(12) INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
23 November 2006 (23.11.2006)

PCT

(10) International Publication Number
WO 2006/123159 A2

(51) International Patent Classification:
*G07C 5/00* (2006.01) *B60R 25/04* (2006.01)

(21) International Application Number:
PCT/GB2006/001838

(22) International Filing Date: 18 May 2006 (18.05.2006)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
0510339.5 20 May 2005 (20.05.2005) GB

(71) Applicant *(for all designated States except US)*: **BALIUS SYSTEMS LIMITED** [GB/GB]; 13 Town Mill Road, Cowbridge, Vale of Glamorgan CF71 7BE (GB).

(72) Inventor; and
(75) Inventor/Applicant *(for US only)*: **STEELE, Francis, John** [GB/GB]; 13 Town Mill Road, Cowbridge, Vale of Glamorgan CF71 7BE (GB).

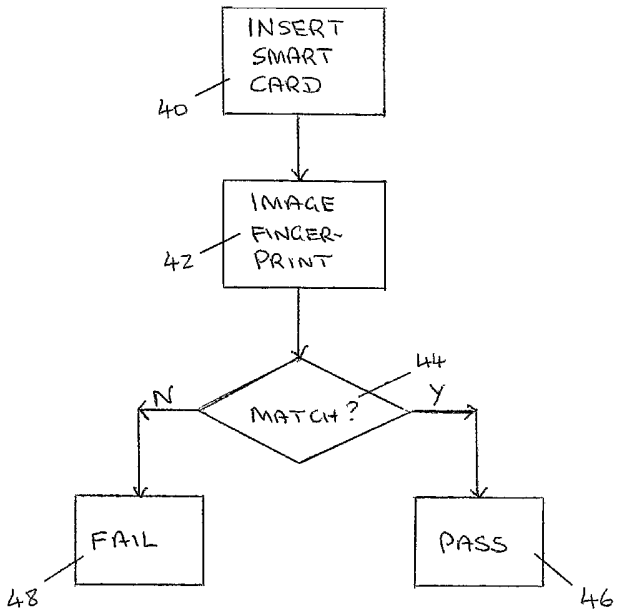
(81) Designated States *(unless otherwise indicated, for every kind of national protection available)*: AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BW, BY, BZ, CA, CH, CN, CO, CR, CU, CZ, DE, DK, DM, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KM, KN, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, LY, MA, MD, MG, MK, MN, MW, MX, MZ, NA, NG, NI, NO, NZ, OM, PG, PH, PL, PT, RO, RU, SC, SD, SE, SG, SK, SL, SM, SY, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, YU, ZA, ZM, ZW.

(84) Designated States *(unless otherwise indicated, for every kind of regional protection available)*: ARIPO (BW, GH, GM, KE, LS, MW, MZ, NA, SD, SL, SZ, TZ, UG, ZM, ZW), Eurasian (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European (AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HU, IE, IS, IT, LT, LU, LV, MC, NL, PL, PT, RO, SE, SI, SK, TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG).

**Published:**
— *without international search report and to be republished upon receipt of that report*

*For two-letter codes and other abbreviations, refer to the "Guidance Notes on Codes and Abbreviations" appearing at the beginning of each regular issue of the PCT Gazette.*

(54) **Title:** IMPROVED DIGITAL TACHOGRAPH




(57) **Abstract:** A digital tachograph is described having an interface arranged to read data stored on an electronic information carrier such as a smart card and a biometric sensor. The electronic information carrier stores biometric data of an authorised driver of a vehicle. The biometric sensor is adapted to obtain biometric data from a person requesting permission to drive the vehicle. The digital tachograph further comprises means for comparing the biometric data of the person requesting permission to drive the vehicle with the biometric data of said authorised driver to determine whether or not the person intending to drive the vehicle is the authorised driver.

WO 2006/123159 A2

# Improved Digital Tachograph

The present invention relates to digital tachographs.

A tachometer is a device that measures the revolutions per minute of a shaft: a tachograph is a device that records measurements made by a tachometer. The use of tachometers and tachographs is well established in the automotive industry, in particular for commercial vehicles, such as heavy goods vehicles, 3.5 tons light commercial vehicles and public service vehicles.

