

9704135-4
IPAS copy

IC CARD AND PERSONAL DATA IDENTIFYING SYSTEM
OPERATIVE THEREWITH

BACKGROUND OF THE INVENTION

(1) Field of the Invention

The present invention relates to IC cards and personal data identifying systems operative therewith, and more particularly to an IC card which has a high security function of identifying its user by collating user's fingerprint and can be suitably used as a passport or the like, and a personal data checking system operative with the same.

(2) Description of the Related Art

A usual passport is produced by printing user's personal data and applying user's photograph. For entry/departure admission, the admission officer visually collates the contents of such a passport with the person applying for the entry or departure admission.

Since the above conventional passport is produced by printing the personal data and applying the photograph, it can be readily forged, and this is posing a serious current social problem. Besides, since the checking is by way of human eyes, it is not possible to prevent illegal entry/departure completely. Also, since the checking requires time, a smooth entry/departure admission process

THIS SHEET HAS BEEN
REPLACED

- 2 -

This Sheet Has Been Replaced



is desired.

SUMMARY OF THE INVENTION

An object of the invention, therefore, is to overcome the problems existing in the prior art, and to provide an IC card which can realize a passport with a high security function to perfectly prevent forging and permit correct and quick confirmation or identification of the user.

According to one aspect of the invention, there is provided an IC card to be checked by a personal data identifying system for confirming an IC card user by collating a registered fingerprint data and an input fingerprint data, the IC card comprising:

- a fingerprint-related data; and

- a storing means for storing in advance the fingerprint-related data and a personal data.

The fingerprint-related data stored in the storing means is a data for reading out the registered fingerprint data (first embodiment) or a fingerprint data (second embodiment).

The registered fingerprint data is a coded data, and a secret key data for decoding the coded registered fingerprint data is stored in the storing means. The IC card further includes a means for preventing re-writing of the fingerprint-related data and the personal data. Further,

THIS SHEET HAS BEEN
REPLACED

This Sheet Has Been Replaced



- 3 -

the IC card includes personal data for a passport.

According to another aspect of the invention, there is provided a personal data identifying system comprising:

a register means in which a fingerprint data of an individual user is registered;

a reading means for reading out a fingerprint-related data stored in a storing means in an IC card, and reading out the registered fingerprint data from the register means based on the read-out fingerprint-related data; and

a checking means for collating the read-out registered fingerprint data with input fingerprint data and determining identity thereof.

In the above, the register means is accessible from a domestic or foreign spot for collating a user's fingerprint by on-line processing.

In the IC card of the second embodiment, the fingerprint-related data stored in the storing means is a fingerprint data registered in the IC card.

In the above, the registered fingerprint data is a coded data, and a secret key data for decoding the coded registered fingerprint data is stored in the storing means.

The personal data identifying system includes a means to read a fingerprint data stored in an IC card and further includes a checking means for collating the read-out fingerprint data with input fingerprint data and determining

identity thereof. The IC card has personal data for a passport and is used for entry and departure admission purposes.

In the personal data identifying system according to the invention, the IC card has personal data for a passport and is used for entry and departure admission purposes.

BRIEF DESCRIPTION OF THE DRAWINGS

The above and other objects, features and advantages of the present invention will be apparent from the following description of preferred embodiments of the invention explained with reference to the accompanying drawings, in which:

Fig. 1 is a block diagram showing an IC passport according to the invention;

Fig. 2 is a block diagram showing an overall IC passport identifying system according to the invention;

Fig. 3 is a block diagram showing an IC passport checking system of a first embodiment according to the invention; and

Fig. 4 is a block diagram showing an IC passport checking system of a second embodiment according to the invention.

PREFERRED EMBODIMENT OF THE INVENTION

Now, a preferred embodiment of the invention is explained with reference to the drawings.

Fig. 1 is a block diagram showing an embodiment of the IC card according to the invention. The IC card 1 comprises a CPU (Central Processing Unit) 11, a RAM (Random Access Memory) 12, a ROM (Read-Only Memory) 13, an I/O (Input/Output interface) 14, and an internal bus 15 interconnecting these elements. All the elements 11 to 15 are provided in a single integrated circuit chip.

The CPU 11 processes data by software stored in the ROM 13. The RAM 12 is used as an operating memory when the data processing is made in the CPU 11, and is also used as a memory for storing the result of the data processing. The I/O 14 has an input/output interface function to and from the IC card 1.

Fig. 2 is a block diagram showing an overall passport checking system operative for the IC card 1 shown in Fig. 1, which is used as a passport. Referring to Fig. 2, a registration acceptance system 21 and a renewal acceptance system 22 are provided in a passport issuing spot 2 for accepting passport registration and renewal applications, respectively.

