(19) Canadian Intellectual Property Office
An Agency of Industry Canada

Office de la Propriété Intellectuelle du Canada
Un organisme d'Industrie Canada

(11) CA 2 256 809 (13) A1

(43) 21.06.2000

(12)

(21) 2 256 809

(51) Int. Cl.[6]: G06K 009/68, G07C 009/00

(22) 21.12.1998

(71) DIGITAL SECURITY CONTROLS LTD.,
1645 Flint Road, DOWNSVIEW, O1 (CA).

(72) PARKER, James (CA).

(74) DENNISON ASSOCIATES

(54) DISPOSITIF D'ENTREE BIOMETRIQUE POUR SYSTEME DE SECURITE
(54) BIOMETRIC INPUT DEVICE FOR SECURITY SYSTEM

(57)

The present invention provides for a biometric input device for a security system. The biometric input device includes a biometric sensor for sensing and input of biometric data, an image capture module for capturing and storage of the inputted biometric data from the biometric sensor, and an input/output module for passing the captured biometric data to a control panel and receiving data from the control panel. The invention also provides for a security system for controlling access to a premises. The security system includes a control panel for overall control of the security system, and one or more input devices for allowing users to interact with the security system. One or more of such input devices is a biometric input device capable of sensing biometric data from a user and capable of passing said sensed biometric data to the control panel for comparison against a database of biometric data of authorized users

OPIC
OFFICE DE LA PROPRIÉTÉ INTELLECTUELLE DU CANADA

CIPO
CANADIAN INTELLECTUAL PROPERTY OFFICE

(12) (19) (CA) **Demande-Application**

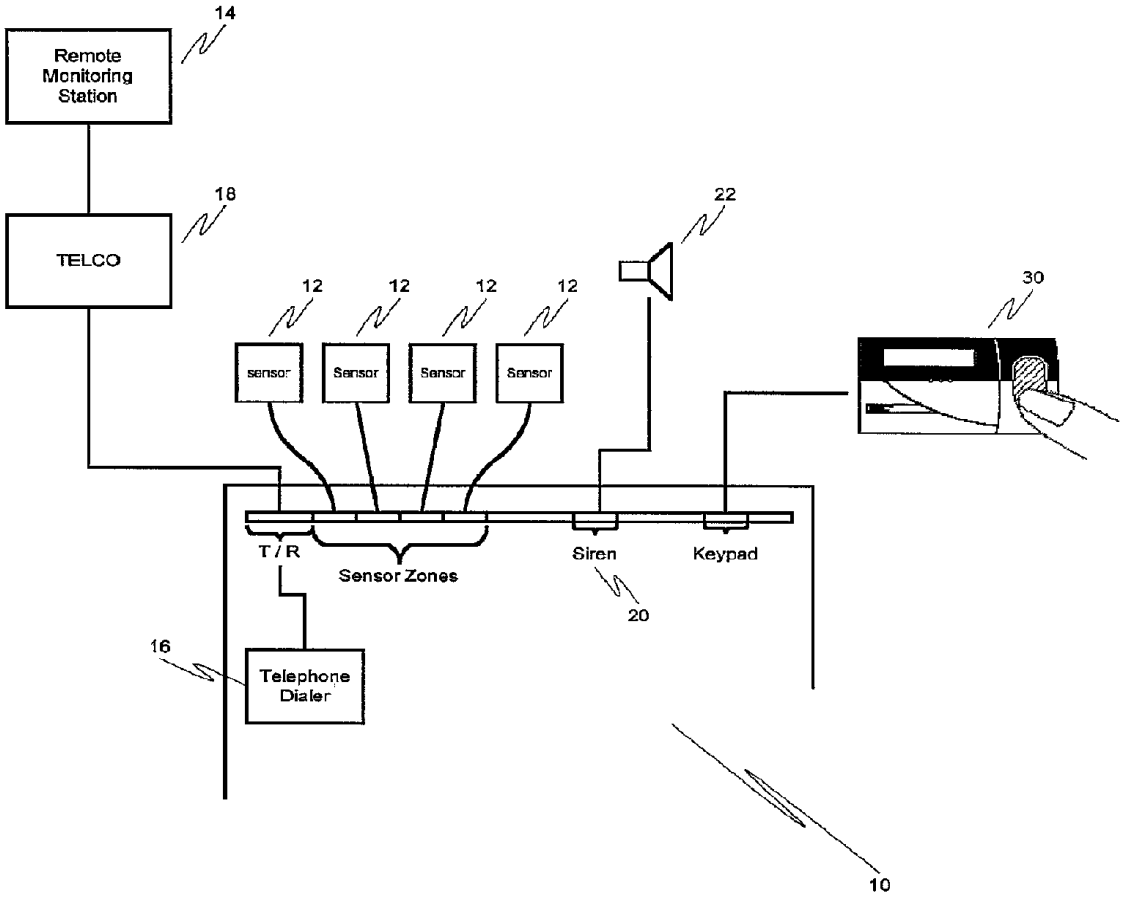
(21) (A1) **2,256,809**
(22) 1998/12/21
(43) 2000/06/21