A number of analogue tachographs are available that can be used to record the usage of a vehicle. For example, known analogue tachographs can record the driving hours of a driver and the speeds and distances travelled. Typically, analogue tachographs record the user's period of duty on a waxed paper disc, or a tachograph chart.

Recently digital tachographs have been developed. A digital tachograph gathers information relating to the usage of the vehicle, such as driving hours, distance travelled, start times, finish times, rest times, driver name, starting location and finishing location and stores this data electronically.

Figure 1 is a block diagram showing the parts of an exemplary digital tachograph. As shown in Figure 1, the digital tachograph is indicated generally by the reference numeral 2 and comprises a speed sensor 4, a vehicle unit 6 and an electronic speedometer 8. The vehicle unit 6 contains a microprocessor and associated memory and receives

data relating to the current speed of the vehicle from the speed sensor 4. The vehicle unit 6 stores the data locally for later use and provides data relating to the current speed of the vehicle to the electronic speedometer 8 for display to the driver.

One intended purpose of the digital tachograph is to make it more difficult for an unscrupulous user to manipulate the data stored than is the case with known analogue tachographs.

It is known to control access to the digital tachograph via one or more smart cards. A smart card typically comprises an embedded microprocessor having a small amount of associated memory storing data, often security related data. Since smart cards usually include memory, it is possible to use the memory of the smart card to store data relating to the use of the vehicle and smart cards can therefore be used as a replacement for the tachograph chart typically used with analogue tachographs.

The inventor has identified a problem with the digital tachographs that are currently being proposed. Although many security issues have been addressed, the proposed systems make little or no attempt to verify the identity of the driver, in particular to ensure that the driver to whom a particular smart card has been issued is in fact the person driving the vehicle.

The present invention seeks to overcome or address one or more of the problems identified above.

The present invention provides a digital tachograph comprising an interface arranged to read data stored on an electronic information carrier, and a biometric sensor, wherein:

the electronic information carrier stores biometric data of an authorised driver of a vehicle;

the biometric sensor is adapted to obtain biometric data from a person requesting permission to drive the vehicle; and

the digital tachograph further comprises means for comparing the biometric data of the person requesting permission to drive the vehicle with the biometric data of said authorised driver to determine whether or not the person intending to drive the vehicle is the authorised driver.

The present invention also provides a method of determining whether a person requesting permission to drive a vehicle is an authorised driver, comprising the steps of:

obtaining biometric data of said authorised user from an electronic information carrier inserted into an interface of a tachograph;

obtaining biometric data of the person requesting permission to drive the vehicle using a biometric reader of said tachograph; and

comparing the biometric data obtained from said person using said biometric reader and said biometric data stored on said electronic information carrier to determine whether or not the person requesting permission to drive the vehicle is the authorised driver.

In one form of the invention, the electronic information carrier is a smart card. Other forms of electronic information carrier could be used, such as a SIM card or a flash memory device.

In one form of the invention, the biometric data is fingerprint data and the biometric sensor is a fingerprint sensor. Of course, other forms of biometric data could be used, such as hand print recognition and iris detection. Indeed, the present invention could be extended to be used with any biometric data. It is also noted that a combination of two or more forms of biometric data could be used. For example, a user could be required to identify themselves using both a fingerprint sensor and an iris scan.

Thus, the present invention provides a system in which a user can gain access to a vehicle using his information carrier, which may be in the form of a smart card. The system prevents unauthorised users from gaining access to that vehicle using that smart card by checking biometric data, such as fingerprint data, relating to the authorised user that is stored on the electronic information carrier. In other words, the system requires a user to identify him/herself and does not rely on the electronic information carrier as the sole form of identification.

The invention may include means for disabling the vehicle unless the person requesting permission to drive the vehicle is identified as the authorised driver. Thus, an unauthorised user would not be able to drive the vehicle. This would provide a significant security feature, making theft of a vehicle significantly more difficult.

