OPIC
Office de la propriété intellectuelle du Canada

CIPO
Canadian Intellectual Property Office

(12) (19) (CA) **Brevet-Patent**

(11) (21) (C) **2,089,579**
(86) 1991/08/14
(87) 1992/02/15
(45) 2000/10/03

(72) MacDonald, John L., GB
(73) JOHN MCLEAN & SONS (ELECTRICAL) DINGWALL LTD., GB

(51) Int.Cl.[5] G06K 19/00, G06K 9/62
(30) 1990/08/14 (9017774.2) GB
(30) 1990/09/07 (9019544.7) GB

(54) **SYSTEME DE SECURITE POUR DOCUMENTS**
(54) **DOCUMENT SECURITY SYSTEM**

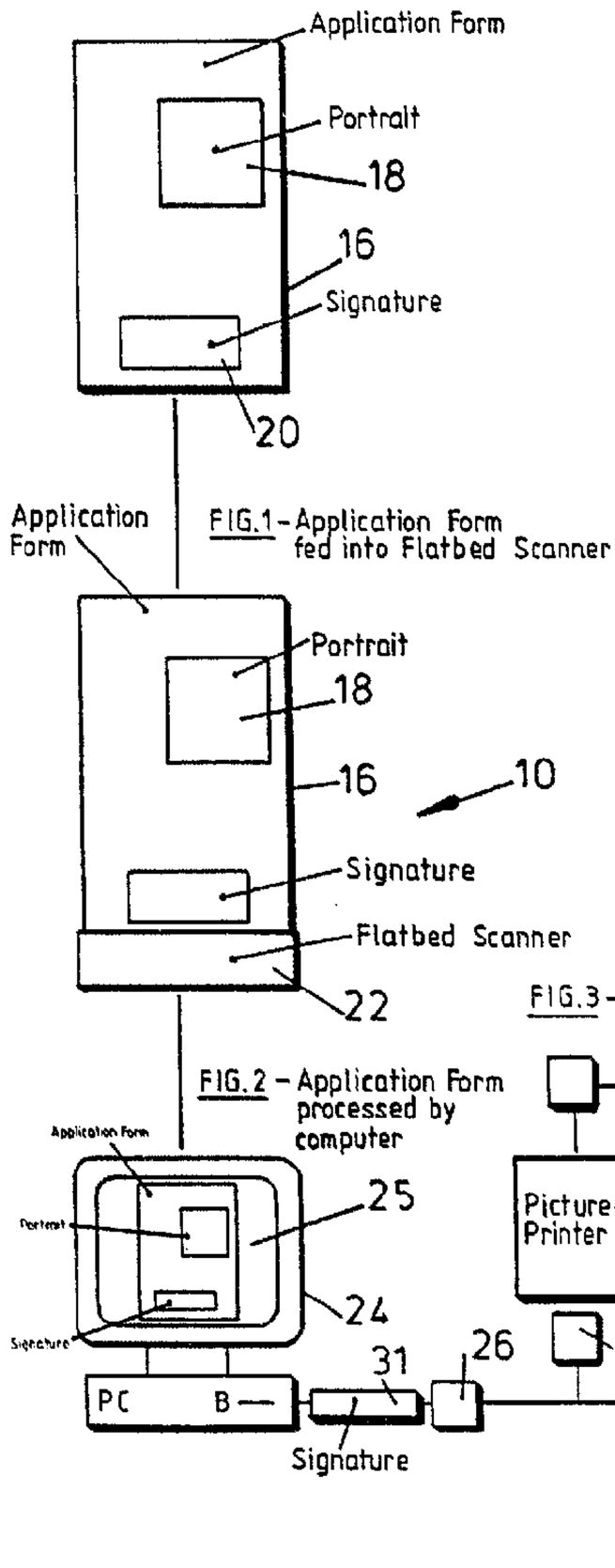


FIG.1 - Application Form fed into Flatbed Scanner

FIG.2 - Application Form processed by computer

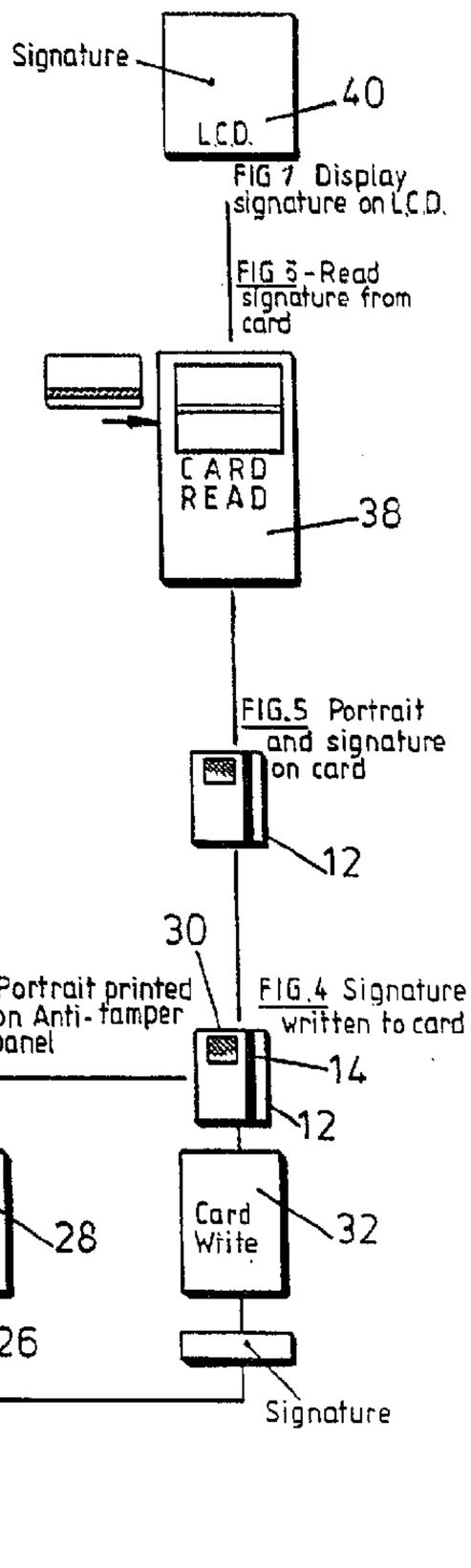


FIG 7 Display signature on L.C.D.

