



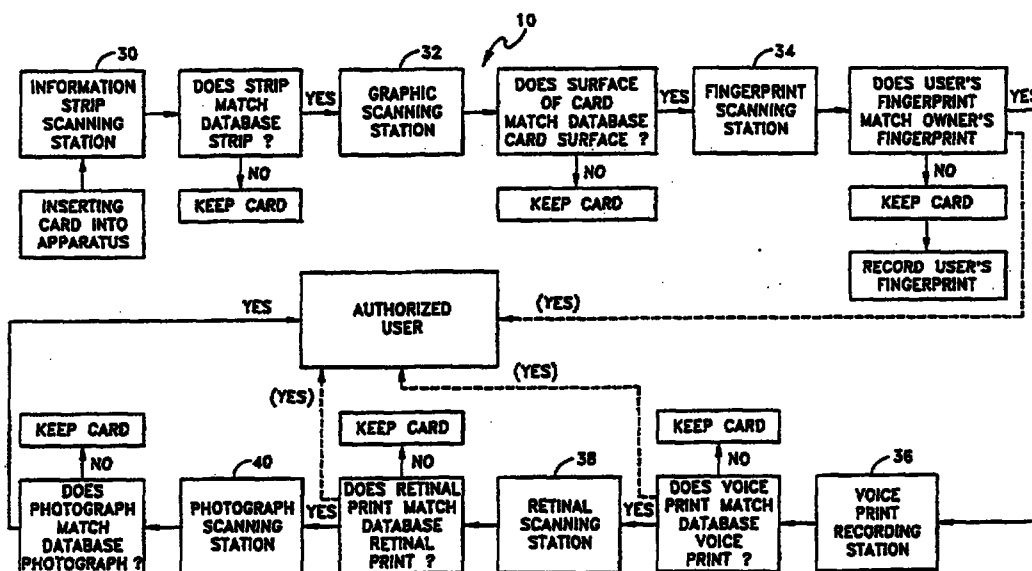
9702659-5

RIMP COPY

INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(51) International Patent Classification 6 : G06K 9/00	A1	(11) International Publication Number: WO 96/18168 (43) International Publication Date: 13 June 1996 (13.06.96)
(21) International Application Number: PCT/US95/15665 (22) International Filing Date: 4 December 1995 (04.12.95) (30) Priority Data: 349,688 5 December 1994 (05.12.94) US (71) Applicant: BOGOSIAN, Charles, A., Jr. [US/US]; 116 Highland Avenue, Warwick, RI 02886 (US). (74) Agents: HOLMES, Stephen, J. et al.; Salter & Michaelson, 321 South Main Street, Providence, RI 02903-7128 (US).	(81) Designated States: AM, AT, AU, BB, BG, BR, BY, CA, CH, CN, CZ, DE, DK, EE, ES, FI, GB, GE, HU, IS, JP, KE, KG, KP, KR, KZ, LK, LR, LT, LU, LV, MD, MG, MN, MW, MX, NO, NZ, PL, PT, RO, RU, SD, SE, SI, SK, TJ, TM, TT, UA, UG, UZ, VN, European patent (AT, BE, CH, DE, DK, ES, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE), OAPI patent (BF, BJ, CF, CG, CI, CM, GA, GN, ML, MR, NE, SN, TD, TG), ARIPO patent (KE, LS, MW, SD, SZ, UG). Published With international search report. <i>PCT A1 + SR</i> <i>Replacement 2.9.97</i> <i>Replacement 19.5.98</i>	

(54) Title: SYSTEM FOR VERIFYING USE OF A CREDIT/IDENTIFICATION CARD INCLUDING RECORDING OF PHYSICAL ATTRIBUTES OF UNAUTHORIZED USERS



(57) Abstract

The present invention is directed to a method and apparatus (10) for verifying an authorized user of a credit/identification card (12). The method includes the steps of scanning the card (12) with an apparatus having a plurality of scanning devices for scanning a bar code (16), scanning the card (12) for evidence of tampering, scanning at least one fingerprint (18) on the card (12), and any other detectable information, and comparing the scanned information on the card (12) to information of the owner stored on at least one accessible database (44) in communication with the apparatus (10). Data transmissions between the apparatus (10) and databases (44) are protected by an encryption system (63). If the information on the card (12) does not match the information germane to the owner of the card which is stored in the database (44), the card (12) is withheld from the user. Otherwise, the user of the card (12) is free to use it for a desired purpose.

1 SYSTEM FOR VERIFYING USE OF A CREDIT/IDENTIFICATION CARD
2 INCLUDING RECORDING OF PHYSICAL ATTRIBUTES OF
3 UNAUTHORIZED USERS

4 Background and Summary of the Invention:

5 This invention relates generally to methods and
6 apparatuses for verifying an authorized user of a credit
7 and/or identification card, and more particularly to a
8 method and apparatus which utilizes a plurality of
9 scanning stations for verifying the authorized user of
10 the card.

11 Recently, attempts have been made to develop systems
12 for preventing the unauthorized use of credit cards.
13 These systems typically utilize various devices for
14 authenticating the identity of the user of such cards.
15 One such system has been to provide on the face of the
16 card a fingerprint of the owner of the card wherein the
17 user's fingerprint must match the fingerprint on the
18 card. The concept of utilizing fingerprint
19 identification as verification for the authenticity of a
20 credit/identification card is well-known. U.S. Patent
21 Nos. 4,582,985 (Löfberg) and 5,180,901 (Hiramatsu) each
22 disclose a typical identifying system. However,
23 fingerprint identification requiring the user's
24 fingerprint to be compared to a fingerprint of the owner
25 on the card suffers from the disadvantage that the credit
26 card may easily be tampered with, e.g., the owner's

1 fingerprint is replaced by the fingerprint of the
2 unauthorized user.

3 Other methods of identifying authorized users of
4 cards also suffer from the same disadvantage. For
5 example, U.S. Patent No. 4,995,086 (Lilley et al.)
6 discloses a verification system whereby a bar code having
7 information about the owner of the card is provided on
8 the card and compared to information kept on a database
9 which communicates with the system. Like fingerprint
10 identification, the bar code which is applied on the
11 surface of the card can be tampered with.

12 Presently, there is a need for a method and
13 apparatus for verifying an authorized user of a
14 credit/identification card which can detect whether the
15 card has been altered so that an unauthorized user is
16 prevented from using the card.

17 Among the several objects of the present invention
18 are the provision of an improved method for verifying an
19 authorized user of a credit/identification card which is
20 capable of detecting whether the card has been tampered
21 with or changed; the provision of such an improved method
22 having several cross-checking steps which substantially
23 ensure authorized use of the card; the provision of such
24 a method capable of verifying whether a fingerprint of
25 the user of a card matches a fingerprint of the owner of
26 the card; the provision of such a method capable of

1 verifying whether a voice print of the user of the card
2 matches a voice print of the owner of the card; the
3 provision of such a method capable of verifying whether
4 a retinal print of the user of the card matches a retinal
5 print of the owner of the card; the provision of such a
6 method which withholds the card from an unauthorized
7 user; and the provision of such a method which is capable
8 of recording a fingerprint of an unauthorized user.

9 Also among the several objects of the present
10 invention are the provision of an improved apparatus for
11 verifying an authorized user of a credit/identification
12 card; the provision of such an apparatus which is capable
13 of detecting whether the card has been tampered; the
14 provision of such an apparatus having several scanning
15 devices for substantially ensuring authorized use of the
16 card; the provision of such an apparatus having a
17 fingerprint scanning device and associated means for
18 verifying whether a fingerprint of the user of the card
19 matches a fingerprint of the owner of the card; the
20 provision of such an apparatus having a microphone and
21 associated means for verifying whether a voice print of
22 the user of the card matches a voice print of the owner
23 of the card; the provision of such an apparatus having a
24 retinal scanning device and associated means for
25 verifying whether a retinal print of the user of the card
26 matches a retinal print of the owner of the card; the

1 provision of such an apparatus which withholds the card
2 from an unauthorized user; the provision of such an
3 apparatus which is capable of recording a fingerprint of
4 an unauthorized user; and the provision of such an
5 apparatus which encrypts data transmission when
6 communicating with a central database.