The electronic information carrier may comprise biometric data relating to only one authorised driver. Thus, each individual user would have an electronic information carrier unique to them. Alternatively, of course, an electronic carrier could contain data relating to two or more authorised users, with a particular authorised user being identified by the biometric sensor. This might be more convenient if, for example, two drivers were authorised to drive a particular vehicle.

In one form of the invention, tachograph data is written to the electronic information carrier. In this form of the invention, the electronic information carrier must have sufficient memory to store the required amount of data. The memory size would, of course, be dependent on the quantity of data required to be stored. For example, a smart card might be issued to a driver and intended to store data relating one day of driving. This might be appropriate if the card were considered to be a backup to a main data store. Alternatively, the card could be intended to store a number of months or years worth of data, in which case the memory would have to be significantly larger. Such a requirement might be appropriate if the card were intended to be the primary store of data relating to a particular user. In one exemplary form of the invention, the smart card is a flash memory card and is arranged to store up to 28 days worth of data in normal use. After that time, the card simply over-writes existing data. The memory device could be an FRAM memory device.

The digital tachograph may further comprise means for receiving two electronic information carriers at any one time. This might be useful where there are two drivers of a vehicle, with one driver resting at any one time.

Embodiments of the invention will now be described with reference to the accompanying schematic drawings of which:

Figure 1 is a block diagram of a known digital tachograph;

Figure 2 is a block diagram of a digital tachograph in accordance with an embodiment of the present invention;

Figure 3 is a schematic cross-section of a capacitive fingerprint sensor; and

Figure 4 is a flow chart demonstrating an algorithm for using the digital tachograph of Figure 2.

Figure 2 shows a digital tachograph, indicated generally by the reference numeral 10, comprising a vehicle unit 12, a speed sensor 14, a fingerprint sensor 16, a smart card interface 18 and a display 20. In a similar manner to the known system described with reference to Figure 1, the vehicle unit 12 of the digital tachograph 10 receives data relating to the current speed of the vehicle from the speed sensor 14 and provides data relating to the current speed of the vehicle to the display 20 for display to the driver.

The vehicle unit 12 also receives data from the fingerprint sensor 16 and the smart card interface 18. The smart card interface reads data stored on a smart card relating to the fingerprint data of a person authorised to drive the vehicle in which the tachograph 10 is installed. As is described

below, the fingerprint sensor 16 is used to obtain fingerprint data of the person intending to drive the vehicle in which the tachograph 10 is installed and the vehicle unit 12 determines whether or not the measured fingerprint data matches the data stored on the smart card inserted into the smart card interface 18. A driver is only allowed to drive the vehicle if such a match is determined.

There are at least two established methods for obtaining fingerprint data. The first involves optical scanning of a finger using a CCD device. The second involves capacitive scanning of a finger. Both methods are well known to persons skilled in the art. Therefore, although an exemplary capacitive scanning scheme is described briefly below, neither capacitive scanning nor optical scanning are described in detail.

In one embodiment of the present invention, the fingerprint sensor 16 is an MBF200 capacitive scanning device available from Fujitsu Microelectronics. The capacitive scanning device includes a 2-D array of capacitive plates of the form shown in Figure 3.

Figure 3 shows a fingerprint sensor, indicated generally by the reference numeral 16, and a portion of a finger 22, in contact with the top portion of the sensor 16. The fingerprint sensor 16 of Figure 3 includes a 2-dimensional array of capacitor plates. Three capacitor plates 30a, 30b and 30c are shown in Figure 3 (of course, a real fingerprint sensor includes a large number of such capacitive plates). The fingerprint sensor includes a dielectric portion 32 located between the capacitive plates and the finger 22, an

active portion 34 in which the capacitive plates are fabricated, and a substrate 36.

A fingerprint is derived from ridges and valleys in a person's finger. For example, the portion of the finger 22 shown in Figure 3 includes ridges 24 and 26 and valley 28. The ridges and valleys of a finger placed against the scanning device (such as ridges 24 and 26 and valley 28) make up the second plate of a capacitor, with the dielectric portion 32 of the fingerprint sensor 16 forming the dielectric of the capacitor. As shown in Figure 3, a ridge of a finger will be closer to a capacitor plate of the scanning device than a valley. Accordingly, the capacitance will vary across the scanning device when a finger is pressed against the scanning device and this varying capacitance can be used to obtain an image of the ridges and valleys of the finger 22, i.e. an image of the fingerprint of the finger 22.