FIG 5 - Read signature from card

FIG.5 Portrait and signature on card

FIG.3 - Portrait printed on Anti-tamper panel

FIG.4 Signature written to card

(57) Système de sécurité pour documents destiné à coder des documents tels que des cartes de crédit, cartes de paiement et autres à l'aide d'un seul signal caractéristique de l'utilisateur, ce signal ne pouvant être lu à l'oeil nu et ne pouvant être lu qu'à l'aide d'un dispositif de lecture de document tel qu'un lecteur de

(57) A document security system is described for encoding documents such as credit cards, chargecards and the like with a unique signal representative of the user which cannot be read by the unaided eye and can only be read using a document reading means such as a card swipe machine. In a preferred arrangement the

OPIC
Office de la propriété intellectuelle du Canada

CIPO
Canadian Intellectual Property Office

(11) (21) (C) **2,089,579**
(86) 1991/08/14
(87) 1992/02/15
(45) 2000/10/03

carte. Selon une conception préférentielle, la signature (20) d'un utilisateur est numérisée par un lecteur numérique (22) et les données numériques sont condensées et codées magnétiquement sur la barre magnétique (14) d'une carte de crédit (12). Le portrait de l'utilisateur (18) peut également être numérisé et imprimé sur un panneau anti-manipulations (30) situé sur la carte. A l'utilisation, l'utilisateur présente la carte (12) dans une banque ou un magasin et le portrait est d'abord comparé avec l'utilisateur et dans l'hypothèse ou il y a ressemblance, la carte (12) est passée à travers un lecteur de carte (38) et la signature codée est lue et affichée sur un écran à cristaux liquides (40). Au point d'utilisation, le vendeur ou le caissier peut comparer la signature lue sur la carte à la signature effective de l'utilisateur pour vérifier l'authenticité de l'utilisateur. Des applications de cette invention et une nouvelle technique de compression numérique sont également décrites.

signature (20) of a user is digitised by a digital scanner (22) and the digital data is compressed and magnetically encoded onto the magnetic stripe (14) of the credit card (12). The user's portrait (18) can also be digitised and printed on an anti-tamper panel (30) on the card. In use, the user presents the card (12) in a bank or store and the portrait is initially compared with the user and assuming there is a likeness, the card (12) is swiped through a card-swipe reader (38) and the encoded signature is read and displayed on an LCD-type display (40). The vendor or teller at the point of use can then compare the signature read from the card with the user's actual signature to verify the authenticity of the user. Embodiments of the invention and a novel digital compression technique are described.

PCT WORLD INTELLECTUAL PROPERTY ORGANIZATION
International Bureau

INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(51) International Patent Classification 5 : G07C 9/00 — **A1**

(11) International Publication Number: WO 92/03804

(43) International Publication Date: 5 March 1992 (05.03.92)

2089579

(21) International Application Number: PCT/GB91/01385

(22) International Filing Date: 14 August 1991 (14.08.91)

(30) Priority data:

9017774.2	14 August 1990 (14.08.90)	GB
9019544.7	7 September 1990 (07.09.90)	GB

(71) Applicant *(for all designated States except US):* SIGNATURE VERIFICATION SYSTEMS LTD. [GB/GB]; Laggan View, Dores Road, Inverness IV1 2DH (GB).

(72) Inventor; and
(75) Inventor/Applicant *(for US only) :* MACDONALD, John, L. [GB/GB]; 44 Swanston Avenue, Inverness FV3 6QW (GB).

(74) Agents: NAISMITH, Robert, Stewart et al.; Cruikshank & Fairweather, 19 Royal Exchange Square, Glasgow G1 3AE (GB).

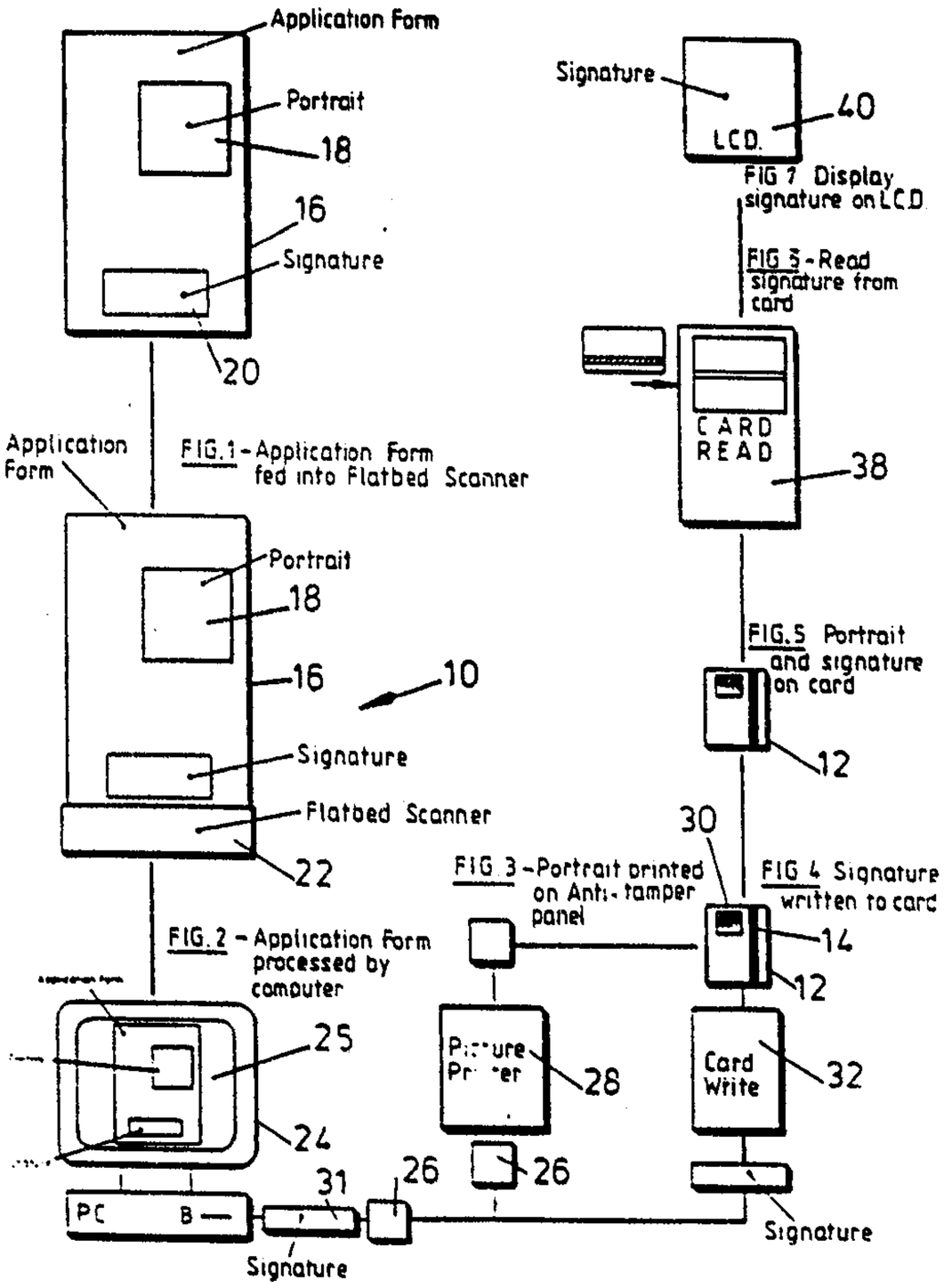
(81) Designated States: AT, AT (European patent), AU, BB, BE (European patent), BF (OAPI patent), BG, BJ (OAPI patent), BR, CA, CF (OAPI patent), CG (OAPI patent), CH, CH (European patent), CI (OAPI patent), CM (OAPI patent), CS, DE, DE (European patent), DK, DK (European patent), ES, ES (European patent), FI, FR (European patent), GA (OAPI patent), GB, GB (European patent), GN (OAPI patent), GR (European patent), HU, IT (European patent), JP, KP, KR, LK, LU, LU (European patent), MC, MG, ML (OAPI patent), MN, MR (OAPI patent), MW, NL, NL (European patent), NO, PL, RO, SD, SE, SE (European patent), SN (OAPI patent), SU+,TD (OAPI patent), TG (OAPI patent), US.