7 In general, a method for verifying an authorized
8 user of a credit/identification card comprises the steps
9 of:

10 (a) inserting the card into an apparatus having a
11 plurality of scanning stations, the card including a
12 surface having a strip thereon which has information
13 germane to the owner of the card, such as an
14 identification number and other personal data, and at
15 least one fingerprint thereon of the owner of the card;

16 (b) scanning the strip of the card at an
17 information strip scanning station of the apparatus for
18 verifying the information of the card including the
19 identification number;

20 (c) comparing the information stored on the strip
21 of the card to information of the owner stored on at
22 least one accessible database in communication with the
23 apparatus, the apparatus withholding the card from the
24 user if the information on the card does not match the
25 information germane to the owner of the card which is
26 stored in the database;

1 (d) scanning the surface of the card at a graphic
2 scanning station of the apparatus which digitizes the
3 surface of the card by imaging every line thereof;

4 (e) converting the image of the surface of the card
5 to a digital numeric sequence;

6 (f) comparing the surface of the card as scanned by
7 the graphic scanning device and converted to a digital
8 numeric sequence to a digital numeric sequence stored in
9 the database for determining whether the card has been
10 tampered with, the apparatus withholding the card from
11 the user if the surface of the card does not match the
12 surface of the card stored by the database;

13 (g) obtaining a fingerprint of the user;

14 (h) scanning the fingerprint of the user at a
15 fingerprint scanning station; and

16 (i) comparing the fingerprint of the user to the
17 fingerprint on the card and to a fingerprint of the owner
18 of the card in the database to ensure authorized use of
19 the card, the apparatus withholding the card from the
20 user if the fingerprint scanned by the fingerprint
21 scanning device does not match the fingerprints on the
22 card and in the database, whereby, upon matching the
23 user's fingerprint to the fingerprints on the card and in
24 the database for ensuring the user of the card is the
25 owner of the card, the apparatus allowing the user to use
26 the card for a desired purpose.

1 An apparatus for carrying out the method of the
2 present invention comprises an information strip scanning
3 device for scanning the information strip of the card and
4 means for comparing the information contained in the
5 strip to information of the owner stored on at least one
6 accessible database in communication with the apparatus.
7 The apparatus withholds the card from the user if the
8 information on the card does not match the information
9 germane to the owner of the card which is stored in the
10 database. The apparatus and database include encryption
11 means for encrypting data transmissions between the
12 apparatus and the database. A graphic scanning device
13 scans the surface of the card in which the graphic
14 scanning device digitizes the surface of the card by
15 imaging every line thereof. Suitable means converts the
16 image of the surface of the card to a digital numeric
17 sequence and means compares the surface of the card as
18 scanned by the graphic scanning device and converted to
19 a digital numeric sequence by the converting means to a
20 digital numeric sequence stored in the database for
21 determining whether the card has been altered. The
22 apparatus withholds the card from the user if the surface
23 of the card does not match the surface of the card stored
24 by the database. A fingerprint scanning device having a
25 pad upon which the user of the card presses with a finger
26 for obtaining a fingerprint of the user scans the

1 fingerprint of the user, and suitable means compares the
2 fingerprint of the user to the fingerprint on the card
3 and to a fingerprint of the owner of the card in the
4 database to ensure authorized use of the card. The
5 apparatus withholds the card from the user if the
6 fingerprint scanned by the fingerprint scanning device
7 does not match the fingerprints on the card and in the
8 database. Thus, upon matching the user's fingerprint to
9 the fingerprints on the card and in the database for
10 ensuring the user of the card is the owner of the card,
11 the apparatus allows the user to use the card for a
12 desired purpose.

13 Other objects, features and advantages of the
14 invention shall become apparent as the description
15 thereof proceeds when considered in connection with the
16 accompanying illustrative drawings.

17

18 **Brief Description of the Drawings:**

19 In the drawings which illustrate the best mode
20 presently contemplated for carrying out the present
21 invention:

22 Fig. 1 is a flow chart illustrating a method for
23 verifying an authorized user of a credit and/or
24 identification card of the present invention;

25 Fig. 2 is a block diagram of an apparatus for
26 carrying out the method of the present invention;

1 Fig. 3 is a credit card of the present invention;
2 and

3 Fig. 4 illustrates the reverse side of the credit
4 card shown in Fig. 3.

5 Corresponding reference numerals designate
6 corresponding parts throughout the several views of the
7 drawings.

8

9 **Detailed Description of the Preferred Embodiment:**

10 Referring now to the drawings, there is generally
11 indicated at 10 a method (illustrated in Fig. 1) for
12 verifying the authorized user of a credit and/or
13 identification card (illustrated in Fig. 3), generally
14 indicated at 12. Preferably, the card 12 should include
15 a surface 14 having at least one fingerprint 18 imprinted
16 thereon of the owner of the card 12. The card preferably
17 has a reverse side 15 (Fig. 4) which has an information
18 strip 16 such as a bar code or magnetic strip, imprinted
19 thereon which has information germane to the owner of the
20 card, such as an identification number and other personal
21 data. The information strip 16 and fingerprint 18 may be
22 imprinted directly onto the card 12 and protected by any
23 suitable laminate as is well-known in the art. As
24 illustrated in Fig. 3, the card 12 has two fingerprints
25 18 of the owner of the card imprinted on surface 14. The
26 card 12 may also include other information, such as a

1 photograph 20 of it's owner and the name and address of
2 the owner. It should be understood that the method 10
3 of the present invention is applicable to any situation
4 where it is desired to verify or authenticate that the
5 user of the card 12 is the owner of the card. The method
6 of the present invention is especially suited to
7 verifying users of credit cards. The method 10 may also
8 be used to verify the identity of authorized persons
9 desiring access to a restricted area (e.g., hospitals,
10 corporate research facilities, etc.). Fig. 2 illustrates
11 an apparatus generally indicated at 22, for carrying out
12 the method of the present invention, the apparatus 22
13 being described in detail after the description of the
14 method 10 of the present invention.

15 Referring now to Fig. 1, method 10 initially
16 comprises the step of inserting the card 12 into an
17 apparatus, such as apparatus 22, having a plurality of
18 scanning stations, namely an information strip scanning
19 station 30, a graphic scanning station 32, a fingerprint
20 scanning station 34, a voice print recording station 36,
21 a retinal scanning station 38, and a photograph scanning
22 station 40. As will be described in greater detail
23 below, the apparatus 22 may embody any number of designs,
24 so long as it is capable of performing the respective
25 verification steps of the method 10.

1 After being inserted into the apparatus 22, the card
2 12 enters an information strip scanning station 30 for
3 scanning the strip 16 of the card 12 to verify the
4 information of the card 12 including the identification
5 number. This information is sent to a microprocessor 42
6 (Fig. 2) which compares the information stored on the
7 information strip 16, to include the card owner's
8 identification number, to information of the owner stored
9 on at least one accessible database 44 (Fig. 2) in
10 communication with the microprocessor 42 of the apparatus
11 22. In order to insure complete security of data
12 transmissions between the apparatus and the database,
13 both the apparatus and database preferably include
14 encryption devices for encrypting and decrypting data
15 transmission. If the information on the strip 16 of the
16 card 12 matches the information stored in the database 44
17 for that particular card, the card 12 is examined by the
18 next station (i.e., the graphic scanning station 32).
19 However, the apparatus 22 withholds the card 12 from the
20 user if the information on the card does not match the
21 information germane to the owner of the card which is
22 stored in the database 44. The card 12, if confiscated,
23 may be stored in any suitable compartment of the
24 apparatus 22 until the apparatus is serviced in which the
25 cards 12 presented by unauthorized users and confiscated
26 by the apparatus 22 may be properly addressed.

1 Next, the card 12 is examined by a graphic scanning
2 32 station in which the surface 14 of the card 12 is
3 digitized by imaging every line thereof. The purpose of
4 examining the surface 14 of the card 12 is to determine
5 whether it has been altered. The image of the surface 14
6 of the card 12 is converted to a digital numeric sequence
7 which is sent to the microprocessor 42 which compares the
8 digital numeric sequence of representing the surface of
9 the card to information directed to a prior scan of the
10 card which is stored on the aforementioned database 44 or
11 another accessible database in communication with the
12 microprocessor 42 of the apparatus 22. If the digital
13 numeric sequence of the card 12 matches the digital
14 numeric sequence stored in the database for that
15 particular card, the card 12 is examined by the next
16 station. However, the apparatus 22 withholds the card 12
17 from the user if the digital numeric sequence of the card
18 does not match the digital numeric sequence which is
19 stored in the database 44. As with the information
20 scanning station 30, the card 12 may be stored in any
21 suitable compartment of the apparatus 22 until the
22 apparatus is serviced in which the cards presented by
23 unauthorized users and confiscated by the apparatus may
24 be properly addressed.

25 As illustrated in Fig. 1, the card 12 is next
26 examined by a fingerprint scanning station 34. This step

1 of the method 10 of the present invention requires the
2 user of the card 12 to provide a fingerprint 18 which is
3 compared to the fingerprint 18 on the card 12 and to a
4 fingerprint of the owner of the card in the
5 aforementioned database 44, or a separate accessible
6 database in communication with the microprocessor 42 of
7 the apparatus 22, to ensure authorized use of the card
8 12. As with the information strip and graphic scanning
9 stations 30, 32, the apparatus 22 withholds the card 12
10 from the user if the fingerprint scanned by the
11 fingerprint scanning station does not match the
12 fingerprints on the card and in the database 44. If the
13 fingerprint of the user matches the fingerprints on the
14 card 12 and in the database 44, the apparatus 22 may
15 allow the user to use the card 12 for a desired purpose,
16 or, as illustrated in Fig. 1, the card 12 may be examined
17 by subsequent stations if a more exacting level of
18 verification is required.