Some ridges of a person's fingerprint terminate at so-called "ending points" and some ridges divide at so-called "bifurcation points". The location of ending points and bifurcation points (collectively termed "minutia") are unique to an individual. The uniqueness of a fingerprint is a result of the uniqueness of the minutiae.

It is relatively easy to determine the presence and location of the minutia of a person's finger from an image generated by a sensor such as the capacitive fingerprint sensor 16 described with reference to Figure 3. Further, software is readily available to determine relationships between the

positioned of the minutia and data relating to these relationships can be stored as "fingerprint data".

In order to determine whether or not a person's fingerprint matches known fingerprint data, an image is taken of the person's fingerprint, for example using a capacitive sensor of the form described above with reference to Figure 3. The minutiae of the fingerprint are extracted from the image and a template of the image derived from the relationships between the minutiae. The template is compared with a reference template derived from the relationship between the minutia of the known fingerprint and a match is determined if the two templates are the same within a predetermined tolerance.

The functionality of the security system of the digital tachograph of the present invention will now be described with reference to the block diagram of Figure 2 and the flow chart of Figure 4.

When a person wishes to drive the vehicle in which the tachograph of the present invention is used, he must use insert his smart card into the smart card interface 18, as indicated at step 40 of Figure 4.

The smart card is individual to the particular driver and is used to store data relating to the driver's details, including his fingerprint data, and is also used to store tachograph data relevant to that driver.

Once the user has inserted his smart card, he must use the fingerprint sensor 16 (which may be the MBF200 capacitive

scanning device described above) in order to allow the system to generate an image of his fingerprint (step 42 of Figure 4). The measured fingerprint data is compared with the data stored on his smart card (step 44) and, if there is a match, a "pass" output is obtained (step 46) and he is able to drive the vehicle. If there is no match, a "fail" output is obtained (step 48) and the vehicle is prevented from being operated.

In this way, a driver is prevented from using a vehicle using another driver's smart card, since his fingerprint data will not match the fingerprint data stored on that card.

A single embodiment of the present invention has been described above. It should be noted, of course, that there are a number of possible variants of the present invention. For example, the capacitive fingerprint sensor could be replaced with any other form of suitable fingerprint sensor (such as an optical fingerprint sensor). Further, a number of variants of the algorithm of Figure 4 will be readily apparent to persons skilled in the art.

The invention has been described with reference to a fingerprint sensor, however fingerprint data is just one of many forms of biometric data. Other biometric data could be used instead of, or in addition to, fingerprint data. For example, hand print data and/or iris data could be used. Of course, suitable sensors to obtain the relevant biometric data would need to be provided.

It should also be noted that whilst the present invention has generally been described with reference to commercial vehicles, such as heavy goods vehicles, the invention is applicable to any vehicle, including aircraft, heavy good vehicles, commercial vehicles, cars, motorbikes and scooters.

Further, whilst the invention has been described with reference to a single driver, the invention is also applicable to vehicles where there are two drivers. For example, a heavy goods vehicle may have two drivers, with one driver resting at any one time. A digital tachograph may be provided with two slots, with each driver inserting an electronic information carrier unique to that driver into a slot of the tachograph. Such a system may require each driver to uniquely identify themselves, e.g. using a fingerprint sensor, each time that the vehicle is used. Thus, when the drivers changeover, the new driver is required to identify him/herself in the same way that the other driver had to. In this way, data relating to a particular driver's use of the vehicle would only be stored on that driver's electronic information carrier.

Claims:

1. A digital tachograph comprising an interface arranged to read data stored on an electronic information carrier, and a biometric sensor, wherein:

the electronic information carrier stores biometric data of an authorised driver of a vehicle;

the biometric sensor is adapted to obtain biometric data from a person requesting permission to drive the vehicle; and

the digital tachograph further comprises means for comparing the biometric data of the person requesting permission to drive the vehicle with the biometric data of said authorised driver to determine whether or not the person intending to drive the vehicle is the authorised driver.