Published
With international search report.

(54) Title: DOCUMENT SECURITY SYSTEM

(57) Abstract

A document security system is described for encoding documents such as credit cards, chargecards and the like with a unique signal representative of the user which cannot be read by the unaided eye and can only be read using a document reading means such as a card swipe machine. In a preferred arrangement the signature (20) of a user is digitised by a digital scanner (22) and the digital data is compressed and magnetically encoded onto the magnetic stripe (14) of the credit card (12). The user's portrait (18) can also be digitised and printed on an anti-tamper panel (30) on the card. In use, the user presents the card (12) in a bank or store and the portrait is initially compared with the user and assuming there is a likeness, the card (12) is swiped through a card-swipe reader (38) and the encoded signature is read and displayed on an LCD-type display (40). The vendor or teller at the point of use can then compare the signature read from the card with the user's actual signature to verify the authenticity of the user. Embodiments of the invention and a novel digital compression technique are described.



+ See back of page

DOCUMENT SECURITY SYSTEM

The present invention relates to a document security system and apparatus for encoding documents such as cheque cards and credit cards with information to ensure that the documentation can be verified as authentic to prevent document fraud and the like. This invention is particularly, but not exclusively, intended to minimise cheque, cheque card and credit card fraud.

It is well known that document fraud, such as credit card frauds, costs several million pounds per annum both to the owners of the documents such as banks, and also to the customers. In addition, there is considerable police and court time devoted to the pursuit, apprehension and punishment of persons involved in the carrying out of such frauds.

An object of the present invention is to provide a document security system and apparatus which obviates or mitigates the above mentioned problem.

This is achieved by storing a unique signal representative of the user, such as a signature, on the document in a digitised and compressed form which cannot be read by the unaided human eye and providing reading means for reading the hidden signal so that the stored signal can be compared with the actual signal.

In a preferred arrangement, the signature of the user is provided on the document, for example, magnetically encoded cheque card or credit card. The

signature cannot be read if the document falls into unauthorised hands. However, the encoded signature may be read at the point of use by a reading machine and displayed on a screen and compared with a stored signature or compared with the presenter's signature to verify the authenticity of the user.

The encoded signal may be optically encoded and consequently can be optically read.

According to one aspect of the present invention there is provided a security system for storing a digitised and compressed signature on a magnetic stripe and comprising means for setting the desired usage size of the signature, means for setting the level of digital data to fit into said desired signature size, scanning means for scanning the signature line by line, and magnetic stripe writing means for writing the compressed data onto said magnetic stripe, the apparatus being characterised by means for determining and removing multiple dots from the scanned image and storage means for storing a number of dots and a number of dot displacements, counting and storage means for counting and storing increment values and the number and position of stray dots, comparison means for comparing the total dot count in said compressed digital data with the digital data level, and scaling means for scaling the image size of the signature by the target or dot count in vertical and horizontal scales.

Preferably the system comprises signal reading means

including magnetic stripe reading means for reading the magnetically encoded information on the magnetic stripe and display means coupled to the signal reading means for visually displaying the decoded signal so that a comparison between the decoded signal and a further signal provided by the user may be made to verify the identity of the user. Preferably also, said magnetic stripe reading means is a card swipe machine and said display means is a LCD visual display for displaying the signal read from the document swiped through the card swipe machine.

Conveniently, a portrait of the user is also recorded by said signal recording means and digitised, and printing means are coupled to said computer for receiving said digitised portrait data and printing the portrait of said user on the document as well as the encoded signal to provide a further level of document security.

According to a further aspect of the invention there is provided a method of compressing a digitised image of a signature characterised by the steps of:

setting the desired image size of the signature and setting the level of digital data to fit into said desired image size;

scanning the digital image of the signature line by line;

on the first scan line removing multiple dots and storing a number of dots and a number of dot

displacements; and

on the second and subsequent scan lines, for each stored dot on the previous line, counting and storing increments values, and counting and storing the number and position of stray dots;

comparing the total dot count in the compressed digital data with the digital data level;

scaling the image size of the signature by the dot count in the vertical and horizontal directions; and

repeating the above steps until the compressed digital data is less than the desired level.

Conveniently, a system embodying the invention includes a plurality of document reading means and displaying means disposed at remote locations, each document reading means and display means being a stand alone retrieval means for reading the digitised signal from the document and displaying the retrieval signal.

Conveniently also, each of said plurality of reading and display means are coupled to a central controller whereby the read signal can be electronically compared with a stored signal and both the stored and electronically read signals displayed for a visual comparison.

The image or signature is encoded in optically or magnetically format onto the document and may be read using a magnetic scanner or an optical scanner.

These and other aspects of the invention will become apparent from the following description when taken in

combination with the accompanying drawings in which:-

Fig. 1 is a schematic diagram of an embodiment of document security system in accordance with present invention;

Figs. 2a,2b depict a credit card in accordance with an embodiment of the present invention with the users portrait on the front and the magnetic stripe with the encoded signature on the back;

Fig. 3 is a diagrammatic example of a credit card printed with a portrait of a user and which carries a magnetically encoded signature using the system of Fig. 1;

Fig. 4 depicts a cheque card overprinted with a portrait of a user using the system of Fig. 1; and

Fig. 5 is a flow charge of a compression algorithm used with the system of Fig. 1 to compress and store signature data on the magnetic stripe of a credit card.

Reference is first made to Fig. 1 of the drawings which depicts a document security system, generally indicated by reference numeral 10, for incorporating a portrait of the user onto the point of a credit card 12 and the user's signature, invisible to the human eye, onto the magnetic stripe 14 on the reverse side of the card, best seen in Figs. 2a,2b, as will be later described in detail.

In the system 10, in order to create a secure card 12 a user who wishes such a card completes an application form 16 by including a self-portrait 18 such as a

passport-type photograph and also his signature 20. The completed application form 16 is fed into a flatbed image scanner 22 (type M3094 E/P, Fujitsu Limited) which digitises the image data at a fast scanning rate of 200 dots (pixels)/inch resolution in a line-art format. The portrait 18 is digitised using grey scale or colour. The digitised data is fed to a personal computer 24 (Apple MacIntosh, Trademark) which displays the digitised signature on the screen 25. In this format there is far too much data, perhaps 8-20K bytes of data in the signature alone, for it to be recorded onto magnetic card stripe.

