

ANTI-FRAUD CARD READER MODULE

The present invention relates to a card reader module, particularly a motorised card reader module, for resisting fraud. The invention is particularly related to preventing fraud at a self-service terminal (SST), such as an ATM (automated teller machine), a point of sale (PoS) terminal, or any other terminal using a motorised card reader module.

ATMs typically store large amounts of cash. This makes them vulnerable to attack by thieves. To combat physical attack, ATMs include a safe for storing the cash. However, ATMs are also vulnerable to attack by fraud.

One type of fraud involves a third party placing a loop of thin, strong, material over a card entry slot in the ATM. The material is so thin that it may not be noticed by an unwary user of the ATM. The material is designed so that:

(1) it prevents a user's card from fully entering a motorised card reader module located behind the card entry slot, and

(2) it prevents the entered user's card from being ejected from the motorised card reader module.

Thus, the design of this material causes an entered card to jam in the module so that the module cannot draw in or eject the card. When this happens, the user generally assumes that the ATM has gone out of service and goes away from the ATM, leaving his/her card jammed in the card reader module.

The third party can then extract the card from the card reader module, remove the thin material, and (if the third

party has observed or otherwise obtained the user's PIN) use the card to withdraw cash from the ATM.

It is an object of an embodiment of the present invention to reduce the possibility of this type of fraud.

According to a first aspect of the invention there is provided a motorised card reader module characterised in that the module includes a trap mechanism operable to trap a card within the card reader module in response to the card reader module detecting a card within the module that cannot be transported.

By virtue of this aspect of the invention when a card is stuck within the module the module is able to trap the card therein, thereby preventing a third party or the authorised card holder from removing the card from the module. This safeguards the card without damaging it in any way.

The card reader module may be able to read data from and write data to a card (that is, it may be a card read/write module), or it may only be able to read data from a card.

Preferably, the trap mechanism is implemented by a width switch and an associated interlock, where the width switch is located within a throat portion of the card reader module and has an arm that is deflected by insertion of a card.

Conventional card reader modules use a width switch to ensure that a shutter within the module is only opened when a card of correct width is inserted, the width of the card being determined by deflection of the width switch. In a

-3-

preferred embodiment, the width switch is locked in a non-deflected position when a card is to be trapped within the module. This has two advantages.

(i) any tampering with the switch (e.g. jamming it in the deflected position) to overcome this security measure will be evident to the card reader as the switch must move normally (from the open to the closed position) during a transaction.

(ii) a conventional card reader module only requires slight modification for use in the present invention.

By locking the width switch, the throat portion becomes too narrow for a card to be removed therethrough.

The trap mechanism may be activated using software and/or firmware and/or hardware control.

Preferably, the card reader module is operable, on detecting that the trap mechanism cannot trap an entered card, to activate a magnetic head located in a throat portion of the card reader module to erase data stored on a magnetic stripe on the entered card. This has the advantage that if the trap mechanism is unable to trap an entered card because part of the card is still in contact with the trap mechanism, then a magnetic head may be used to erase the data on the card so that the card is much less valuable to a fraudulent third party.

According to a second aspect of the present invention there is provided a self-service terminal comprising a fascia defining a card entry slot, and a card reader module located behind the card entry slot, characterised in that the module includes a trap mechanism operable to trap a card

-4-

within the card reader module in response to the card reader module detecting a card within the module that cannot be transported.

The terminal may be an ATM.

According to a third aspect of the invention there is provided a motorised card reader module including a shutter and a width switch, characterised in that the width switch is operable to trap a card within the card reader module in response to the card reader module detecting a card within the module that cannot be transported.

The module may include a throat portion having a magnetic read/write head located so that only items of the correct width (as determined by the width switch) and having magnetic data (detected by the magnetic read/write head) are recognised as magnetic cards.

The module may be operable, on detecting that the width switch cannot trap a card within the module, to activate the read/write head to erase any data stored on a magnetic stripe in a card located in the vicinity of the width switch.

The module may activate an alarm on detecting a card within the module that cannot be transported. This alarm may be audible or visual, and may be relayed automatically to an appropriate person, for example to a person authorised to service the terminal.

The card reader module may use sensors to detect that a card cannot be transported (that is, having jammed). The event of a card having jammed may be indicated by any convenient technique. For example, where a first sensor

-5-

detects the presence of a card and a second sensor does not detect the presence of the card a predetermined time after the first sensor detected the presence of the card. Another example is where a sensor continuously detects the presence of a card for a predetermined time interval. A further example is where a sensor detects the presence of a card for a predetermined time during attempted transportation of the card in a forward direction and the same sensor detects the presence of the card for a predetermined time during attempted transportation of the card in a reverse direction. Any one or any combination of these techniques may be used to detect that a card cannot be transported.