19 In the event that the user does not match the
20 fingerprint 18 on the card 12 or the fingerprint of the
21 owner of the card as stored in the database 44, the
22 method of the present invention further includes the step
23 of recording the fingerprint of the user. The purpose of
24 this additional step is to obtain evidence which could
25 possibly be used to identify the unauthorized user of the
26 card. The recorded fingerprint of the unauthorized user

1 could be compared to fingerprints stored in other
2 databases, such as criminal file databases, employee
3 databases, etc.

4 As mentioned above, if additional verification is
5 necessary, the card 12 may be examined by the voice print
6 recording station 36, the retinal scanning station 38 and
7 the photograph scanning station 40. It should be
8 understood that any of these additional scanning steps
9 may be performed separately, or in any combination, and
10 still fall within the scope of the present invention.

11 Referring still to Fig. 1, the method 10 of the
12 present invention may require the user of the card 12 to
13 speak into a voice print recording station 36 of the
14 apparatus 22 for obtaining a voice print of the user.
15 This voice print is digitized and sent to the
16 microprocessor 42 where it is compared to a voice print
17 of the owner of the card 12 which is stored in the
18 database 44, or a separate accessible database in
19 communication with the microprocessor 42. As with the
20 other stations, if the voice print of the user does not
21 match the voice print of the owner stored in the database
22 44, the apparatus 22 withholds the card 12 until it is
23 properly disposed of. Otherwise, the apparatus 22 may
24 allow the user to use the card 12 for a desired purpose,
25 or the card 12 may be examined by subsequent stations if
26 a more exacting level of verification is required.

1 Accordingly, method 10 also may require the user of
2 the card 12 to look into a retinal scanning station 38 of
3 the apparatus 22 for obtaining a retinal print of the
4 user. This retinal print is then sent to the
5 microprocessor 42 where it is compared to a retinal print
6 of the owner of the card which is stored in the database
7 44, or a separate accessible database in communication
8 with the microprocessor 42. As with the other stations,
9 if the retinal print of the user does not match the
10 retinal print of the owner stored in the database 44, the
11 apparatus 22 confiscates the card. If the retinal print
12 of the user matches the retinal print of the owner stored
13 in the database 44, the apparatus 22 may allow the user
14 to use the card 12 for a desired purpose, or the card 12
15 may be examined by subsequent photograph scanning station
16 40.

17 At the photograph scanning station 40, the
18 photograph 20 on the card 12 is scanned and compared to
19 a photograph of the owner of the card which is stored in
20 the database 44 for additionally ensuring that the card
21 12 has not been tampered with. This scanning station 40
22 is preferably more sensitive than the graphic scanning
23 station 32, since the latter is designed to locate the
24 various components of the card 12 rather than the details
25 of the photograph of the owner. Thus, if the photograph
26 20 of the owner of the card 12 has been replaced by a

1 photograph of the user, and the card passes through the
2 graphic scanning station 32 without being confiscated,
3 the microprocessor 42 will recognize that the photographs
4 do not match whereby the apparatus 22 confiscates the
5 card 12 from the user. If the photographs do match, the
6 apparatus will allow the user to use the card for a
7 desired purpose and the verification process is complete.

8 Turning now to Fig. 2, there is illustrated the
9 apparatus 22 of the present invention which comprises an
10 information scanning device 50, a graphic scanning device
11 52, a fingerprint scanning device 54, a microphone 56 and
12 means 58 for digitizing a person's voice, a retinal
13 scanning device 60 and a photograph scanning device 62.
14 The microprocessor 42 obtains the information gathered by
15 these devices and compares it to information stored on
16 the database 44, or, as mentioned above, a plurality of
17 separate databases in communication with the
18 microprocessor 42. The apparatus 22 and databases 44
19 preferably include encryption devices 63 for encrypting
20 and decrypting data transmissions therebetween. The
21 encryption devices 63 effectively prevent someone from
22 tapping into the telephone lines to illegally steal or
23 copy the digital transmissions during the verification
24 process. Encryption devices 63 of the type contemplated
25 are manufactured by Datotek, Inc. of Dallas, TX. The
26 apparatus 22 may embody different forms, however, it is

1 envisioned that it would be constructed similarly to an
2 automatic teller machine ("ATM") or the like which is
3 designed to receive and process cards.

4 More specifically, the information strip scanning
5 device 50 is provided for scanning a bar code or magnetic
6 strips of the card 12. As illustrated, the
7 microprocessor 42 includes means 64 for comparing the
8 information contained in the strip 16 of the card 12 (to
9 include the card owner's identification number) to
10 information of the owner stored on the database 44. If
11 the information on the card 12 does not match the
12 information of the database 44, the apparatus 22
13 confiscates the card 12. The information strip scanning
14 device 50 may be any of the commercially available
15 scanners for scanning bar codes, such as a scanner sold
16 by Symbol Technologies, Inc., Bohemia, NY under the model
17 no. PDF 417.

18 The graphic scanning device 52 scans surface 14 of
19 the card 12 for determining whether the card 12 has been
20 physically altered. A converter 66 (broadly "converting
21 means") is provided for converting the image of the
22 surface 14 of the card 12 to a digital numeric sequence.
23 This digital numeric sequence is sent to the
24 microprocessor 42 which further includes means 68 for
25 comparing the surface 14 of the card 12 as scanned by the
26 graphic scanning device 52 and converted to a digital

1 numeric sequence by the converter 66 to a digital numeric
2 sequence stored in the database 44 (or in another
3 database in communication with the microprocessor 42) for
4 determining whether the card 12 has been tampered with.
5 If the digital numeric sequence which represents the
6 surface 14 of the card 12 does not match the digital
7 numeric sequence of the of the database 44, the apparatus
8 22 withholds the card 12. The graphic scanning device 52
9 and converter 66 may be any of the commercially available
10 graphic scanners and converters, such as a scanner
11 manufactured by Hewlett-Packard Corporation of
12 California.

13 The fingerprint scanning device 54 has a pad (not
14 shown) upon which the user of the card 12 presses with a
15 finger for obtaining a fingerprint of the user. The
16 fingerprint scanning device 54 scans the fingerprint of
17 the user as obtained by the pad and sends it to the
18 microprocessor 42 which includes means 70 for comparing
19 the fingerprint of the user to the fingerprint 18 on the
20 card 12 and to a fingerprint of the owner of the card in
21 the database 44. If the fingerprint 18 of the user of
22 the card does not match the fingerprint 18 on the card 12
23 or the fingerprint in the database 44, the apparatus 22
24 withholds the card.

25 The fingerprint scanning device 54 may also include
26 a recording feature (not shown) in which the fingerprint

1 of the unauthorized user is recorded for later use, such
2 as comparing it to fingerprints in other databases. This
3 recording feature would assist in the apprehension of the
4 unauthorized user.

5 The fingerprint scanning device 54 may be any of the
6 commercially available fingerprint scanning systems, such
7 as a fingerprint scanner sold by Electronic Data Systems
8 Corp., Dallas, TX or the fingerprint scanners disclosed
9 in the Löffberg and Hiramatsu patents.

10 The apparatus 22 described thus far is capable of
11 achieving the method 10 of the present invention, i.e.,
12 capable of comparing the information on the strip 16 of
13 the card 12 to information about the owner on the
14 database 44, determining whether the card 12 has been
15 altered, and comparing the fingerprint of the user with
16 the fingerprint 18 on the card 12 and the fingerprint in
17 the database 44. The apparatus 22 may further include
18 the aforementioned microphone 56 and associated means 58
19 for recording the user's voice, the retinal scanning
20 device 60 and the photograph scanning device 62 for
21 increasing the level of verification. It should be
22 understood that the apparatus 22 may include each of
23 these additional devices or any combination thereof,
24 depending upon the desired level of verification.

25 The microphone 56 is for receiving the user's voice
26 when the user speaks therein. A recorder 58 (broadly

1 "means for recording") records the user's voice after the
2 user has spoken into the microphone 56 and converts the
3 analog signals to digital signals for obtaining a voice
4 print of the user. The voice print is sent to the
5 microprocessor 42 which includes means 72 for comparing
6 the voice print of the user to a voice print of the owner
7 of the card which is stored in the database 44, or in
8 another accessible database. If the voice print of the
9 user of the card 12 does not match the voice print in the
10 database 44, the apparatus 22 confiscates the card 12
11 from the user. The microphone 56, recorder 58, and voice
12 recognition software may comprise any of the commercially
13 available voice recognition systems, such as a voice
14 recognition system sold by Texas Instruments of Dallas,
15 TX.

16 The retinal scanning device 60 is for obtaining a
17 retinal print of the user after the user looks into the
18 retinal scanning device 60. The retinal print is sent to
19 the microprocessor 42 which includes means 74 for
20 comparing the retinal print of the user to a retinal
21 print of the owner of the card 12 which is stored in the
22 database 44, or in another accessible database. If the
23 retinal print of the user of the card 12 does not match
24 the retinal print in the database 44, the apparatus 22
25 withholds the card 12 from the user. The retinal

1 scanning device 60 may be purchased from Ophthalmic
2 Imaging Systems, Inc. of Sacramento, CA.