The digitised portrait information 26 is fed to a picture printer 28 for printing the users portrait on an anti-tamper panel 30 on the front of the credit card 12. The signature 20 is compressed into 160 bytes or less of information as will be later described and the compressed signature data 31 is fed to a magnetic card write machine 32 which writes the compressed data onto certain available tracks on the magnetic stripe 14. In the present case the data is written onto 2 tracks, track 0 and track 4, but this may be varied depending on the particular application. The standard credit card is 3.375" wide and the magnetic stripe 14 is the same width. Thus, the data is compressed to fit the magnetic stripe width so that for each track there are approximately 200 bits per inch; this is why two tracks are needed to hold 160 bytes of compressed data. It will be appreciated

that one byte of the 160 bytes is used as a check sum byte to ensure that data is correctly written to the card or document.

Thus, the security coded credit card 12 contains the users portrait 18 on a tamper-proof panel 30 and the users signature electronically compressed and stored magnetically on tracks 0 and 4 of the magnetic stripe 14 as seen in Figs. 2a,2b and Fig. 3. Similarly, the portrait 18 without the signature may be printed onto personal cheques as shown in Fig. 4.

In order to use the card and ensure that the user is authentic, the card is presented to a point of sale position, e.g. the teller in a bank. The teller takes the card and firstly views the card portrait and compares it with the user before him. The card is then passed through a card reader such as a card swipe machine 38 which has a small LCD T.V. type display 40 coupled thereto. The card read-write machine is not ISO standard having been modified by the addition of switches and firmware inside so that 8 bits can be written to any of the tracks. The compressed signature of the user is firstly decoded from the tracks and displayed to the teller only on the LCD T.V. type display 40. When the user signs a cheque or other document the teller then compares his actual signature with the card-stored signature and, if satisfied as to the authenticity of the vendor, permits the transaction to be completed. Should the signatures be sufficiently different to cause doubt

as to the user's authenticity the vendor may terminate the transaction.

Thus, it will be appreciated that because the signature is invisible to the human eye it cannot be forged and the chances of a fraudulent user being able to sign a duplicate signature to the card-stored signature is negligible. The provision of the users portrait on the credit card further enhances security.

A further level of security may be provided by encoding the digitised portrait or signature to form a scrambled signal and to print the scrambled signal on the cheque, cheque card or other document. At the time of use, the user signs the cheque in the usual way. The scrambled signature cannot be read except by the teller who can "read" the scrambled code with a machine having a decryption algorithm. The teller is thus able to compare the scrambled signal, representative of portrait or signature, with the stored information. This means that the teller has access to a device either retrieving the unscrambled data from master storage unit or for reading the scrambled information on the document and descrambling it so that a comparison can be made at the point of use.

As described above, a particularly convenient solution to the problem is achieved by printing an unscrambled portrait of the user on the document or card as shown in Figs. 2, 3 and 4 for ease of immediate comparison and also providing an unscrambled signal

representative of the signature of the user on the card. With existing technology, this comparison can be readily effected in most stores or businesses where document verification is required.

The personal computer 24 and card reader 38 may be connected by a suitable network or other suitable link to a distributed group of computers or terminals which have access to the stored information.

Reference is now made to Fig. 5 of the drawings which depicts a flow chart of the compression technique used with the system of Fig. 1 to compress the data digitised by the flatbed image scanner 22 to a sufficiently small number of bytes, in our case 160 bytes, to fit onto 2 tracks or the magnetic stripe 14 on the credit card 12, but which, when read, will display clearly a legible facsimile of the actual signature of the user. In practice, the compression technique has to reduce the scanned 200 dots/inch image occupying 8-20K bytes of file space to 160 bytes. The technique parameters could be raised to accommodate higher byte capacities to suit tracks being developed with higher bit densities, for example 420 bits per inch instead of 210 bits per inch. Alternatively, an additional track may be added to the magnetic stripe 14 to receive compressed data.

The encoding of magnetic stripe is well established and is not disclosed here. Reference is made to an article in Auto ID Today by Sjoerd P. Wouda entitled

Magnetic Strip Technology (Vo. 7, June 1989). Because space on each track is limited the compressed data is stored in bit fields which do not fall necessarily on bit boundaries. For example, a 5-bit field could be stored as 3 bits in one byte and 2 bits in the next byte so that no bits are wasted.

Compression of the scanned data is achieved by using the fact that the raster scanned image data is stored as a number of lines of dots. The stored data is first processed, one line at a time, to remove multiple dots which are next to each other as some of these are redundant. For example, a typical pen width at 200 dots/inch scanning results up to 15 to 20 bits in the scanned image and these "multiples" are removed. In addition, the compression technique makes use of the fact that the data in a scanned signature is not random. For example, in a scanned signature if a dot is encountered in one line, then it is likely that a dot will be found on the next line either directly below or slightly to the right or left. This is resolved down to four possibilities; a dot below, a dot one space left, a dot one space right or none of these and these four possibilities are represented by 2 bits.

Referring to Fig. 5, when starting with the first line (line 0) in the image there is a bit field 42 to store a number of points, then a number of bit fields which give the distance to the first point, the distance from the last point to the current point etc. By using

the increments algorithm there will be as many increments on the next line (line 1) as points on line so that there is no need for any increment count. Line 1 is therefore scanned 44 for increments and store 46, and then re-scanned 48 to detect any points, called strays, which are not picked-up as increments, and then a further line is encoded in the same format as line 1 with a dot count field plus as many dot displacement fields 50. Thus, line 1 is stored as a dot count plus a bit of dot displacements on line 2 and subsequent lines are stored as a number of increments, each increment being encoded on 2 bits, with the number of increments being the same as the number of dots on the previous line, plus the number of strays and the displacements of those strays.

It is desired to reduce the data to 160 bytes, i.e. 1280 bits and the actual scanned image may contain perhaps 2-300 lines and 6-800 columns. In practice best results have been obtained when this image is scaled down to a maximum of 63 lines by 127 columns. Vertical and horizontal scales are first picked (Fig. 4) which match these values and then the image is scanned and compressed. The number of bits in the scanned image is then compared 52 with the target, i.e. 1280 bits in this example. If the number of compressed image bits is greater than the target number of bits, then the number of horizontal and vertical scan lines is scaled down by the number of allowable (target) bits to actual bits 54,56 (target/dot count $_{HOR;}$ target/dot count $_{VERT}$) so that

the target number of bits is obtained in two or three iterations. If the number of compressed image bits is less than the target number, the compression is complete.