According to a fourth aspect of the present invention there is provided a method of preventing fraud, the method comprising the steps of: providing a trap mechanism for trapping a card within a card reader module; detecting entry of a card into the card reader module; monitoring transport of the card within the card reader module; and, in response to detection of a failure of the card reader module to transport the card correctly, activating the trap mechanism to trap the card.

The method may include the further step of displaying on a monitor a message informing the user about the capture of his/her card.

The method may include the steps of detecting continued activation of a first sensor but not detecting activation of a second sensor within a predetermined time. The first sensor may be a width sensor (width switch) for sensing the width of the card, and/or a magnetic stripe detecting sensor for detecting the correct orientation of a card. The

magnetic stripe detecting sensor may be a magnetic read/write head.

The second sensor may be a read head sensor located in the vicinity of a magnetic card reading head within the card reader module.

The method may include the step of: on detecting that the trap mechanism is unable to trap the card, activating a read/write head for erasing any data stored on the card. The trap mechanism may be unable to trap the card if the card jams while maintaining the width switch in a deflected position.

According to a fifth aspect of the present invention there is provided a method of preventing fraud, the method comprising the steps of: providing a magnetic head for erasing data stored on a magnetic stripe carried by a card; detecting entry of a card into the card reader module; monitoring transport of the card within the card reader module; and, in response to detection of a failure of the card reader module to transport the card correctly, activating the magnetic head to erase any data stored on the stripe on the card.

According to a sixth aspect of the present invention there is provided a motorised card reader module characterised in that the module includes a magnetic head operable to erase data stored by a magnetic stripe on a card in response to the card reader module detecting a card within the module that cannot be transported.

Preferably, the magnetic head is located in a throat portion of the module.

The magnetic head may be an erase coil or a magnetic read/write head.

The module may erase data by passing an erase current through the magnetic head.

These and other aspects of the invention will be apparent from the following specific description, given by way of example, with reference to the accompanying drawings, in which:

Fig 1 is a schematic front view of a motorised card reader module according to an embodiment of the present invention;

Fig 2 is a schematic side view of the module of Fig 1;

Fig 3 is a schematic plan view of a card at a first position in the module of Figs 1 and 2;

Fig 4 is a schematic plan view of a card at a second position in the module of Figs 1 and 2;

Fig 5 is a schematic plan view of a card at a third position in the module of Figs 1 and 2;

Fig 6 is a schematic plan view of a card at a fourth position in the module of Figs 1 and 2; and

Fig 7 is a perspective view of a self-service terminal according to another embodiment of the present invention.

Reference is now made to Figs 1 and 2, which are front and side schematic views respectively of a motorised card reader/writer (MCRW) module 10.

The module 10 is a modified version of a conventional MCRW module made by Sankyo (trade mark) and available from

Sankyo at 1-17-2, SHINBASHI, MINATO-KU, TOKYO, 1058633, Japan.

Module 10 comprises a housing 12 coupled to a throat portion 14 and is suitable for reading a standard size magnetic stripe card.

The throat portion 14 defines a slot 16 into which a magnetic stripe card may be inserted, and includes a shutter 18 pivotally coupled to the housing 12. With the shutter 18 in the open position, a card may be conveyed between the housing 12 and the throat portion 14; whereas, with the shutter 18 in the closed position no card may pass between the throat portion 14 and the housing 12. When the leading edge of a card passes the shutter 18, the shutter 18 is biased against the top of the card so that the shutter 18 automatically closes once the trailing edge of the card clears the shutter 18.

The throat portion 14 includes a trap mechanism 20 comprising a card width switch 22 and an interlock 24. The card width switch 22 has an elongated arm 26 that is pivotally mounted to the throat portion 14. The interlock 24 is in the form of a solenoid and pin arrangement, whereby when the pin protrudes from the solenoid it locks the switch 22 and prevents the arm 26 from pivoting.

The switch's arm 26 is deflected by a card on insertion and ejection of the card. Switch 22 detects when the arm 26 has been deflected by a card and when the arm 26 is in the undeflected position.

If a user inserts a conventional magnetic stripe card into the throat portion 14 then the arm 26 is deflected and

-9-

switch 22 detects the deflection of the arm 26, which indicates the presence of the card.

The housing 12 includes a shutter detect sensor 27 for detecting whether the shutter 18 is in an open or closed position.