An IC card passport processing system 23 produces a passport by registering necessary personal data on a blank

IC card 24 based on the data accepted at the acceptance systems 21 and 22.

When a registration of a new passport is applied for, the registration acceptance system 21 accepts the application. At this time, a personal data to be registered on the passport is inputted. The personal data includes the nationality, permanent domicile, address, name, age, sex distinction, height and weight of the user, in addition to the passport number, as well as the fingerprint identifying the user.

The IC card passport processing system 23 codes all the personal data including the fingerprint data. The coding may be made by the CPU 11 according to a coding program stored in the ROM 13 (Fig. 1).

The coded data is registered in a DB (database) 4 by a passport identifying system 3 at the government agency concerned (the Foreign Ministry in the case of Japan).

The personal data excepting the coded fingerprint data are stored in a memory of the IC card 24 before the issuance thereof to the applicant (or user). In the IC card 24 is also stored secrete key data, which is necessary when the coded data is decoded and the fingerprint is collated at an entry/departure admission system 5 or 6 described later.

A user's face photograph is of course printed on the

front surface of the IC card 24. A digital sign which is issued by the Foreign Ministry is further stored._

When a passport renewal is applied for, the renewal application system 22 accepts the application, and the IC card passport processing system 23 reads out data of the old passport and makes a check as to whether the recorded data has been tampered. Afterwards, the old passport is discarded. The IC card 24 is then issued afresh in the same way as in the case of the registration application as described above.

The IC card passport which is issued in this way, is used for the purpose of confirmation or identification in the entry/departure admission systems 5 and 6 installed in airports and also in an overseas passport network system 7.

Fig. 3 is a block diagram showing a fingerprint collation system for passport confirmation in such entry/departure admission systems 5 and 6. Referring to Fig. 3, an IC card reading unit 31 reads out data stored in the IC card passport 1 and forwards the read-out data to a decoding unit 31.

The decoding unit 32 decodes the coded personal data by using a secret key in the read-out data. Where the fingerprint collating system is on-line coupled to a passport identifying system 3 (see Fig. 2), which is installed in the Foreign Ministry, the database 4 is on-line accessed

at this time, and the pertinent user's fingerprint data is instantaneously transmitted to the decoding unit 32 and simultaneously decoded.

A fingerprint collating unit 34 collates actual user's fingerprint data read out by a fingerprint scanner 33 and registered fingerprint data decoded by the decoding unit 32, and forwards the result of collation to a checking unit 35 for confirmation/non-confirmation check.

By organizing a network such that the overseas passport checking system 7 shown in Fig. 2 can be on-line coupled to the Foreign Ministry passport identifying system 3, it is possible to make correct and instantaneous passport confirmation in domestic and foreign checking spots.

In the first embodiment explained above, the database 4 is installed at the Foreign Ministry for fingerprint registration (registered fingerprint data at the database) and is on-line coupled via the network to domestic and foreign checking spots. However, in the second embodiment hereinafter explained, by having the user's fingerprint data registered in the IC card passport (registered fingerprint data in the IC), it is possible to simplify the system.

Fig. 4 is a block diagram showing a fingerprint collating system of a second embodiment according to the invention. Parts like those in Fig. 3 are designated by

like reference numerals. In the IC card 1 in this instance, a fingerprint data in addition to personal data of the passport is stored in a memory. Therefore, in the IC card passport processing system 23 of the passport issuing spot 2 shown in Fig. 2, the fingerprint data is stored in a memory in the blank IC card 24 with other personal data.

Again in this case, a personal data and a fingerprint data are coded, and a secret key data necessary for the decoding is stored in the IC card memory. As in the preceding embodiment, the personal data including the fingerprint data is registered in the database 4 installed in the Foreign Ministry.

An IC card reading unit 31 reads out personal data and fingerprint data, and also secret key data, from the IC card 1, and supplies the read-out data to a decoding unit 32. The decoding unit 32 decodes the coded personal data and fingerprint data by using the secret key data, and supplies the decoded fingerprint data to a fingerprint collating unit 34.

The fingerprint collating unit 34 collates user's fingerprint data from a fingerprint scanner 33 and the coded fingerprint data, and supplies the result of collation to a checking unit 35. The checking unit 35 makes a confirmation/non-confirmation check according to the collation result.

To prohibit tampering of the stored contents in the IC card 1, a tampering prevention program (or commonly called tamper-resist program) can be stored in the ROM 13 (see Fig. 1). When it is detected that the tampering is about to be made, this program is started to cause self-destruction of the content.