The technique contains several optimisation features, one of which is that the bit fields are reduced in size from the theoretical minimum to save space. For example, because more than 15 strays are rarely encountered on one line, the count of strays is encoded on 4 bits only. If there is a stray count >15 in the 4-bit field, 15 is put in the 4-bit field and then the next 6-bit field is used for the full stray count. Therefore, on that particular line storage capacity has been lost, but overall the technique has saved 5 to 10% of storage. The same technique is also applied to the storage of displacements
on a line.

It will be understood that various modifications may be made to the embodiment herebefore described before departing from the scope of the invention. In the apparatus described, for example, a video camera could be used for taking portraits and the image scaled to provide a digitised portrait. Alternatively, a still photograph or signature could be digitised using a digitising tablet. In addition, the flatbed image scanner 22 may be used to digitise a picture of the fingerprint of a user to provide a unique signal representative of that user and this signal compressed using a similar technique described with reference to the signature. A similar

compression technique may be used to compress the portrait data. The compressed data may be optically encoded onto the document and read by an optical card reader (OCR) using existing OCR technology. The photograph and/or image of the user may be located on the signature strip on a credit card and the scrambled code may be contained in a medium which can be decoded by an optical scanner or magnetic scanner.

The laser printer may be replaced by any other suitable digitally controlled printer such as an ink-jet printer or electro-static printer. In addition, it is not necessary for other remote terminals to be directly connected to a master computer which stores all the information or a stand-alone reader to compare the presenter's signature with that which is encoded. The remote terminals may be connected by a modem. The information may be stored on a disc which may be sent to a remote location and inserted into an appropriate host terminal which has software to enable the comparisons of portrait and encoded signature to be made with the presenter's signature. Signatures or portraits could also be faxed to remote locations from a central location to facilitate verification. It will be understood that document is a general term applicable to a variety of objects such as credit cards, smart cards, chargecards, cheques, cheque guarantee cards, files, folders, I.D. cards, security access cards and any other suitable document where it is desirable to ensure the authenticity

of the user and prevent fraud.

Advantages of the present invention are that there are extra levels of security to enable verification of the user to take place and that the comparison is effected on the basis of characteristics which are believed to be unique to the user, for example, the portrait signature, fingerprint or combinations of these. Thus, the opportunity for forgery or fraud in connection with such documentation is considerably minimised. The system uses existing technology and is designed to interface with existing systems, thus it can readily be set up in existing environments without specialist expertise.

In the case of a smart card, i.e. one that has a processor and storage means, the signature and portrait could be contained in the storage means therein.

CLAIMS

1. A security system for storing a digitised and compressed signature of a user on a magnetic stripe and comprising means for setting a desired usage size of the signature, means for setting a level of digital data to fit into said desired usage size, image scanning means for scanning the signature line by line, means for determining and removing multiple dots from the scanned image of the signature, storage means for storing a number of dots and a number of dot displacements, counting and storage means for counting and storing increment values and a number and a position for stray dots, comparison means for comparing a total dot count in said compressed data with a target count from the set level of digital data, scaling means for scaling the size of the image of the signature by the target or total dot count in vertical and horizontal scales and magnetic stripe writing means for writing compressed data as magnetically encoded information onto said magnetic stripe.

2. A security system according to claim 1 and arranged to compress the signature to 160 bytes or less.

3. A security system according to claim 1 or 2 and comprising magnetic stripe reading means for reading the magnetically encoded information on the magnetic stripe to provide a decoded signal, and display means coupled to the stripe reading means for visually displaying the decoded signal of the signature so that a comparison

between the signature and a further signature provided by the user may be made to verify the identity of the user.

4. A security system according to claim 3, wherein the magnetic stripe reading means is a card-swipe machine and the display means is a LCD visual display for displaying the signal read from a document swiped through the card-swipe machine.

5. A security system according to claim 3 or 4 and comprising data encryption means for encrypting the digital data prior to writing the digital data onto the magnatic stripe, the magnetic stripe reading means including data decrypting means for decrypting the encrypted data stored on the magnetic stripe.

6. A security system according to any one of the preceding claims, wherein the magnetic stripe is held on a credit card, cheque card or smart card.

7. A security system according to any of the preceding claims, wherein the image scanning means is also arranged to scan a portrait of a user and the system comprises printing means for receiving digitised portrait data and for printing the portrait of the user onto a document holding said magnetic stripe to provide a further level of security.

8. A security system according to claim 7, wherein the portrait is contained in a tamper-proof panel on the document.

9. A security system according to any one of the preceding claims, wherein the user's signature is encoded

onto two tracks of the magnetic stripe.

10. A method of compressing a digitised image of a signature comprising the step of:

setting a desired image size of the signature and setting a level of digital data to fit into said desired image size;

scanning the digital image of the signature line by line from a first scan line to a second and subsequent scan lines;

on the first scan line removing multiple dots and storing a number of dots and a number of dot displacements;

on the second and subsequent scan lines, for each stored dot on a previous line, counting and storing increments values, and counting and storing a number and a position for stray dots;

comparing a total dot count representing a compressed digitised image size with the digital data level;

scaling the image size of the signature by the total dot count in both vertical and horizontal directions; and

repeating the above steps until the compressed digitised image size is less than the set level of digital data.

11. A method of verifying the authenticity of a user of a document, the method comprising:

storing a compressed, digitised, image of a signature of the user obtained by the method of claim 10

B

onto a magnetic stripe on the document;

reading the stored, compressed, digitised image from the document with a stand alone reading means; and

displaying the signature so that the signature can be compared with an actual signature provided by a presenter or user of the document to allow verification of the authenticity of the user.

12. Apparatus for storing a digitised and compressed signature on a magnetic stipe in 160 bytes or less of data, said apparatus comprising means for setting a desired usage size of the signature and means for setting a level of digital data to fit into said desired usage size, image scanning means for scanning said signature line by line, means for determining and removing multiple dots from said scanned image of the signature and storage means for storing a number of dots and a number of dot displacements, counting and storage means for counting and storing increment value and a number and a position for stray dots, comparison means for comparing a total dot count in said compressed data with a target count from the set level of digital data, scaling means for scaling the size of the image of the signature by the target or total dot count in vertical and horizontal scales, and magnetic stripe writing means for writing compressed data onto said magnetic stripe.