2. A digital tachograph as claimed in claim 1, further comprising means for disabling the vehicle unless the person requesting permission to drive the vehicle is identified as the authorised driver.

3. A digital tachograph as claimed in claim 1 or claim 2, wherein said electronic information carrier is a smart card.

4. A digital tachograph as claimed in any one of claims 1 to 3, wherein the electronic information carrier comprises biometric data relating to only one authorised driver.

5. A digital tachograph as claimed in any preceding claim, wherein, in use, tachograph data is written to the electronic information carrier.

6. A digital tachograph as claimed in any preceding claim, wherein said biometric data is fingerprint data and said biometric sensor is a fingerprint sensor.

7. A digital tachograph as claimed in any preceding claim, comprising means for receiving two electronic information carriers at any one time.

8. A method of determining whether a person requesting permission to drive a vehicle is an authorised driver, comprising the steps of:

obtaining biometric data of said authorised user from an electronic information carrier inserted into an interface of a tachograph;

obtaining biometric data of the person requesting permission to drive the vehicle using a biometric reader of said tachograph; and

comparing the biometric data obtained from said person using said biometric reader and said biometric data stored on said electronic information carrier to determine whether or not the person requesting permission to drive the vehicle is the authorised driver.

9. A method as claimed in claim 8, further comprising the step of disabling the vehicle unless the person requesting permission to drive the vehicle is identified as the authorised driver.

10. A method as claimed in claim 8 or claim 9, wherein said biometric data is fingerprint data and said biometric reader is a fingerprint reader.

