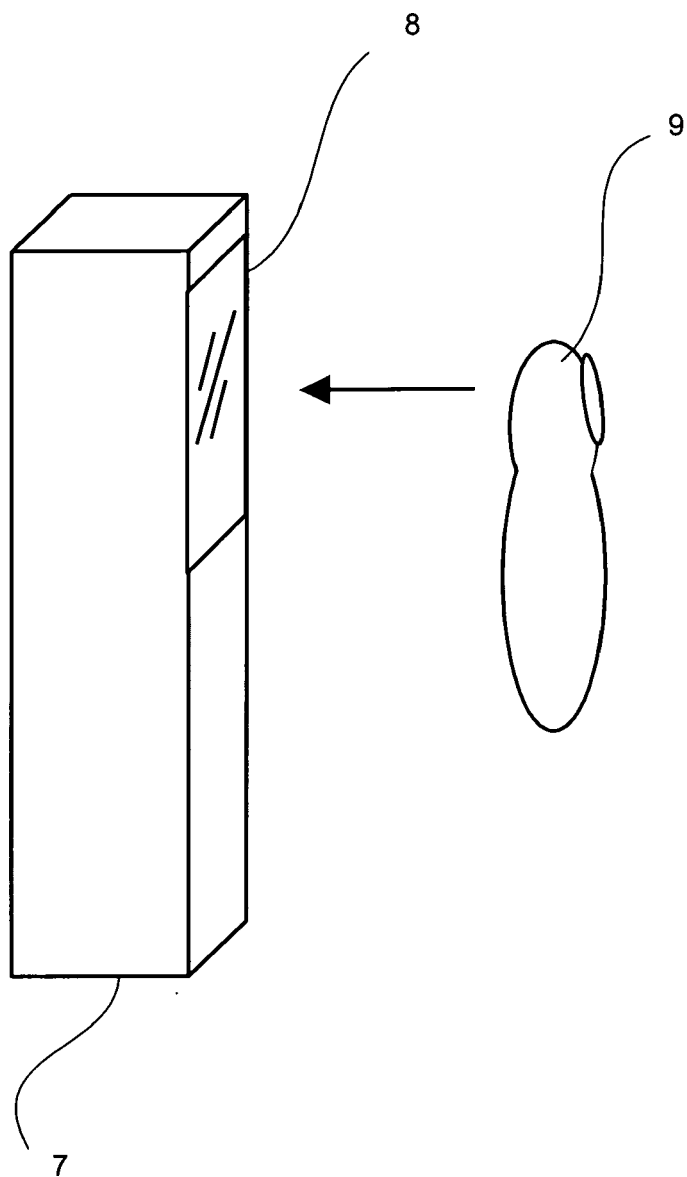


FIGURE 2

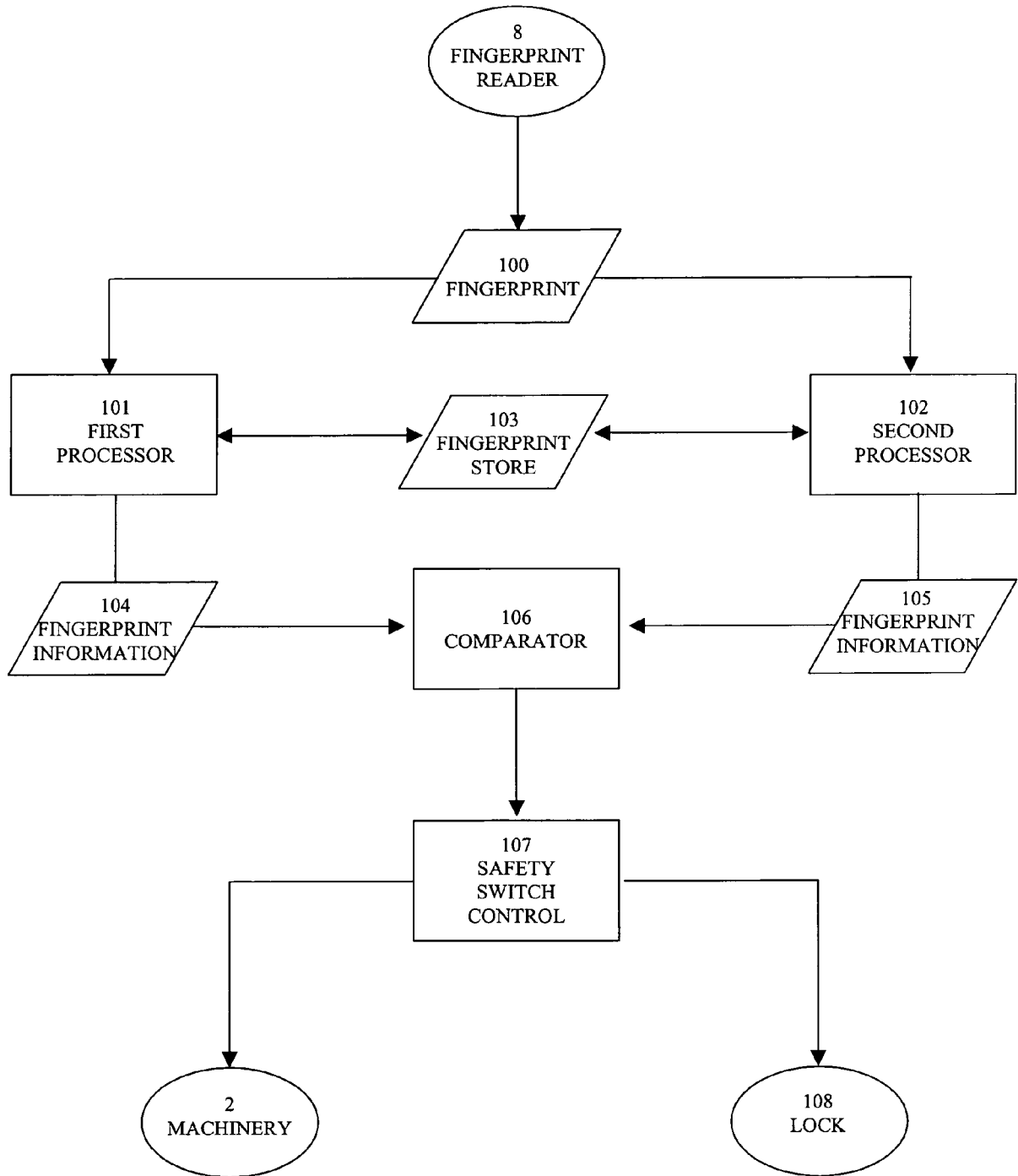