The throat portion 14 also includes a magnetic head in the form of a read/write head 28. Magnetic head 28 is used to detect that a magnetic stripe is present on a card being inserted. If no magnetic stripe is detected then the shutter 18 will not be opened, even if the arm 26 is deflected. Thus, shutter 18 will only be opened if a card is entered that has

- (1) the correct width (as detected by switch 22), and
- (2) a magnetic stripe in the correct location (as detected by read/write head 28).

Thus, if a magnetic stripe card is inserted in a wrong orientation the shutter 18 will not open.

Referring particularly to Fig 2, the housing 12 also includes a linear transport mechanism, shown generally by arrow 30, comprising four pairs of rollers 32,34,36,38 and associated stretchable endless toothed belts (not shown) for transporting a card when it is within the housing 12.

The housing 12 defines an entrance/exit slot 40 at one end and a card retention/capture slot 42 at the opposite end. When a card is inserted by a user, the first pair of rollers 32 pinch the leading edge of the card and draw the card into the housing 12. When the trailing edge of the card clears the shutter 18, the shutter 18 closes thereby

-10-

capturing the card within the housing 12, and the card reading operation begins.

The housing 12 includes four sensors for accurately locating the position of the card within the housing 12.

A card present sensor 44 is located in the vicinity of the throat portion 14 at the first pair of rollers 32. The sensor 44 is in the form of an optical sensor for detecting the presence of a card inserted into the housing 12.

A card eject sensor 46 is located a predetermined distance from the throat portion 14 to ensure that on ejection of a card the card protrudes from the throat portion 14 by a sufficient distance to allow a user to grip and remove the card.

A card detect sensor 48 is located at the second pair of rollers 34 in the vicinity of a card read/write head 50 so that when the leading edge of a card is detected, the magnetic stripe on the card may be read by the card read head 50.

A card stop sensor 52 is located distal from the throat portion 14 at the third pair of rollers 36. The card stop sensor 52 is spaced from the card read sensor 48 by a distance less than the length of a standard card, so that when the card stop sensor 52 detects the leading edge of a card, the card is still in contact with the card read sensor 48.

The card is only transported beyond the card stop sensor 52 if the card is to be conveyed out of the retention slot 42 and retained by the card reader module 10. Where the module 10 is used in an ATM, this may occur because a

-11-

user has inserted the wrong PIN on a predetermined number of occasions, or because the card is registered as stolen.

The four sensors 44,46,48,52 are located so that once a card enters the housing 12 it can always be located by at least one of the sensors 44,46,48,52, unless the card is conveyed out of the retention slot 42.

Fig 3 shows a card 60 having a magnetic stripe 62, the card being located at the entrance of the throat portion 14 of the module 10. In Fig 3 the arm 26 is in the undeflected position and the shutter 18 is closed.

Fig 4 shows the card 60 partially within the housing 12. The shutter 18 is open and resting on the card 60, so sensor 27 detects the open shutter 18. The arm 26 is in the deflected position, so switch 22 detects the deflected arm 26. Read/write head 28 is in contact with the magnetic stripe 62, so head 28 detects magnetic data on the stripe 62.

Fig 5 shows the card 60 having cleared switch 22. The card 60 has been jammed within the module 10 by a loop of material (not shown) so that the card cannot be transported by the module 10.

The shutter 18 is still open and resting on the card 60, so sensor 27 still detects the open shutter 18. The arm 26 has returned to the undeflected position, so switch 22 detects that the arm 26 is undeflected. Read/write head 28 is not in contact with the magnetic stripe 62, so head 28 does not detect magnetic data. As a large portion of the card 60 is inside the housing 12, sensor 44 and eject sensor 46 detect the presence of the card 60. However, the card 60

-12-

is not in contact with the card read sensor 48, so sensor 48 does not detect the card 60.

After a predetermined length of time between sensor 44 detecting the presence of a card and sensor 48 not detecting the card 60, for example ten seconds, the module 10 attempts to eject the card; however, the material (not shown) stops ejection of the card. Thus the module 10 can neither capture nor eject the card 60.

After another predetermined time during which the module 10 attempts to transport the card 60 (for example, 20 seconds) and in which sensor 44 continues detecting the presence of the card 60 but sensor 48 does not detect the presence of the card 60, the module 10 activates the interlock 24 to lock the arm 26 and prevent the card 60 from being removed.