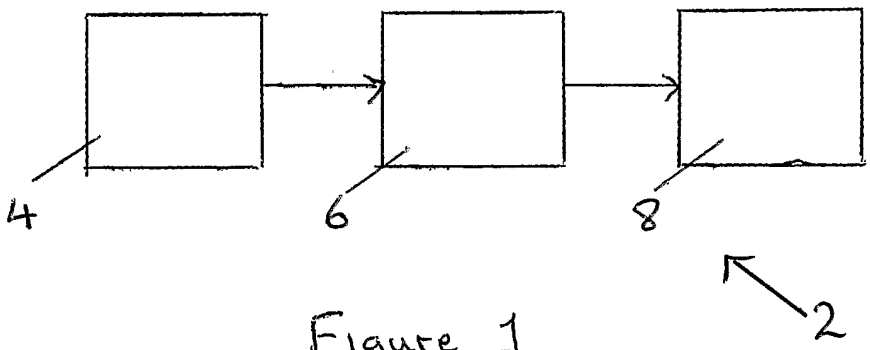



Figure 1

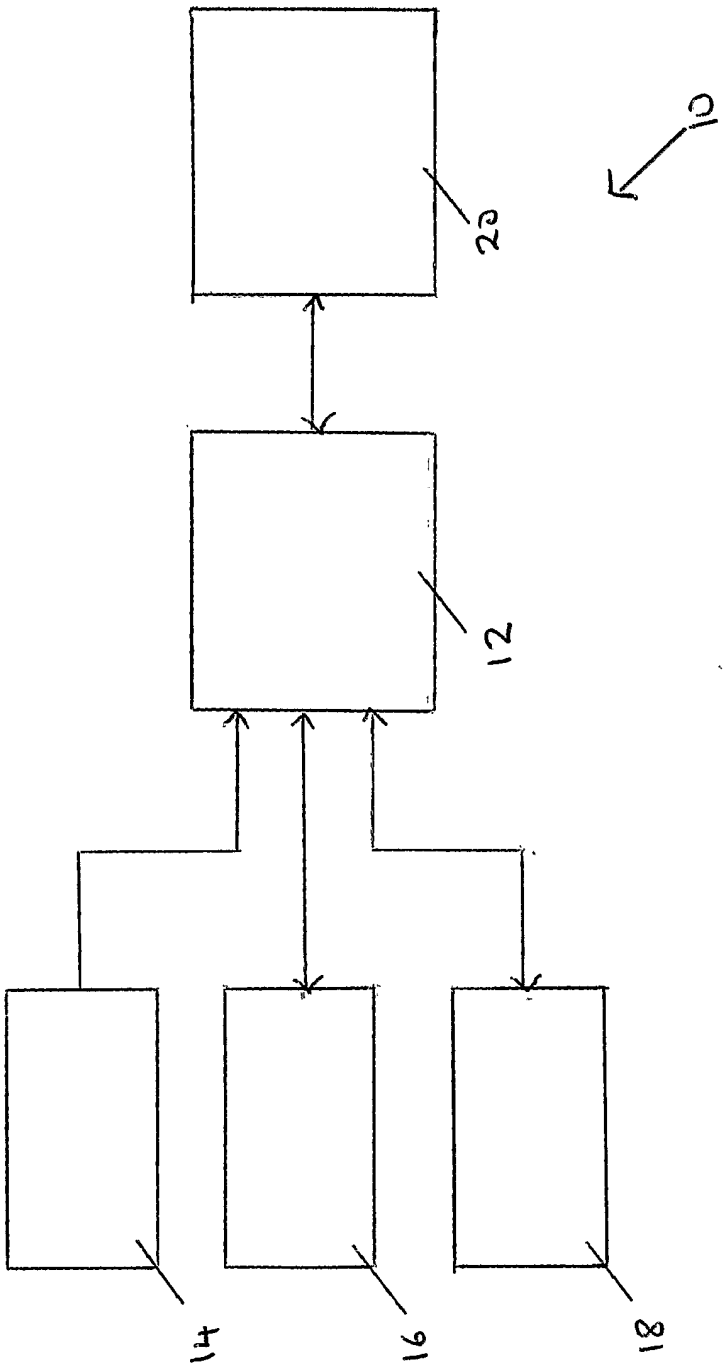



Figure 2

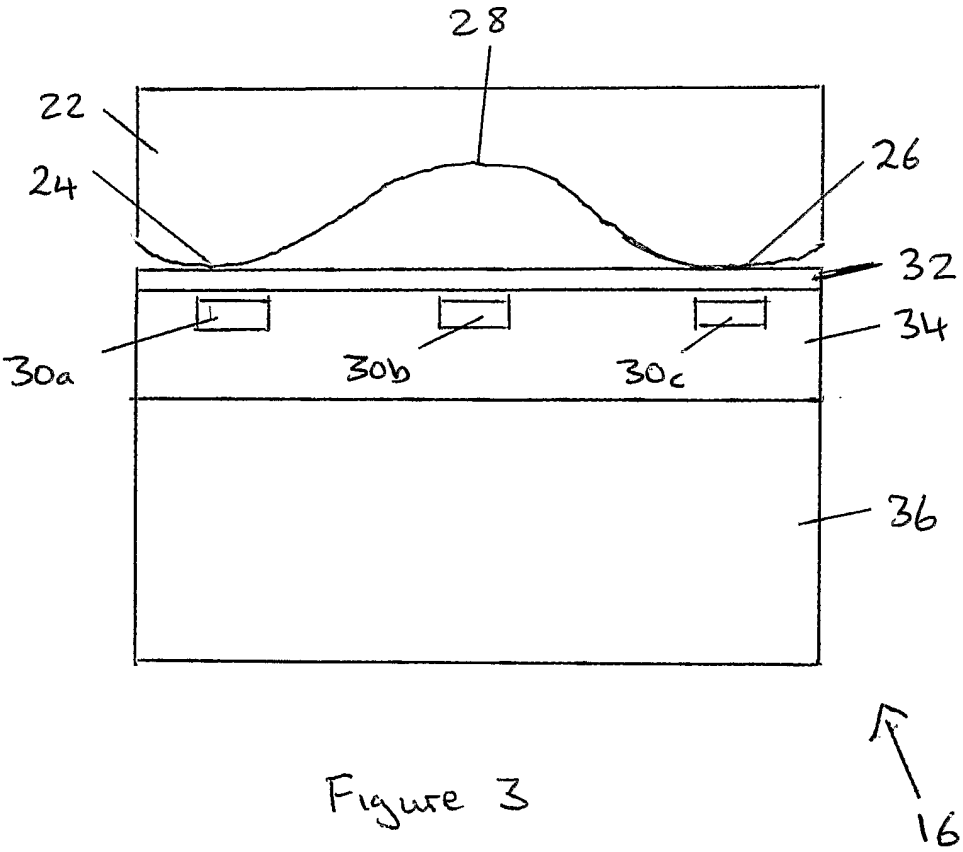