FIGURE 3a

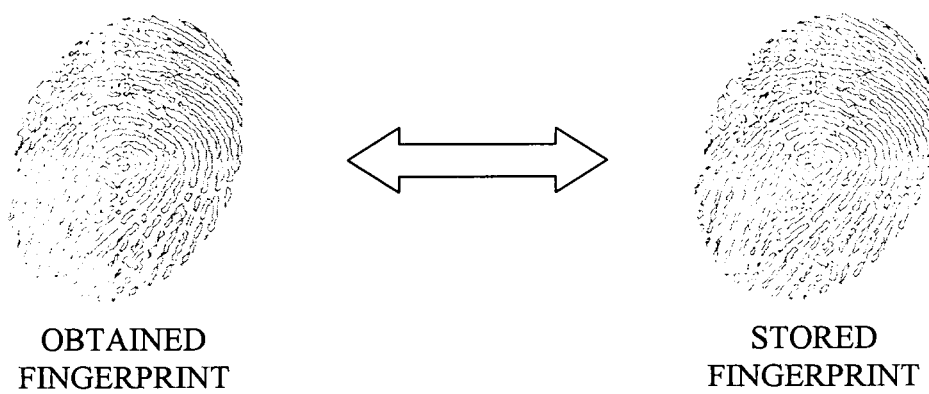


FIGURE 3b