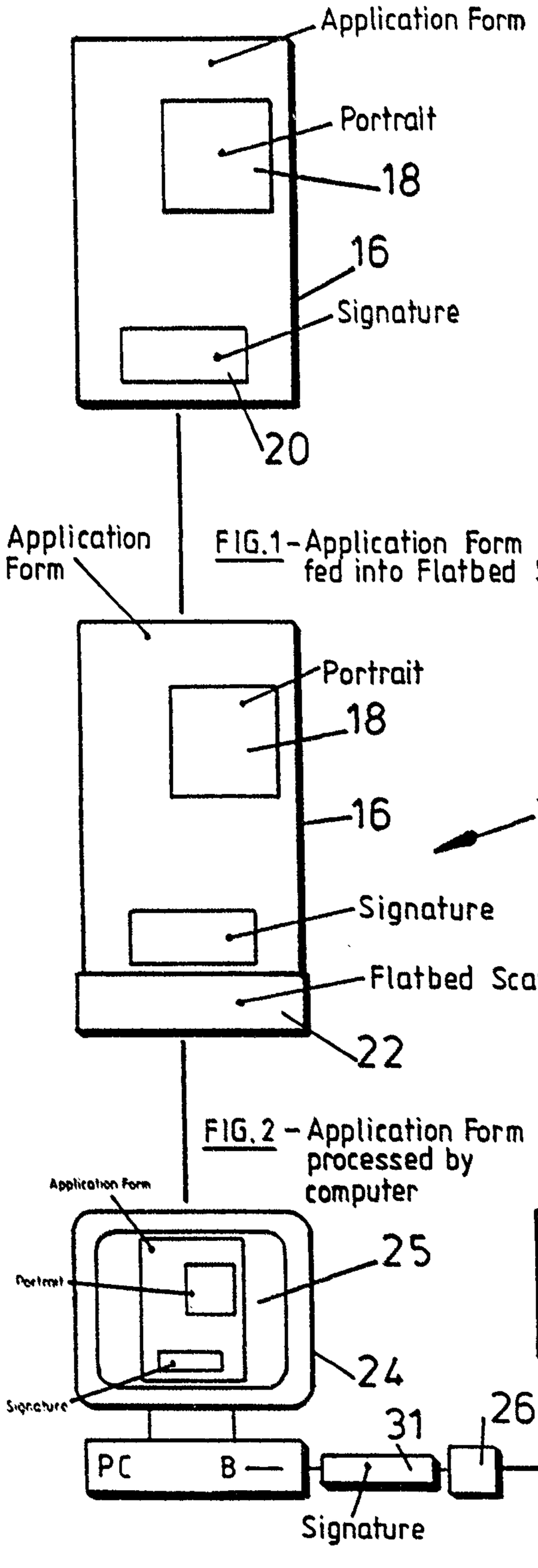


FIG.1 - Application Form fed into Flatbed Scanner

FIG.2 - Application Form processed by computer

FIG.3 - Portrait printed on Anti-tamper panel

FIG.4 Signature written to card

FIG.5 Portrait and signature on card

FIG 7 Display signature on L.C.D.

FIG 5 - Read signature from card

FIG. 1

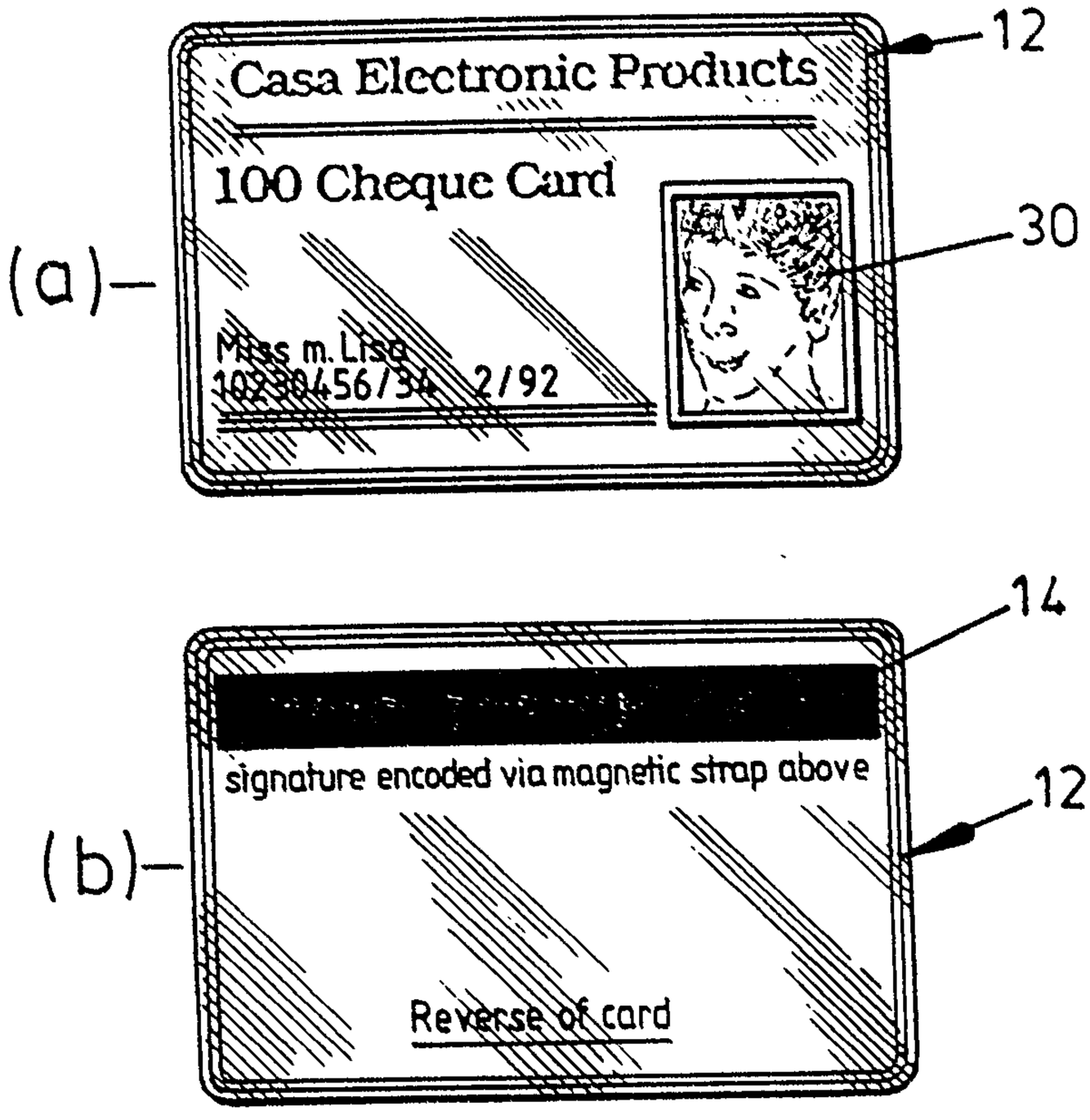

(a)
Casa Electronic Products
100 Cheque Card
Miss m. Lisa
102 3045 6/34 2/92
12
30
(b)
signature encoded via magnetic strap above
Reverse of card
14
12