3 Lastly, apparatus 22 includes the photograph
4 scanning device 62 which is for scanning the photograph
5 20 on the card 12. This scanning device 62 is preferably
6 more sensitive than the graphic scanning device 54, since
7 the latter is designed to locate the main components of
8 the card rather than details of the photograph of the
9 card's owner. This information is sent to the
10 microprocessor 42 which includes means 76 for comparing
11 the photograph 20 as scanned by the scanning device 62 to
12 a photograph of the owner of the card 12 which is stored
13 on the database 44, or on another accessible database,
14 for ensuring that the card 12 has not been tampered with,
15 namely, that the photograph 20 has not been replaced by
16 the photograph of the user. If the photograph 20 on the
17 card 12 does not match the photograph in the database 44,
18 the apparatus 22 withholds the card from the user. The
19 photograph scanning device 62 may also be purchased from
20 Hewlett-Packard Corporation.

21 The microprocessor 42 of the apparatus 22 may be
22 chosen from any of the commercially available
23 microprocessors wherein the software may comprise a
24 menuing system such as a system designed by Galacticom,
25 Inc. of Ft. Lauderdale, FL. It is envisioned that this
26 menuing system, when authorized use of the card is

1 verified, enables the card's user to choose from many
2 options such as credit, banking, money transfer, hospital
3 or health care authorization etc. In this connection,
4 the software may also be designed for a single-purpose
5 use. For example, a hospital may require health care
6 authorization before admission or treatment. The system
7 software could be specifically designed to access and
8 store appropriate data for billing, such as date, type of
9 treatment, location of the facility etc. Other single-
10 purpose applications, such as bank ATM's would access and
11 store different information germane to the purpose. It
12 is also contemplated that a machine code number and
13 location could be coded in a bar code format and affixed
14 inside the apparatus, wherein a separate bar code reader
15 (not shown) would read the bar code and store that
16 information with other information germane to each card
17 transaction.

18 It should be observed that the method 10 and
19 apparatus 22 of the present invention are capable of
20 verifying the authorized user of a credit/identification
21 card, and of determining whether the card has been
22 altered.

23 While there is shown and described herein certain
24 specific structure embodying the invention, it will be
25 manifest to those skilled in the art that various
26 modifications and rearrangements of the parts may be made

1 without departing from the spirit and scope of the
2 underlying inventive concept and that the same is not
3 limited to the particular forms herein shown and
4 described except insofar as indicated by the scope of the
5 appended claims.



THIS SHEET HAS BEEN
REPLACED

Claims

WHAT IS CLAIMED IS:

- 1 1. A method for verifying an authorized user of a
2 credit/identification card comprising the steps of:
3 inserting the card into an apparatus having a
4 plurality of scanning stations, the card including a
5 surface having a strip thereon which has information
6 germane to the owner of the card, such as an
7 identification number and other personal data, and at
8 least one fingerprint thereon of the owner of the card;
9 scanning the strip of the card at an information
10 strip scanning station of said apparatus for verifying
11 the information of the card including the identification
12 number;
13 comparing the information stored on the strip of the
14 card to information of the owner stored on at least one
15 accessible database in communication with said apparatus,
16 the apparatus withholding the card from the user if the
17 information on the card does not match the information
18 germane to the owner of the card which is stored in the
19 database;
20 scanning the surface of the card at a graphic
21 scanning station of said apparatus which digitizes the
22 surface of the card by imaging every line thereof;



THIS SHEET HAS BEEN
REPLACED

24

This Sheet Has Been Replaced



23 converting the image of the surface of the card to
24 a digital numeric sequence;

25 comparing the surface of the card as scanned by said
26 graphic scanning device and converted to a digital
27 numeric sequence to a digital numeric sequence stored in
28 said database for determining whether the card has been
29 tampered with, the apparatus withholding the card from
30 the user if the surface of the card does not match the
31 surface of the card stored by the database;

32 obtaining a fingerprint of the user;

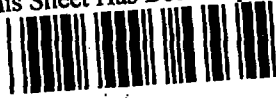
33 scanning the fingerprint of the user at a
34 fingerprint scanning station; and

35 comparing the fingerprint of the user to said
36 fingerprint on the card and to a fingerprint of the owner
37 of the card in the database to ensure authorized use of
38 the card, the apparatus withholding the card from the
39 user if the fingerprint scanned by the fingerprint
40 scanning device does not match the fingerprints on the
41 card and in the database; whereby, upon matching the
42 user's fingerprint to the fingerprints on the card and in
43 the database for ensuring the user of the card is the
44 owner of the card, said apparatus allowing the user to
45 use the card for a desired purpose,

46 said method further comprising the step of recording
47 the fingerprint of the user of the card in the event the



This Sheet Has Been Replaced



25

THIS SHEET HAS BEEN
REPLACED

48 fingerprint of the user does not match the fingerprint on
49 the card or the fingerprint of the owner of the card.

1 2. The method as set forth in claim 1 further
2 comprising the steps of:

3 requiring the user of the card to speak into a
4 microphone of the apparatus for obtaining a voice print
5 of the user; and

6 comparing the user's voice print to a voice print of
7 the owner of the card which is stored in the database,
8 the apparatus withholding the card from the user if the
9 user's voice does not match the voice print of the owner
10 stored in the database.

1 3. The method as set forth in claim 2 further
2 comprising the steps of:

3 obtaining a retinal print of the user at a retinal
4 scanning station; and

5 comparing the user's retinal print to a retinal
6 print of the owner of the card which is stored in the
7 database, the apparatus withholding the card from the
8 user if the user's retinal print does not match the
9 retinal print of the owner stored in the database.

1 4. The method as set forth in claim 3 further
2 comprising the steps of:



* C L M S *

THIS SHEET HAS BEEN
REPLACED

26

This Sheet Has Been Replaced



3 scanning a photograph of the user on the card at a
4 photograph scanning station;

5 comparing the photograph as scanned by the
6 photograph scanning station to a photograph of the owner
7 of the card which is stored on the database for ensuring
8 that the card has not been tampered with, the apparatus
9 withholding the card from the user if the photograph on
10 the card does not match the photograph stored in the
11 database.

1 5. The method as set forth in claim 1 further
2 comprising the steps of:

3 obtaining a retinal print of the user at a retinal
4 scanning station; and

5 comparing the user's retinal print to a retinal
6 print of the owner of the card which is stored in the
7 database, the apparatus withholding the card from the
8 user if the user's retinal print does not match the
9 retinal print of the owner stored in the database.

1 6. The method as set forth in claim 1 further
2 comprising the steps of:

3 scanning a photograph of the user on the card at a
4 photograph scanning station; and

5 comparing the photograph as scanned by the
6 photograph scanning station to a photograph of the owner



* C L N S *



THIS SHEET HAS BEEN
REPLACED

7 of the card which is stored on the database for ensuring
8 that the card has not been tampered with, the apparatus
9 withholding the card from the user if the photograph on
10 the card does not match the photograph stored in the
11 database.

1 7. An apparatus for verifying an authorized user of a
2 credit/identification card including a surface having a
3 strip thereon which has information germane to the owner
4 of the card, such as an identification number and other
5 personal data, and at least one fingerprint thereon of
6 the owner of the card, said apparatus comprising:

7 an information strip scanning device for scanning
8 the information strip of the card;

9 means for comparing the information contained in the
10 strip to information of the owner stored on at least one
11 accessible database in communication with said apparatus,
12 the apparatus withholding the card from the user if the
13 information on the card does not match the information
14 germane to the owner of the card which is stored in the
15 database;

16 a graphic scanning device for scanning the surface
17 of the card, said graphic scanning device digitizing the
18 surface of the card by imaging every line thereof;

19 means for converting the image of the surface of the
20 card to a digital numeric sequence;



THIS SHEET HAS BEEN
REPLACED

28

This Sheet Has Been Replaced



means for comparing the surface of the card as scanned by said graphic scanning device and converted to a digital numeric sequence by said converting means to a digital numeric sequence stored in said database for determining whether the card has been tampered with, the apparatus withholding the card from the user if the surface of the card does not match the surface of the card stored by the database;

a fingerprint scanning device having a pad upon which the user of the card presses with a finger for obtaining a fingerprint of the user, said fingerprint scanning device scanning the fingerprint of the user; and

means for comparing the fingerprint of the user to said fingerprint on the card and to a fingerprint of the owner of the card in the database to ensure authorized use of the card, the apparatus withholding the card from the user if the fingerprint scanned by the fingerprint scanning device does not match the fingerprints on the card and in the database; whereby, upon matching the user's fingerprint to the fingerprints on the card and in the database for ensuring the user of the card is the owner of the card, said apparatus allowing the user to use the card for a desired purpose,

said apparatus further comprising means for recording the fingerprint of the user of the card in the event the fingerprint of the user does not match the



* C L M S *

THIS SHEET HAS BEEN
REPLACED

47 fingerprint on the card or the fingerprint of the owner
48 of the card.