As a different example of the tampering prevention, a technique disclosed in Japanese Patent Application Kokai Publication No. Hei 3-100753 may be utilized. In this technique, when the IC chip is opened for the tampering purpose, light is detected, thereupon causing deletion of the registered content with memory resetting, or deletion of ROM data, or destruction of LSI with high voltage application.

While the above description has covered the case wherein the IC card is applied to a passport, it is also possible to apply the IC card to driver's licenses, credit cards, membership cards, company employee cards, health insurance cards, bank cards (cash cards), and so forth. Again in these cases, a fingerprint data is used together with necessary personal data.

Where the IC card is applied to a driver's license, the systems 3, 2 and 5 to 7 shown in Fig. 2 serve as driver's license identification, issuing and collating systems, respectively. This application is convenient particularly

for collation and recording of data made by policemen in the case of violation of road traffic laws. —

Where the IC card is applied to a credit card, a credit card system can likewise be readily organized. The collation and recording may be made when a shopping is made by the user.

Where the IC card is applied to a membership card, a membership card issuing system can likewise be readily organized. In this case, mainly when the member applies for the membership, the collation and recording may be made.

Where the IC card is applied to a health insurance certificate, a health insurance card issuing system can likewise be readily organized. In this case, mainly when the user visits hospitals, the collation and recording may be made.

Where the IC card is applied to a company employee card, the collation and recording may be made when a company employee enters and leaves the company or makes payment for, for example, meals on bank account. Also, where the IC card is applied to a bank card, collation and recording are made when the user utilizes it in an ATM or CD machine.

The IC card may further be commonly applied to an electronic money system to obtain electric money with a higher security function.

As has been described in the foregoing, according to the invention, fingerprint data is used for collation. Thus, the identification of the user will be extremely accurate and, in application to the passport, illegal entry or departure can be readily detected.

Besides, a passport which is constituted by the IC card, is small in size and light in weight just like a credit card or a cash card, and can be very conveniently carried. Moreover, when combined with electronic money, the convenience can be further enhanced.

While the invention has been described in its preferred embodiments, it is to be understood that the words which have been used are words of description rather than limitation and that changes within the purview of the appended claims may be made without departing from the true scope of the invention as defined by the claims.



THIS SHEET HAS BEEN
REPLACED

- 13 -

This Sheet Has Been Replaced



What is claimed is:

1. An IC card to be checked by a personal data identifying system for confirming an IC card user by collating a registered fingerprint data and an input fingerprint data, said IC card comprising:
 - a fingerprint-related data; and
 - a storing means (12) for storing in advance said fingerprint-related data and a personal data.
2. The IC card according to claim 1, in which said fingerprint-related data stored in the storing means is a data for reading out said registered fingerprint data.
3. The IC card according to claim 1, in which said registered fingerprint data is a coded data, and which comprises a secret key data for decoding the coded registered fingerprint data which secret key data is stored in the storing means.
4. The IC card according to claim 1, which further comprises a means for preventing re-writing of the fingerprint-related data and the personal data.
5. The IC card according to claim 1, in which said personal data includes personal data for a passport.
6. A personal data identifying system comprising:
 - a register means (4) in which a fingerprint data of an

THIS SHEET HAS BEEN
REPLACED



- 14 -

This Sheet Has Been Replaced



individual user is registered;

a reading means (31,32) for reading out a fingerprint-related data stored in a storing means (12) in an IC card (1), and reading out the registered fingerprint data from the register means (4) based on the read-out fingerprint-related data; and

a checking means (34,35) for collating the read-out registered fingerprint data with input fingerprint data and determining identity thereof.

7. The personal data identifying system according to claim 6, in which said register means (4) is accessible from a domestic or foreign spot for collating a user's fingerprint by on-line processing.

8. The IC card according to claim 1, in which said fingerprint-related data stored in the storing means is a fingerprint data registered in the IC card.

9. The IC card according to claim 8, in which the registered fingerprint data is a coded data, and which comprises a secret key data for decoding the coded registered fingerprint data which secret key data is stored in the storing means (12).

10. A personal data identifying system which comprises a means to read a fingerprint data stored in an IC card

THIS SHEET HAS BEEN
REPLACED

- 15 -



according to claim 8 and which further comprises a checking means for collating the read-out fingerprint data with input fingerprint data and determining identity thereof.

11. The personal data identifying system according to claim 6, in which the IC card has personal data for a passport and is used for entry and departure admission purposes.

12. The personal data identifying system according to claim 10, in which the IC card has personal data for a passport and is used for entry and departure admission purposes.

This Sheet Has Been Replaced