FIG. 2


BANK OF SCOTLAND
£100 Cheque Card
30

FIG. 3

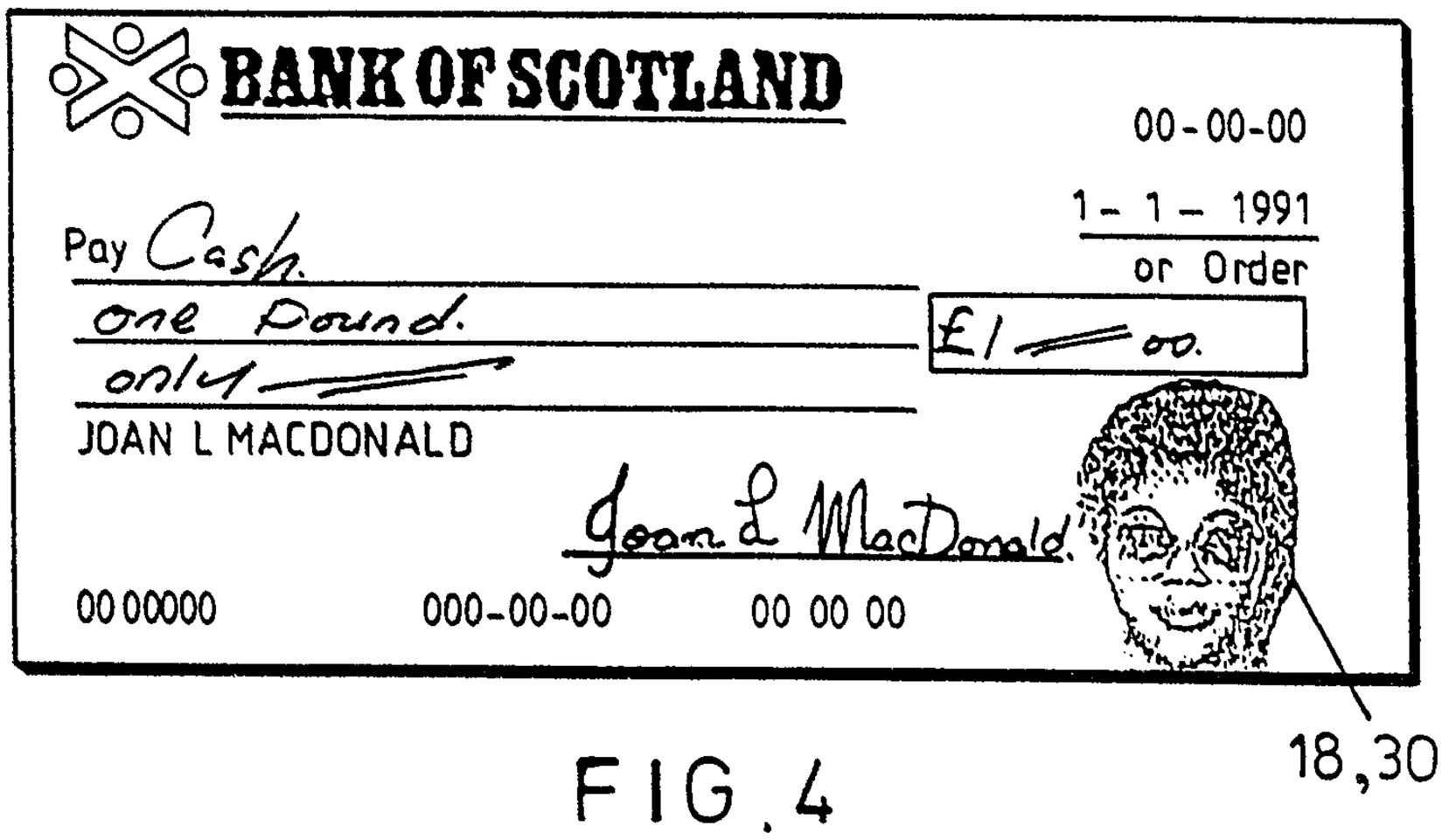

BANK OF SCOTLAND
00-00-00
1- 1- 1991
Pay Cash.
or Order
one Pound.
£1 — 00.
only —
JOAN L MACDONALD
Joan L MacDonald.
00 00000
000-00-00
00 00 00
18,30