Fig 6 shows the card 60 still in contact with the arm 26. The card 60 has been jammed within the module 10 by a loop of material (not shown) so that the card 60 cannot be transported by the module 10. However, as the card 60 is still in contact with the arm 26, the interlock 24 cannot be activated. Thus, when the module 10 detects that the card 60 cannot be transported and that the interlock 24 cannot be activated, ATM software activates (sends an erase current to) the read/write head 28 to delete the data stored on the magnetic stripe 62. This ensures that if the card 60 is retrieved by a fraudulent third party, sufficient magnetic data has been erased so that card 60 cannot be used in motorised or swipe card reader modules. The read/write head 28 may be activated (continuously or intermittently) until the card 60 is removed so that most of (or all) the data on

-13-

the magnetic stripe 62 is erased when the card 60 is removed from the module 10.

Fig 7 is a perspective view of an SST 70, in the form of an ATM, including the module of Figs 1 to 6. The ATM 70 comprises a chassis (not shown) for supporting a fascia 72, exterior panels 74 and internal ATM modules (not shown). The fascia 72 incorporates a user interface 76. The fascia 72 defines a plurality of slots so that when the fascia 72 engages fully with the chassis and panels 74 the slots align with user interface elements located within the ATM 70.

The user interface 76 comprises a display 78, a cash dispense slot 80, a card entry/exit slot 82 (herein referred to as a card entry slot), a receipt slot 84, and an encrypting keypad 86.

The fascia 72 has a lock mechanism 88 for securing the fascia 72 to and for releasing the fascia 72 from the chassis and panels 74.

Referring to Figs 1 to 7, in the event of a fraudulent third party placing a length of thin, strong, material (not shown) over the ATM card entry slot 82, the operation of the ATM 70 would be as follows.

An unwary user may approach the ATM 70 and insert his card into ATM card entry slot 82. The card enters throat slot 16; deflects arm 26, thereby opening the shutter 18; enters the housing 12; is pinched by first rollers 32; and is drawn into housing 12. However, as the card is being drawn into housing 12 the material (not shown) stops the card from fully entering the housing 12. At this position part of the card is still underneath the shutter 18 so that

-14-

the shutter 18 cannot close. Sensor 44 detects the presence of the card, but sensor 48 does not detect the presence of a card. After a predetermined length of time, for example ten seconds, the module 10 attempts to eject the card; however, the material (not shown) stops ejection of the card. Thus the module 10 can neither draw in nor eject the card.

After another predetermined time (for example, 20 seconds) during which the module 10 attempts to eject the card, if sensor 44 continues to detect the presence of a card but sensor 48 does not detect the presence of a card, the module 10 then determines via switch 22 whether the arm 26 is deflected or undeflected.

(1) If the arm 26 is undeflected then the module 10 activates the interlock 24 to prevent removal of the card.

(2) If the arm 26 is deflected then the module 10 activates the read/write head 28 to erase any magnetic data stored on the magnetic stripe on the card.

In the event of condition (1) above, the ATM 70 displays a message on the display 78 informing the user that the card has been retained.

In the event of condition (2) above, the ATM 70 displays a message on the display 78 informing the user that the card is not usable.

The display may also provide details of how the user may apply for the card back or for a new card.

The ATM 10 then informs a service centre that it is out of operation due to possible fraud. A service engineer is then called to remove the material and the card (if still present) so that the ATM 70 is restored to working order.

-15-

To remove the card, the service engineer lifts the fascia 72 and resets the interlock 24 on the module 10. The engineer can then remove the material and the card in a similar way to the third party.

Various modifications may be made to the above described embodiment within the scope of the invention, for example, the interlock may be implemented in a number of different ways. The predetermined time periods, such as when one sensor detects a card but another sensor does not detect a card may be longer or shorter than 20 seconds. Any convenient combination of the sensors 26,27,28,44,46,48 may be used (for example sensor 27 and sensor 48; or, sensor 44 and sensor 48) to detect that a card has jammed within the housing 12. The self-service terminal may be a non-cash kiosk. In other embodiments, a different MCRW modules than that described may be used, for example, an MCRW module from Omron.

CLAIMS

1. A motorised card reader module (10) characterised in that the module (10) includes a trap mechanism (20) operable to trap a card (60) within the card reader module (10) in response to the card reader module (10) detecting a card (60) within the module (10) that cannot be transported.

2. A module according to claim 1, wherein the trap mechanism (20) is implemented by a width switch (22) and associated interlock (24), where the width switch (22) is located within a throat portion (14) of the card reader module (10).

3. A module according to claim 1 or 2, wherein the card reader module is operable, on detecting that the trap mechanism (20) cannot trap an entered card, to activate a magnetic head (28) located in a throat portion (14) of the card reader module (10) to erase data stored on a magnetic stripe on the entered card.