1 8. The apparatus as set forth in claim 7 further
2 comprising:

3 a microphone;

4 means for recording the user of the card's voice
5 after the user has spoken into the microphone for
6 obtaining a voice print of the user; and

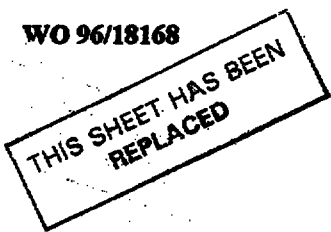
7 means for comparing the user's voice print to a
8 voice print of the owner of the card which is stored in
9 the database, the apparatus withholding the card from the
10 user if the user's voice does not match the voice print
11 of the owner stored in the database.

1 9. The apparatus as set forth in claim 8 further
2 comprising:

3 a retinal scanning device for obtaining a retinal
4 print of the user after the user looks into the retinal
5 scanning device; and

6 means for comparing the user's retinal print to a
7 retinal print of the owner of the card which is stored in
8 the database, the apparatus withholding the card from the
9 user if the user's retinal print does not match the
10 retinal print of the owner stored in the database.





This Sheet Has Been Replaced



1 10. The apparatus as set forth in claim 9 further
2 comprising:

3 a scanning device for scanning a photograph of the
4 user on the card; and

5 means for comparing the photograph as scanned by the
6 scanning device to a photograph of the owner of the card
7 which is stored on the database for ensuring that the
8 card has not been tampered with, the apparatus
9 withholding the card from the user if the photograph on
10 the card does not match the photograph stored in the
11 database.

1 11. The apparatus as set forth in claim 9 further
2 comprising:

3 a scanning device for scanning a photograph of the
4 user on the card; and

5 means for comparing the photograph as scanned by the
6 scanning device to a photograph of the owner of the card
7 which is stored on the database for ensuring that the
8 card has not been tampered with, the apparatus
9 withholding the card from the user if the photograph on
10 the card does not match the photograph stored in the
11 database, said voice print, retinal print and photograph
12 comparing means comprising a microprocessor.



* C L M S *



THIS SHEET HAS BEEN
REPLACED

1 12. The apparatus as set forth in claim 7 further
2 comprising:

3 a retinal scanning device for obtaining a retinal
4 print of the user after the user looks into the retinal
5 scanning device; and

6 means for comparing the user's retinal print to a
7 retinal print of the owner of the card which is stored in
8 the database, the apparatus withholding the card from the
9 user if the user's retinal print does not match the
10 retinal print of the owner stored in the database.

1 13. The apparatus as set forth in claim 7 further
2 comprising:

3 a scanning device for scanning a photograph of the
4 user on the card; and

5 means for comparing the photograph as scanned by the
6 scanning device to a photograph of the owner of the card
7 which is stored on the database for ensuring that the
8 card has not been tampered with, the apparatus
9 withholding the card from the user if the photograph on
10 the card does not match the photograph stored in the
11 database.

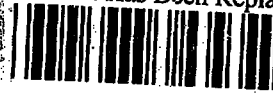
1 14. The apparatus as set forth in claim 7 further
2 comprising an encryption device for encrypting and
3 decrypting data transmissions between said apparatus and



THIS SHEET HAS BEEN
REPLACED

32

This Sheet Has Been Replaced



4 said database, said database including a corresponding
5 encryption device.

1 15. A method of verifying an authorized user of a
2 credit/identification card comprising the steps of:

3 reading an information strip on the card, said
4 information strip having information germane to the owner
5 of the card;

6 comparing said information to a corresponding set of
7 information stored in a remote database, whereby said
8 card is withheld if said information does not match said
9 corresponding set of information stored in the remote
10 database;

11 obtaining a digitized image of a surface of said
12 card;

13 comparing said obtained digitized image of said card
14 to a corresponding digitized image of said card stored in
15 said remote database, whereby said card is withheld if
16 said obtained digitized image does not match said
17 corresponding digitized image stored in said remote
18 database;

19 obtaining an image of a physical attribute of the
20 user of the card;

21 comparing said obtained image of said physical
22 attribute of said user to a corresponding image of said
23 physical attribute of said owner stored in said remote



* C L H S *



24 database, whereby said card is withheld if said obtained
25 image of said physical attribute does not match said
26 stored image of said physical attribute, and further
27 whereby said obtained image of said physical attribute is
28 recorded if said obtained image of said physical
29 attribute does not match said stored image of said
30 physical attribute, said user being allowed to conduct a
31 desired electronic transaction if said obtained image of
32 said physical attribute of said user matches said stored
33 image of said physical attribute of said owner.

1 16. The method of claim 15 wherein said physical
2 attribute comprises a fingerprint.

1 17. The method of claim 15 wherein said physical
2 attribute comprises a voice print.

1 18. The method of claim 15 wherein said physical
2 attribute comprises a retinal print.

1 19. The method of claim 16 further comprising the step
2 of obtaining an image of a second physical attribute of
3 said user, and comparing said obtained image of said
4 second physical attribute of said user to a corresponding
5 image of a second physical attribute of said owner stored
6 in said remote database, whereby said card is withheld if



THIS SHEET HAS BEEN
REPLACED

34

This Sheet Has Been Replaced



7 said obtained image of said second physical attribute
8 does not match said corresponding stored image of said
9 second physical attribute, and further whereby said
10 obtained image of said second physical attribute is
11 recorded if said obtained image of said second physical
12 attribute does not match said corresponding stored image
13 of said second physical attribute, said user being
14 allowed to conduct a desired electronic transaction if
15 said obtained image of said second physical attribute of
16 said user matches said stored image of said second
17 physical attribute of said owner.

1 20. The method of claim 19 wherein said second physical
2 attribute comprises a voice print.

1 21. The method of claim 19 wherein said second physical
2 attribute comprises a retinal print.

1 22. The method of claim 15 further comprising the step
2 of encrypting transmissions of said information to and
3 from said remote database.

1 23. Apparatus for verifying an authorized user of a
2 credit/identification card comprising:



* C L M S *

This Sheet Has Been Replaced



35

THIS SHEET HAS BEEN
REPLACED

3 means for reading an information strip on said card,
4 said information strip having information germane to the
5 owner of the card;

6 means for communicating with a remote database
7 having corresponding set of information germane to said
8 owner of said card;

9 means for comparing said information to said
10 corresponding set of information stored in said remote
11 database, said card being withheld by said apparatus if
12 said information does not match said corresponding set of
13 information stored in the remote database;

14 means for obtaining a digitized image of a surface
15 of said card;

16 means for comparing said obtained digitized image of
17 said card to a corresponding digitized image of said card
18 stored in said remote database, said card being withheld
19 by said apparatus if said obtained digitized image does
20 not match said corresponding digitized image stored in
21 said remote database;

22 means for obtaining an image of a physical attribute
23 of the user of the card;

24 means for comparing said obtained image of said
25 physical attribute of said user to a corresponding image
26 of said physical attribute of said owner stored in said
27 remote database, said card being withheld by said
28 apparatus if said obtained image of said physical



THIS SHEET HAS BEEN
REPLACED

36

This Sheet Has Been Replaced



29 attribute does not match said stored image of said
30 physical attribute; and

31 means for recording said obtained image of said
32 physical attribute if said obtained image of said
33 physical attribute does not match said stored image of
34 said physical attribute, said user being allowed to
35 conduct a desired electronic transaction if said obtained
36 image of said physical attribute of said user matches
37 said stored image of said physical attribute of said
38 owner.

1 24. The apparatus of claim 23 wherein said physical
2 attribute of said user comprises a fingerprint.

1 25. The apparatus of claim 23 wherein said physical
2 attribute of said user comprises a voice print.

1 26. The apparatus of claim 23 wherein said physical
2 attribute of said user comprises a retinal print.

1 27. The apparatus of claim 24 further comprising means
2 for obtaining an image of a second physical attribute of
3 said user, and means for comparing said obtained image of
4 said second physical attribute of said user to a
5 corresponding image of a second physical attribute of
6 said owner stored in said remote database, said card



THIS SHEET HAS BEEN
REPLACED

7 being withheld if said obtained image of said second
8 physical attribute does not match said corresponding
9 stored image of said second physical attribute, said
10 apparatus still further comprising means for recording
11 said obtained image of said second physical attribute if
12 said obtained image of said second physical attribute
13 does not match said corresponding stored image of said
14 second physical attribute,

15 said user being allowed to conduct a desired
16 electronic transaction if said obtained image of said
17 second physical attribute of said user matches said
18 stored image of said second physical attribute of said
19 owner.

1 28. The apparatus of claim 27 wherein said second
2 physical attribute comprises a voice print.

1 29. The apparatus of claim 27 wherein said second
2 physical attribute comprises a retinal print.

1 30. The apparatus of claim 23 further comprising means
2 for encrypting data transmissions between said apparatus
3 and said remote database.