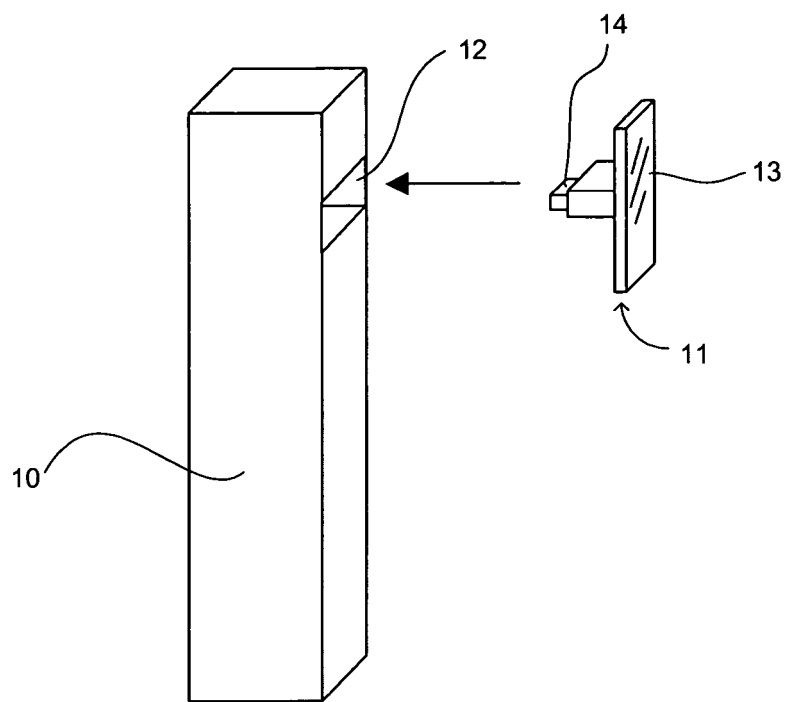


FIGURE 4a

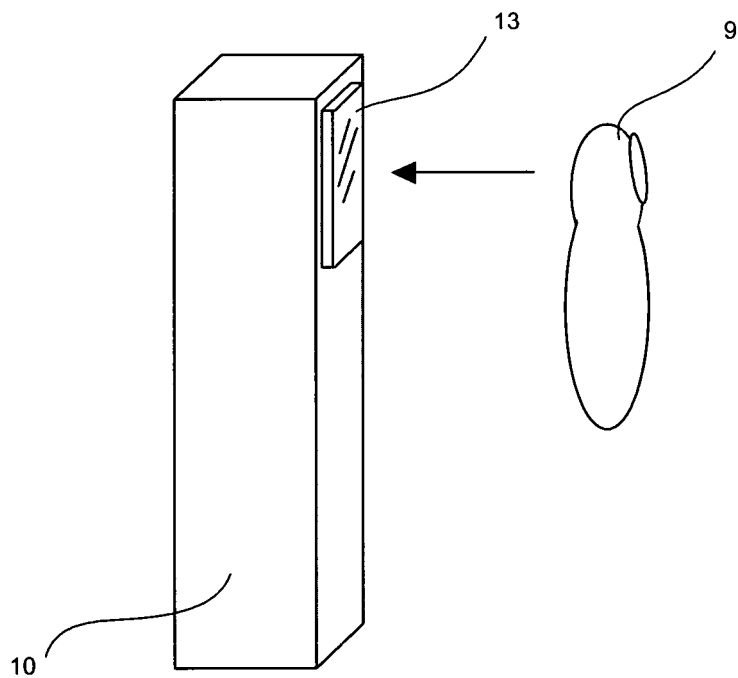


FIGURE 4b