4. A self-service terminal (70) comprising a fascia (72) defining a card entry slot (82), and a card reader module (10) located behind the card entry slot (82), characterised in that the module includes a trap mechanism (20) operable to trap a card within the card reader module in response to the card reader module detecting a card within the module that cannot be transported.

5. A motorised card reader module (10) including a shutter (18) and a width switch (22), characterised in that the width switch (22) is operable to trap a card within the card reader module (10) in response to the card reader

module detecting a card within the module that cannot be transported.

6. A module according to claim 5, wherein the module is operable to activate an alarm on detecting a card within the module that cannot be transported.

7. A method of preventing fraud, the method comprising the steps of: providing a trap mechanism for trapping a card within a card reader module; detecting entry of a card into the card reader module; monitoring transport of the card within the card reader module; and, in response to detection of a failure of the card reader module to transport the card correctly, activating the trap mechanism to trap the card.

8. A method according to claim 7, wherein the method includes the further step of displaying on a monitor (78) a message informing the user about the capture of his/her card.

9. A method according to claim 7 or 8, wherein the method includes the steps of detecting continued activation of a first sensor but not detecting activation of a second sensor within a predetermined time.

10. A method according to any of claims 7 to 9, wherein the method includes the step of: on detecting that the trap mechanism is unable to trap the card, activating a read/write head for erasing any data stored on the card.

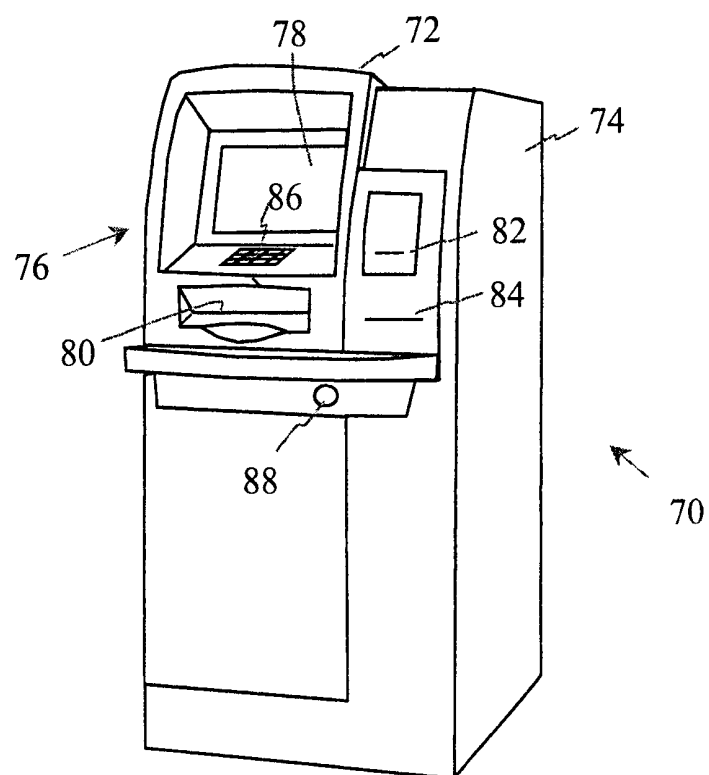
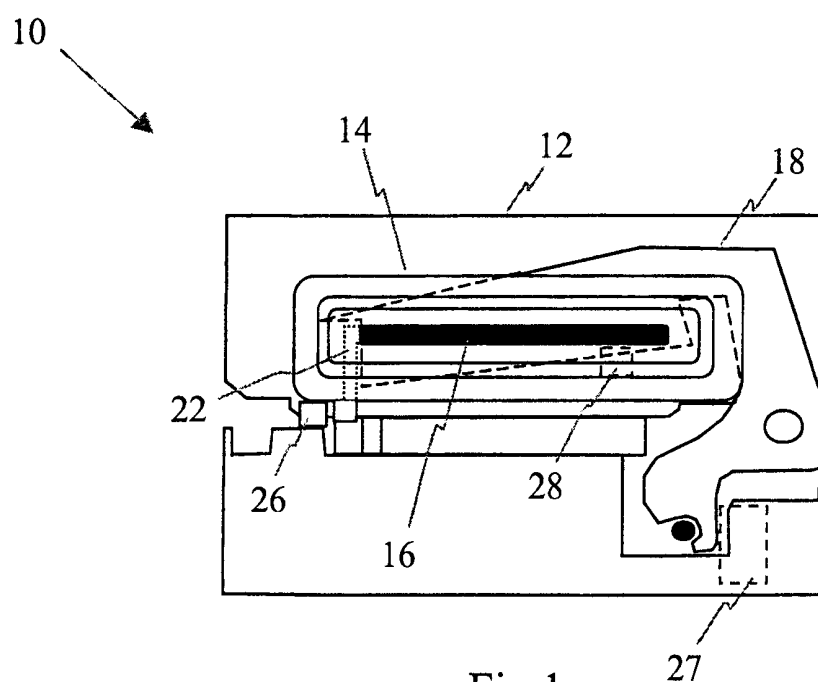
11. A motorised card reader module (10) characterised in that the module (10) includes a magnetic head (28) operable to erase data stored on a magnetic stripe (62) on a card

-18-

(60) in response to the card reader module (10) detecting a card (60) within the module (10) that cannot be transported.