This Sheet Has Been Replaced



* C L M S *

THIS SHEET HAS BEEN
REPLACED

38

This Sheet Has Been Replaced



1 31. A method for conducting a secure electronic
2 transaction using a credit/identification card comprising
3 the steps of:

4 reading an information strip on the card, said
5 information strip having information germane to the owner
6 of the card;

7 comparing said information to a corresponding set of
8 information stored in a remote database, whereby said
9 card is withheld if said information does not match said
10 corresponding set of information stored in the remote
11 database;

12 obtaining an image of a physical attribute of the
13 user of the card;

14 comparing said obtained image of said physical
15 attribute of said user to a corresponding image of said
16 physical attribute of said owner stored in said remote
17 database, whereby said card is withheld if said obtained
18 image of said physical attribute does not match said
19 stored image of said physical attribute, and further
20 whereby said obtained image of said physical attribute is
21 recorded if said obtained image of said physical
22 attribute does not match said stored image of said
23 physical attribute; and

24 selecting a desired electronic transaction from a
25 predetermined menu system, said user being allowed to
26 conduct a desired electronic transaction if said obtained





THIS SHEET HAS BEEN
REPLACED

27 image of said physical attribute of said user matches
28 said stored image of said physical attribute of said
29 owner.

1 32. The method of claim 31 wherein said physical
2 attribute comprises a fingerprint.

1 33. The method of claim 31 wherein said physical
2 attribute comprises a voice print.

1 34. The method of claim 31 wherein said physical
2 attribute comprises a retinal print.

1 35. The method of claim 32 further comprising the step
2 of obtaining an image of a second physical attribute of
3 said user, and comparing said obtained image of said
4 second physical attribute of said user to a corresponding
5 image of a second physical attribute of said owner stored
6 in said remote database, whereby said card is withheld if
7 said obtained image of said second physical attribute
8 does not match said corresponding stored image of said
9 second physical attribute, and further whereby said
10 obtained image of said second physical attribute is
11 recorded if said obtained image of said second physical
12 attribute does not match said corresponding stored image
13 of said second physical attribute, said user being



THIS SHEET HAS BEEN
REPLACED

This Sheet Has Been Replaced



14 allowed to conduct a desired electronic transaction if
15 said obtained image of said second physical attribute of
16 said user matches said stored image of said second
17 physical attribute of said owner.

1 36. The method of claim 35 wherein said second physical
2 attribute comprises a voice print.

1 37. The method of claim 35 wherein said second physical
2 attribute comprises a retinal print.

1 38. The method of claim 31 further comprising the step
2 of encrypting transmissions of said information to and
3 from said remote database.

1 39. Apparatus for conducting a secure electronic
2 transaction using a credit/identification card
3 comprising:

4 means for reading an information strip on said card,
5 said information strip having information germane to the
6 owner of the card;

7 means for communicating with a remote database
8 having corresponding set of information germane to said
9 owner of said card;

10 means for comparing said information to said
11 corresponding set of information stored in said remote





THIS SHEET HAS BEEN
REPLACED

12 database, said card being withheld by said apparatus if
13 said information does not match said corresponding set of
14 information stored in the remote database;

15 means for obtaining an image of a physical attribute
16 of the user of the card;

17 means for comparing said obtained image of said
18 physical attribute of said user to a corresponding image
19 of said physical attribute of said owner stored in said
20 remote database, said card being withheld by said
21 apparatus if said obtained image of said physical
22 attribute does not match said stored image of said
23 physical attribute; and

24 means for recording said obtained image of said
25 physical attribute if said obtained image of said
26 physical attribute does not match said stored image of
27 said physical attribute, said user being allowed to
28 conduct a desired electronic transaction if said obtained
29 image of said physical attribute of said user matches
30 said stored image of said physical attribute of said
31 owner.

1 40. The apparatus of claim 39 wherein said physical
2 attribute of said user comprises a fingerprint.

1 41. The apparatus of claim 39 wherein said physical
2 attribute of said user comprises a voice print.





1 42. The apparatus of claim 39 wherein said physical
2 attribute of said user comprises a retinal print.

1 43. The apparatus of claim 40 further comprising means
2 for obtaining an image of a second physical attribute of
3 said user, and means for comparing said obtained image of
4 said second physical attribute of said user to a
5 corresponding image of a second physical attribute of
6 said owner stored in said remote database, said card
7 being withheld if said obtained image of said second
8 physical attribute does not match said corresponding
9 stored image of said second physical attribute, said
10 apparatus still further comprising means for recording
11 said obtained image of said second physical attribute if
12 said obtained image of said second physical attribute
13 does not match said corresponding stored image of said
14 second physical attribute,

15 said user being allowed to conduct a desired
16 electronic transaction if said obtained image of said
17 second physical attribute of said user matches said
18 stored image of said second physical attribute of said
19 owner.

1 44. The apparatus of claim 43 wherein said second
2 physical attribute comprises a voice print.



THIS SHEET HAS BEEN
REPLACED

1 45. The apparatus of claim 43 wherein said second
2 physical attribute comprises a retinal print.

1 46. The apparatus of claim 39 further comprising means
2 for encrypting data transmissions between said apparatus
3 and said remote database.