FIG. 4

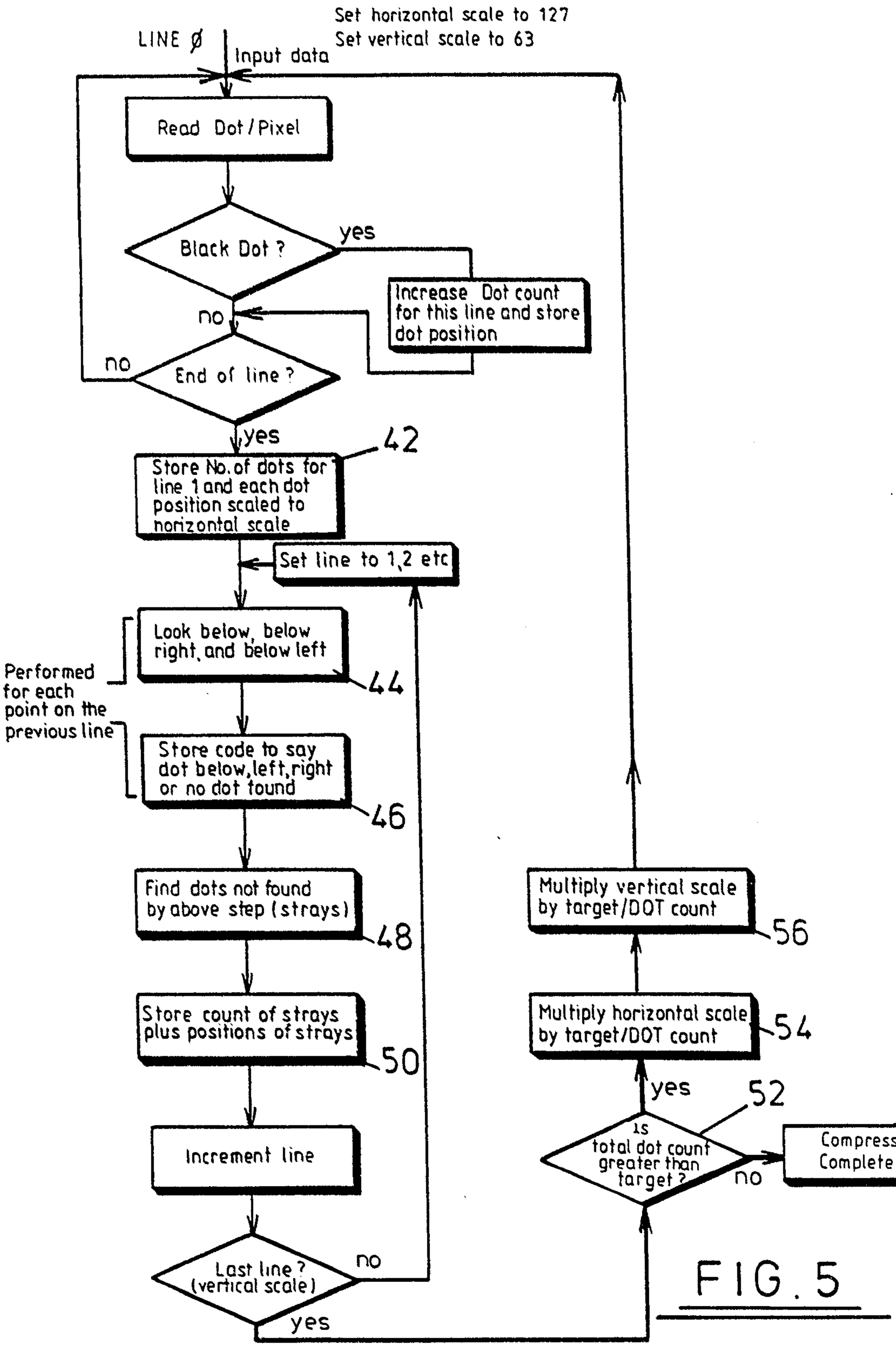

Set horizontal scale to 127
Set vertical scale to 63
LINE ø
Input data
Read Dot / Pixel
Black Dot ?
yes
Increase Dot count for this line and store dot position
no
End of line ?
no
yes
42
Store No. of dots for line 1 and each dot position scaled to horizontal scale
Set line to 1,2 etc
Look below, below right, and below left
44
Performed for each point on the previous line
Store code to say dot below, left, right or no dot found
46
Find dots not found by above step (strays)
48
Store count of strays plus positions of strays
50
Increment line
Last line ? (vertical scale)
no
yes
Multiply vertical scale by target/DOT count
56
Multiply horizontal scale by target/DOT count
54
yes
52
Is total dot count greater than target ?
no
60
Compression Complete

FIG. 5

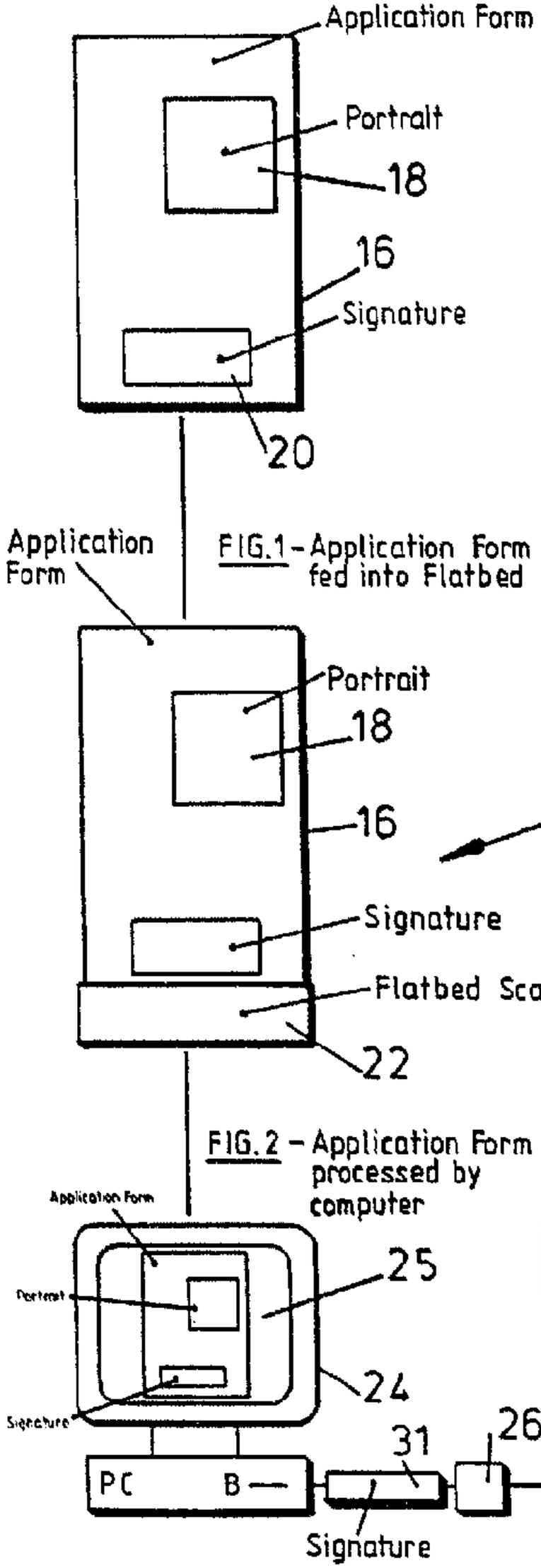


FIG.1 - Application Form fed into Flatbed Scanner

FIG.2 - Application Form processed by computer

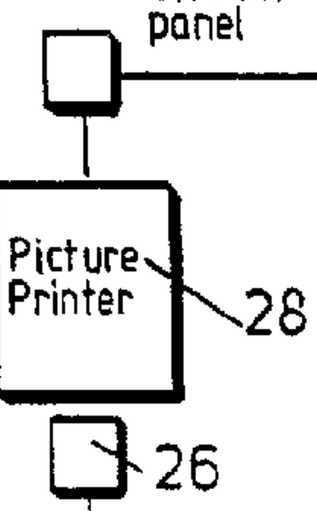


FIG.3 - Portrait printed on Anti-tamper panel

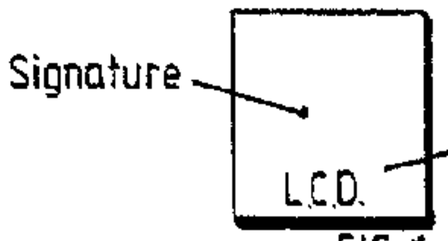


FIG 7 Display signature on L.C.D.

FIG 6 - Read signature from card

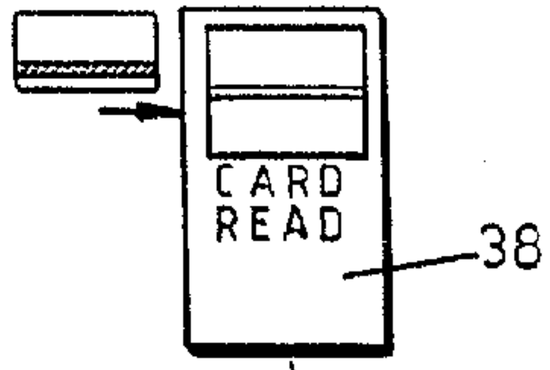


FIG.5 Portrait and signature on card

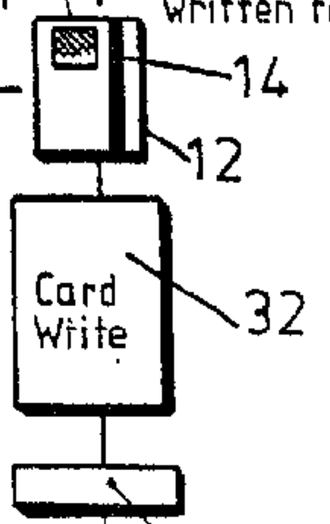


FIG.4 Signature written to card