12. A module according to claim 11, wherein the magnetic head is located in a throat portion (14) of the module (10).

1/4



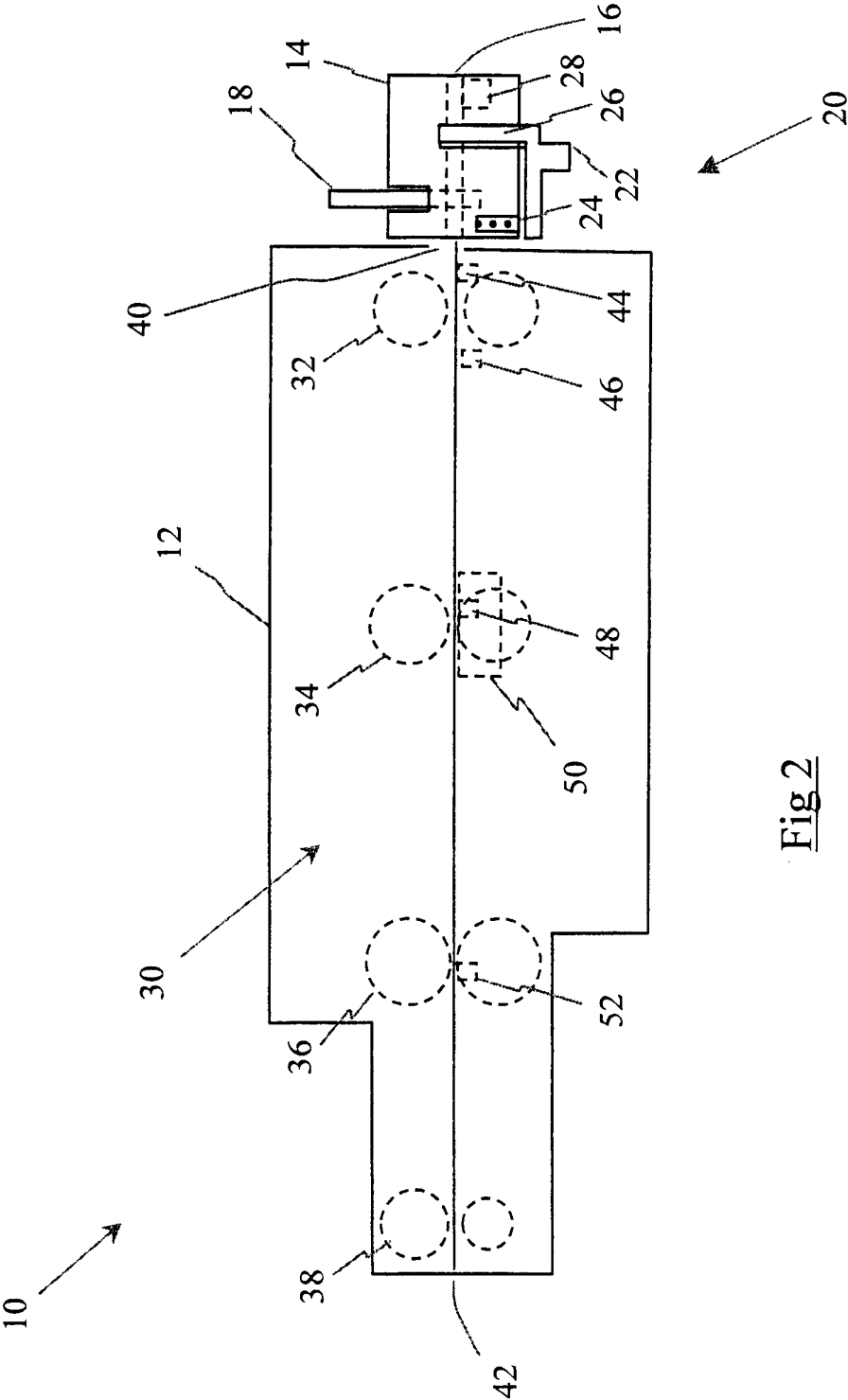
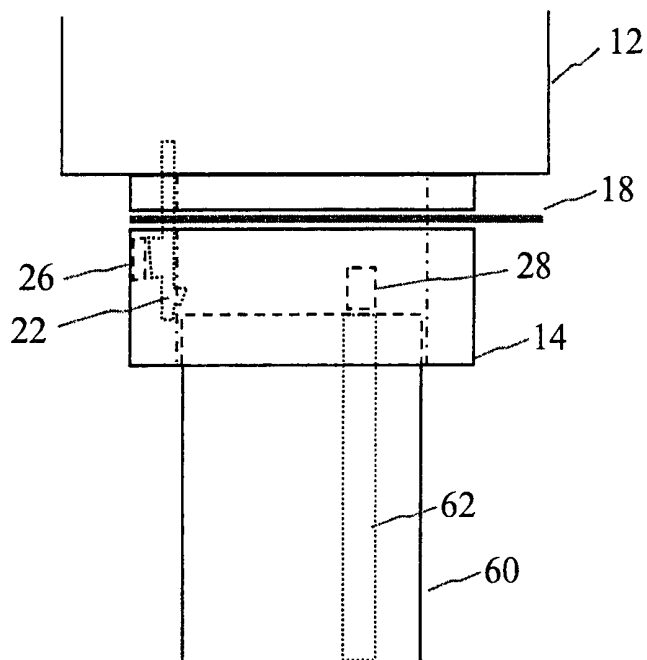
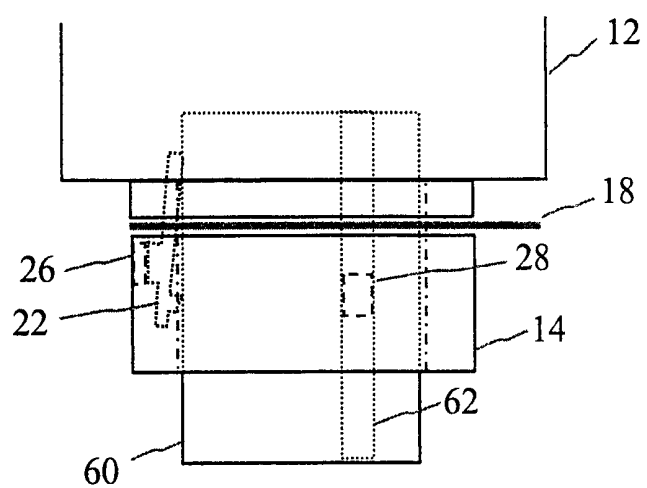