This Sheet Has Been Replaced



* C L M S *

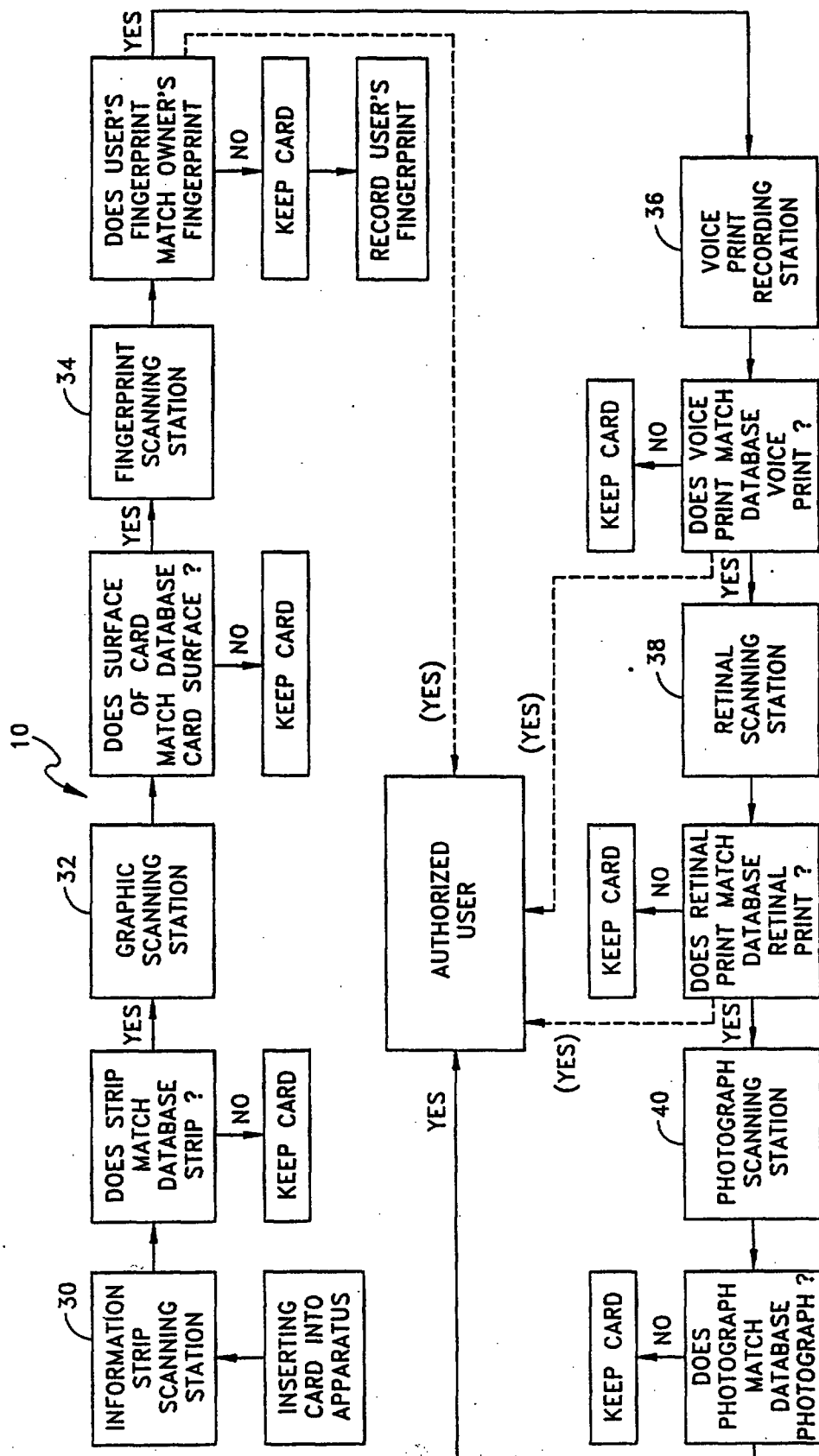


FIG. 1

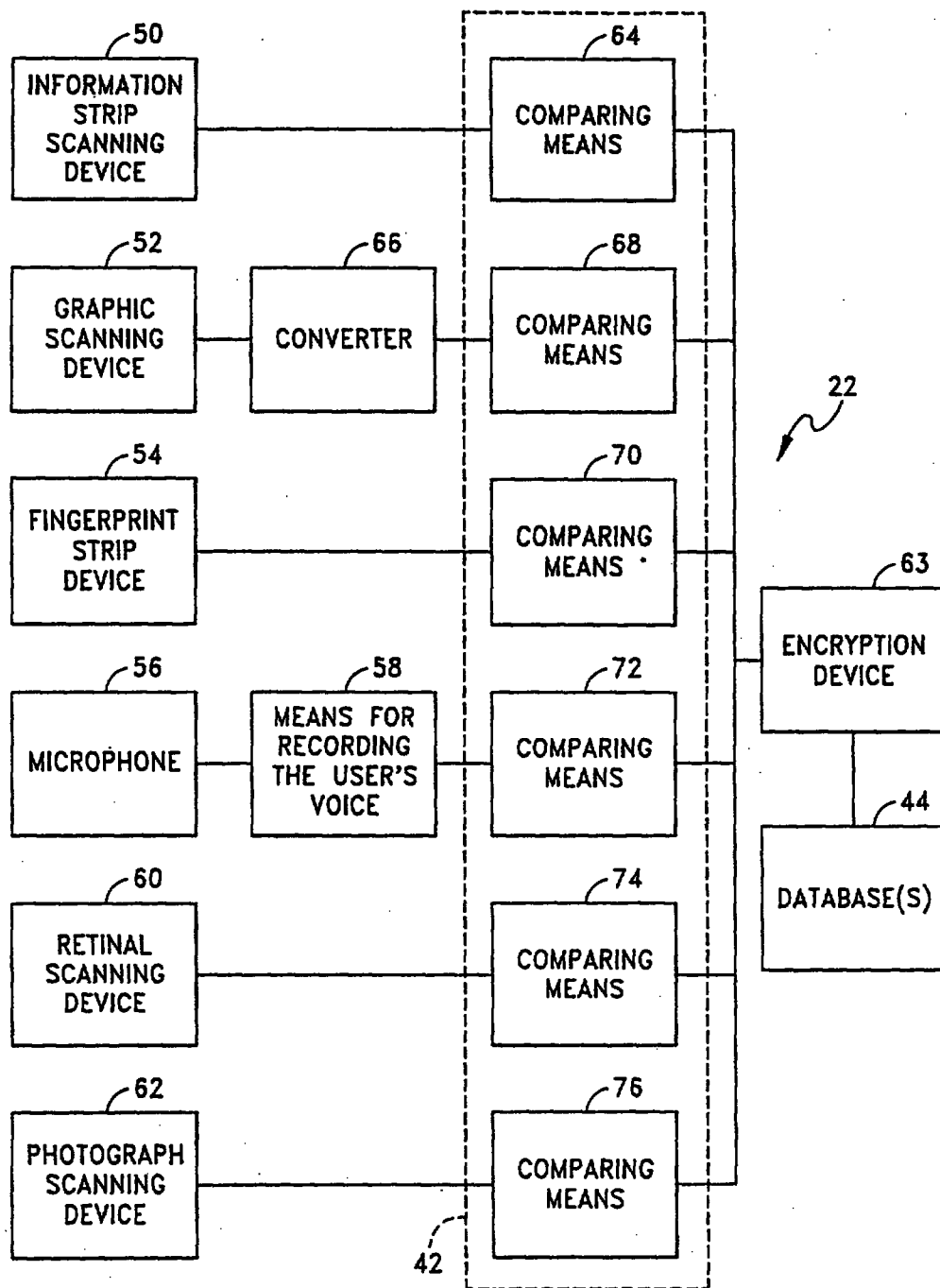
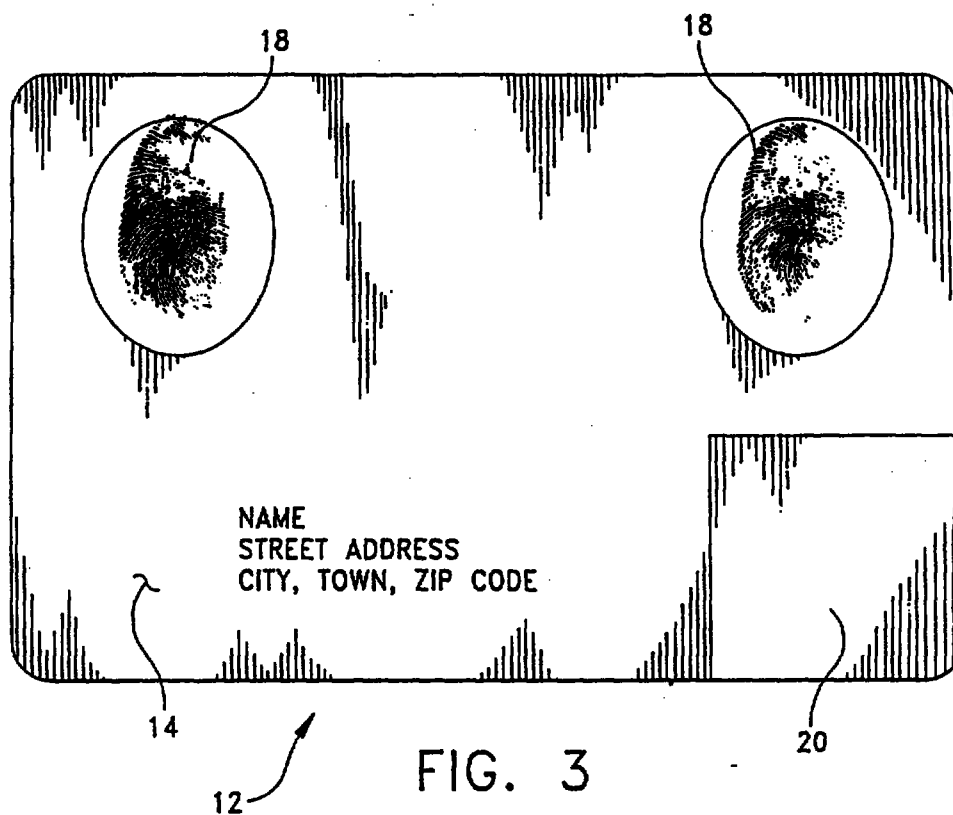
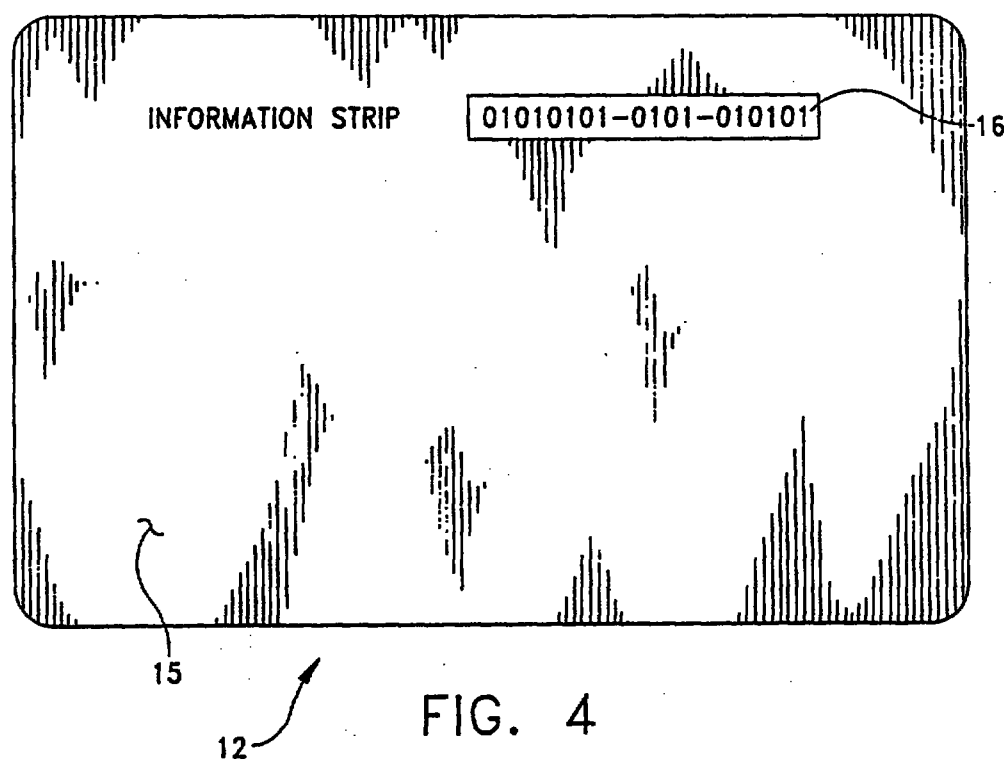
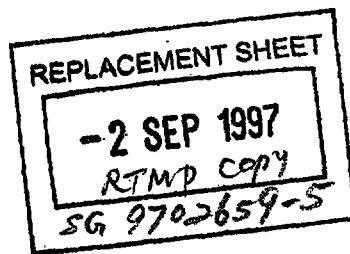