Figure 3

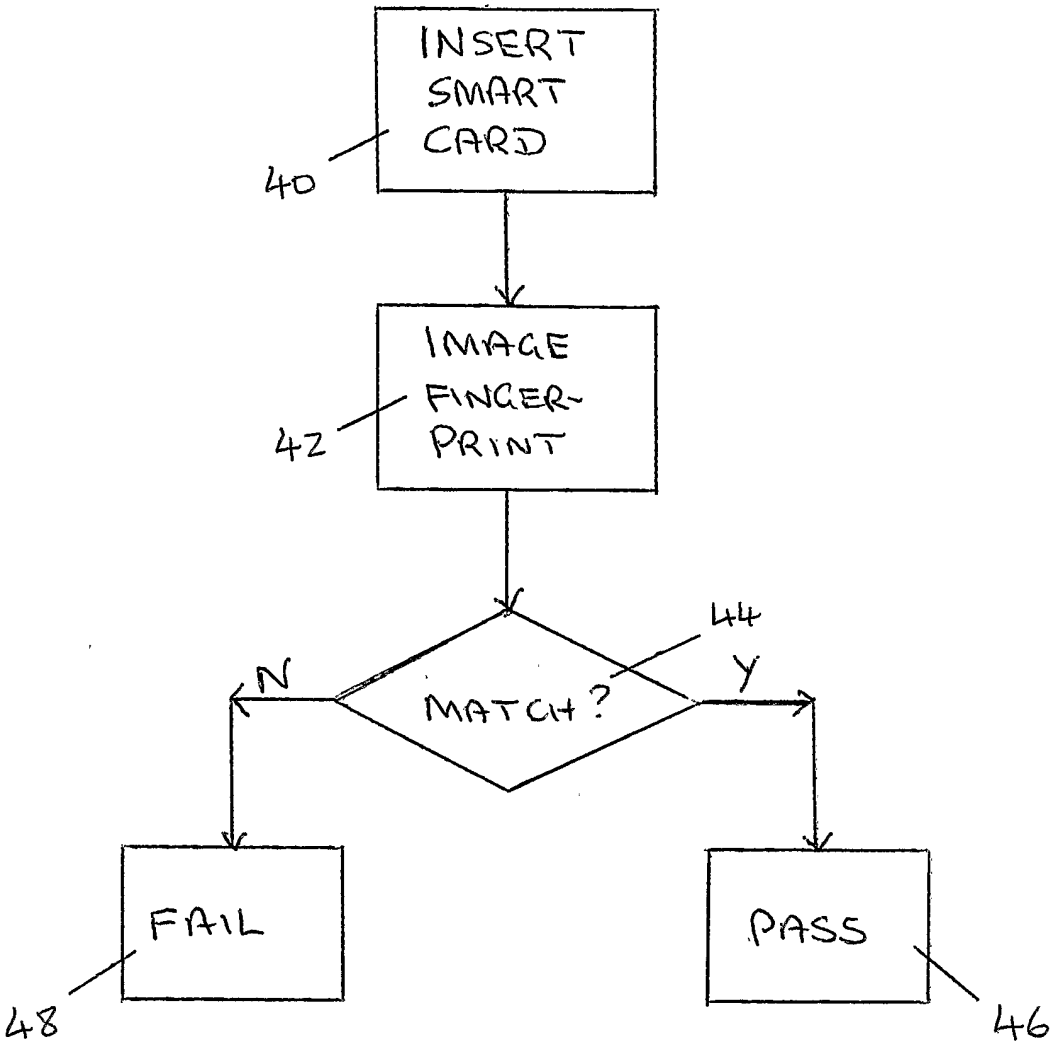

INSERT SMART CARD
40
IMAGE FINGER-PRINT
42
MATCH ?
44
N
Y
FAIL
48
PASS
46

Figure 4