Fig 2

3/4

Fig 3Fig 4

4/4

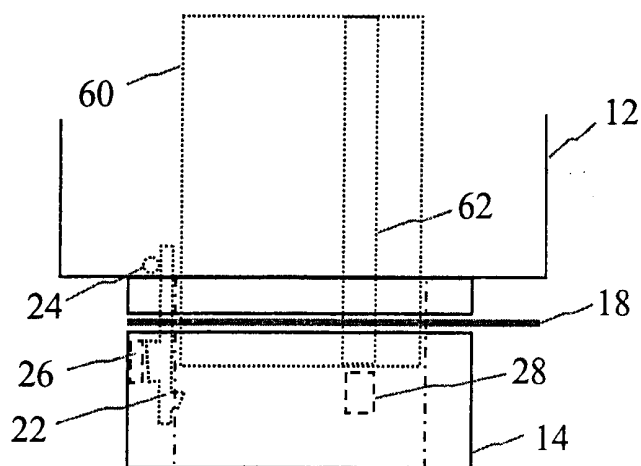


Fig 5

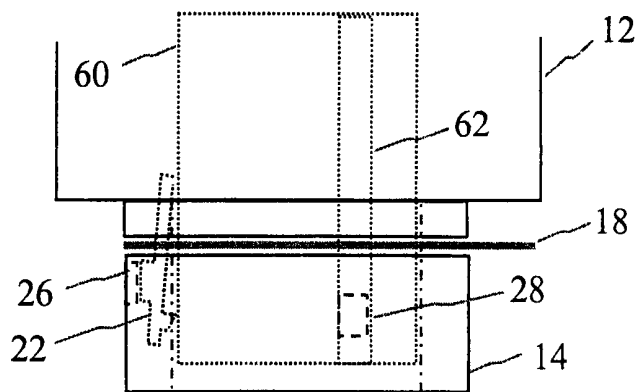


Fig 6

INTERNATIONAL SEARCH REPORT

In ternational Application No

PCT/GB 01/01214

A. CLASSIFICATION OF SUBJECT MATTER
IPC 7 G06K13/08 G06K13/067

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)