FIG. 2





Substitute sheet -
1 September 1997

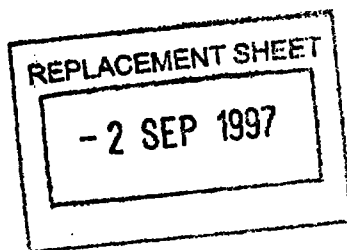
23

Claims

WHAT IS CLAIMED IS:

- 1 1. A method for electronically verifying an
2 authorized user of a credit/identification card
3 comprising the steps of:
4 scanning an information strip of an identification
5 card in a scanning apparatus to obtain an identification
6 code assigned to an owner of the card;
7 locating an information file of the owner stored on
8 a database in communication with said scanning apparatus,
9 said information file being located using said
10 identification code;
11 obtaining an image of a physical attribute of the
12 user of said identification card;
13 comparing said obtained image of the user of the
14 card to an image of a corresponding physical attribute of
15 the owner of the card stored in the information file of
16 the owner of the card to positively identify the user of
17 the card as the owner of the card whereby upon matching
18 the user's image to the owner's corresponding image said
19 user is authorized to use the card for a desired purpose;
20 and
21 recording the image of the user of the card in the
22 event the image of the physical attribute of the user
23 does not match the corresponding image of the
24 corresponding physical attribute of the owner of the card
25 stored in the information file of the owner of the card.
- 1 2. The method as set forth in claim 1 further
2 comprising the steps of obtaining an image of a second
3 physical attribute of the user of said identification
4 card;
5 comparing said second obtained image of the user of
6 the card to a second image of a corresponding physical





Substitute sheet -
1 September 1997

24

7 attribute of the owner of the card stored in the
8 information file to further positively identify the user
9 of the card as the owner of the card whereby upon
10 matching the user's obtained images to the owner's
11 corresponding images said user is authorized to use the
12 card for a desired purpose; and

13 recording the obtained images of the user of the
14 card in the event the images of the physical attributes
15 of the user do not match the corresponding images of the
16 corresponding physical attributes of the owner of the
17 card stored in the information file of the owner of the
18 card.

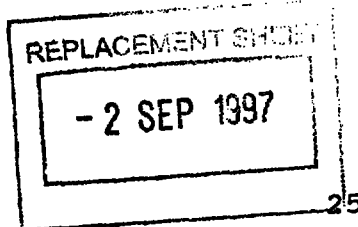
1 3. The method as set forth in claim 1 wherein said
2 step of obtaining an image of a physical attribute of the
3 user comprises obtaining a scanned image of a fingerprint
4 of the user.

1 4. The method as set forth in claim 1 wherein said
2 step of obtaining an image of a physical attribute of the
3 user comprises obtaining a scanned image of a retinal
4 print of the user.

1 5. The method as set forth in claim 1 wherein said
2 step of obtaining an image of a physical attribute of the
3 user comprises obtaining a voice print of the user.

1 6. The method as set forth in claim 1 wherein said
2 step of obtaining an image of a physical attribute of the
3 user comprises obtaining a photographic image of the
4 user's facial features.





Substitute sheet -
1 September 1997

1 7. The method as set forth in claim 2 wherein said
2 steps of obtaining images of physical attributes of the
3 user comprise the steps of obtaining a scanned image of
4 a fingerprint of the user, and obtaining a second image
5 of a retinal print of the user.

1 8. The method as set forth in claim 2 wherein said
2 steps of obtaining images of physical attributes of the
3 user comprise the steps of obtaining a scanned image of
4 a fingerprint of the user, and obtaining a voice print of
5 the user.

1 9. The method as set forth in claim 2 wherein said
2 steps of obtaining images of physical attributes of the
3 user comprise the steps of obtaining a scanned image of
4 a retinal print of the user, and obtaining a voice print
5 of the user.

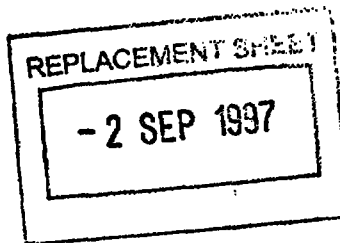
1 10. The method as set forth in claim 1 further
2 comprising the step of encrypting communication of said
3 information to and from said remote database.

1 11. The method as set forth in claim 2 further
2 comprising the step of encrypting communication of said
3 information to and from said remote database.

1 12. The method as set forth in claim 1 further
2 comprising the step of selecting a desired electronic
3 transaction from a predetermined menu system when said
4 user is authorized to use said card.

1 13. An apparatus for verifying an authorized user
2 of a credit/identification card including an information
3 strip thereon which has information germane to the owner





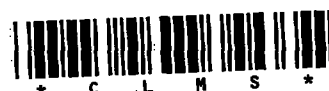
Substitute sheet -
1 September 1997

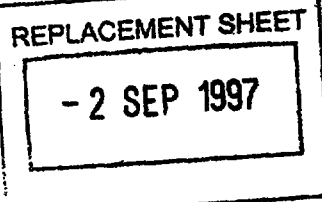
26

4 of the card including an identification code assigned to
5 the owner of the card, said apparatus comprising:
6 a scanning device for scanning the information strip
7 of the card and obtaining said identification code from
8 said information strip;
9 means for communicating with a remote database and
10 for locating an information file on said database which
11 corresponds to said identification code;
12 means for obtaining an image of a physical attribute
13 of the user of the card;
14 means for comparing said obtained image of the user
15 of the card to an image of a corresponding physical
16 attribute of the owner of the card stored in the
17 information file of the owner of the card to positively
18 identify the user of the card as the owner of the card
19 whereby upon matching the user's image to the owner's
20 corresponding image said user is authorized to use the
21 card for a desired purpose; and
22 means for recording the image of the user of the
23 card in the event the image of the physical attribute of
24 the user does not match the corresponding image of the
25 corresponding physical attribute of the owner of the card
26 stored in the information file of the owner of the card.

1 14. The apparatus as set forth in claim 13 wherein
2 said means for obtaining an image of a physical attribute
3 of the user comprises a fingerprint scanning device, and
4 said stored image of a physical attribute of the owner
5 comprises a stored image of a fingerprint of the owner of
6 the card.

1 15. The apparatus as set forth in claim 13 wherein
2 said means for obtaining an image of a physical attribute
3 of the user comprises a microphone for obtaining a voice





Substitute sheet -
1 September 1997

27

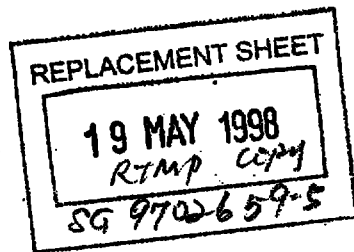
4 print of the user, and said stored image of a physical
5 attribute of the owner comprises a stored voice print of
6 the owner of the card.

1 16. The apparatus as set forth in claim 13 wherein
2 said means for obtaining an image of a physical attribute
3 of the user comprises a retinal scanning device for
4 obtaining a retinal print of the user, and said stored
5 image of a physical attribute of the owner comprises a
6 stored image of a retinal print of the owner of the card.

1 17. The apparatus as set forth in claim 13 wherein
2 said means for obtaining an image of a physical attribute
3 of the user comprises a photo scanning device, and said
4 stored image of a physical attribute of the owner
5 comprises a stored photo image of facial attributes of
6 the owner of the card.

1 18. The apparatus as set forth in claim 13 further
2 comprising an encryption device for encrypting and
3 decrypting data transmissions between said apparatus and
4 said database, said database including a corresponding
5 encryption device.





Substitute sheet
18 May 1998

28

19. A method for electronically verifying the identity of an individual attempting to electronically gain access to a service on a computer system comprising the steps of:

obtaining an identification code assigned to an owner of an account for said service;

locating an information file of said owner stored on a database in communication with said computer system, said information file being located using said identification code;

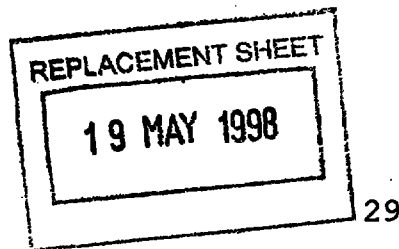
obtaining an image of a physical attribute of said individual;

comparing said obtained image of said individual to an image of a corresponding physical attribute of said owner of said account stored in the information file of the owner of the account to positively identify the individual as the owner of the identification code whereby upon matching the individuals image to the owner's corresponding image said user is authorized to gain access to said service; and

recording the image of the individual in the event the image of the physical attribute of the individual does not match the corresponding image of the corresponding physical attribute of the owner of the identification code stored in the information file of the owner of the account.

20. The method as set forth in claim 19 wherein said step of obtaining an image of a physical attribute of the user comprises obtaining a scanned image of a fingerprint of the user.





Substitute sheet
18 May 1998

29

21. The method as set forth in claim 19 wherein said step of obtaining an image of a physical attribute of the user comprises obtaining a scanned image of a retinal print of the user.

22. The method as set forth in claim 19 wherein said step of obtaining an image of a physical attribute of the user comprises obtaining a voice print of the user.



* C L N S *