IPC 7 G06K

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practical, search terms used)

EPO-Internal, PAJ, WPI Data

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category *	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	US 5 264 688 A (MATSUNO RYUJI ET AL) 23 November 1993 (1993-11-23) column 2, line 49 - line 65 column 4, line 7 - line 44	1,4,7-9
Y		2,3,5,6, 10
X	GB 2 293 476 A (SANKYO SEIKI SEISAKUSHO KK) 27 March 1996 (1996-03-27) the whole document	11,12
Y		3,10
A		9
Y	EP 0 236 846 A (SIEMENS AG) 16 September 1987 (1987-09-16) column 3, line 28 -column 4, line 19 column 5, line 34 -column 6, line 11 figures 1,2	2,5,6
	--- -/--	

☒ Further documents are listed in the continuation of box C.

☒ Patent family members are listed in annex.

* Special categories of cited documents:

A document defining the general state of the art which is not considered to be of particular relevance

E earlier document but published on or after the international filing date

L document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)

O document referring to an oral disclosure, use, exhibition or other means

P document published prior to the international filing date but later than the priority date claimed

T later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

X document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

Y document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art.

& document member of the same patent family

Date of the actual completion of the international search

13 July 2001

Date of mailing of the international search report

19/07/2001

Name and mailing address of the ISA

European Patent Office, P.B. 5818 Patentlaan 2
NL - 2280 HV Rijswijk
Tel. (+31-70) 340-2040, Tx. 31 651 epo nl,
Fax: (+31-70) 340-3016

Authorized officer

Bhalodia, A

INTERNATIONAL SEARCH REPORT

International Application No

PCT/GB 01/01214

C.(Continuation) DOCUMENTS CONSIDERED TO BE RELEVANT

Category *	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	US 5 317 137 A (WILKINS JOHN L) 31 May 1994 (1994-05-31) column 2, line 19 - line 58 column 3, line 11 - line 40 column 5, line 18 -column 6, line 17	7,8
A	----- EP 0 363 992 A (OMRON TATEISI ELECTRONICS CO) 18 April 1990 (1990-04-18) column 7, line 56 -column 8, line 52; figures 2,3	1-6,9-12
A	----- US 6 045 377 A (KAJIURA MOTOMU) 4 April 2000 (2000-04-04) column 7, line 53 -column 8, line 2 column 9, line 8 - line 47 figures 1,2	2,5
A	----- EP 0 784 284 A (NCR INT INC) 16 July 1997 (1997-07-16) column 3, line 47 -column 4, line 32 -----	1

INTERNATIONAL SEARCH REPORT

Information on patent family members

International Application No

PCT/GB 01/01214

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
US 5264688 A	23-11-1993	DE 4120549 A	02-01-1992
GB 2293476 A	27-03-1996	JP 2990485 B	13-12-1999
		JP 8096093 A	12-04-1996
		DE 19535787 A	28-03-1996
EP 0236846 A	16-09-1987	AT 59716 T	15-01-1991
		DE 3766853 D	07-02-1991
		GR 3001388 T	11-09-1992
US 5317137 A	31-05-1994	NONE	
EP 0363992 A	18-04-1990	JP 2181288 A	16-07-1990
		JP 2707670 B	04-02-1998
		JP 2126386 A	15-05-1990
		JP 2585759 B	26-02-1997
		JP 2127790 A	16-05-1990
		AT 136382 T	15-04-1996
		AT 189326 T	15-02-2000
		AT 182999 T	15-08-1999
		DE 68926141 D	09-05-1996
		DE 68926141 T	12-12-1996
		DE 68929047 D	09-09-1999
		DE 68929047 T	13-04-2000
		DE 68929147 D	02-03-2000
		DE 68929147 T	21-09-2000
		EP 0696008 A	07-02-1996
		EP 0696009 A	07-02-1996
		ES 2088779 T	16-09-1996
		ES 2138695 T	16-01-2000
		US 5196687 A	23-03-1993
		SG 48972 A	18-05-1998
		SG 43174 A	17-10-1997
		SG 43239 A	17-10-1997
US 6045377 A	04-04-2000	JP 7192805 A	28-07-1995
		US 5899763 A	04-05-1999
		US 6155853 A	05-12-2000
		EP 0729655 A	04-09-1996
		SG 48117 A	17-04-1998
		TW 404520 Y	01-09-2000
		WO 9514317 A	26-05-1995
EP 0784284 A	16-07-1997	JP 9223208 A	26-08-1997
		US 5828043 A	27-10-1998