(72) PARKER, James, CA
(71) DIGITAL SECURITY CONTROLS LTD., CA

(51) Int.Cl.[6] G06K 9/68, G07C 9/00

(54) **DISPOSITIF D'ENTREE BIOMETRIQUE POUR SYSTEME DE SECURITE**

(54) **BIOMETRIC INPUT DEVICE FOR SECURITY SYSTEM**



(57) The present invention provides for a biometric input device for a security system. The biometric input device includes a biometric sensor for sensing and input of biometric data, an image capture module for capturing and storage of the inputted biometric data from the biometric sensor, and an input/output module for passing the captured biometric data to a control panel and receiving data from the control panel. The invention also provides for a security system for controlling access to a premises. The security system includes a control panel for overall control of the security system, and one or more input devices for allowing users to interact with the security system. One or more of such input devices is a biometric input device capable of sensing biometric data from a user and capable of passing said sensed biometric data to the control panel for comparison against a database of biometric data of authorized users

ABSTRACT OF THE DISCLOSURE

The present invention provides for a biometric input device for a security system. The biometric input device includes a biometric sensor for sensing and input of biometric data, an image capture module for capturing and storage of the inputted biometric data from the biometric sensor, and an input/output module for passing the captured biometric data to a control panel and receiving data from the control panel. The invention also provides for a security system for controlling access to a premises. The security system includes a control panel for overall control of the security system, and one or more input devices for allowing users to interact with the security system. One or more of such input devices is a biometric input device capable of sensing biometric data from a user and capable of passing said sensed biometric data to the control panel for comparison against a database of biometric data of authorized users

JJ-10 303CA

TITLE: BIOMETRIC INPUT DEVICE FOR SECURITY SYSTEM

FIELD OF THE INVENTION

The present invention is directed to an input device for a security system which incorporates a biometric sensor for increased control over authorization of entry into the premises in which the security system is located.

BACKGROUND OF THE INVENTION

Security systems are becoming widespread in use with most commercial establishments and many residential establishments having security systems installed. Such security systems generally include a control panel which controls the overall operation of the system, one or more input devices such as keypad controllers for user access to the system and various detectors and sensors. The control panel is generally mounted in an area of restricted access, such as a utility room or basement, and contains the system electronics, back-up power sources, and may include an interface for remote monitoring and two way communication over telephone lines or other communication channels. Security systems are generally divided into several zones or areas of protection and each of these zones generally has one or more detection devices or sensors such as motion detectors, door or window contacts, glass break detectors, or shock sensors connected to it. In some security systems, smoke detectors or other fire detection devices may also be connected to the control panel.

Security systems generally have one or more input devices such as keypad controllers or card swipe readers etc., which are used by the user to send input to the security system. Many input devices such as keypad controllers are also used by the user to instruct the security system. The keypad controller may be used to send commands to the system to control the operation of the system and may also display system information. Such keypad controllers generally have a status display which

may include either individual indicators, such as light emitting diodes or may include a LCD or LED display, which is capable of displaying a number of alpha-numeric characters used to display simple messages regarding the status and operation of the system. Recently, graphical controllers have also been proposed having a graphical display screen capable of displaying a floor plan of the premises at which the security system is installed. Such graphical controllers may also include touch screen technology or user input.

The input device such as the keypad controller is also used by the user to arm and disarm the security system. Each user of a security system with a keypad controller is given a unique personal identification number or PIN, which is generally a sequence of numbers which are entered by the user, in order, on a numeric keypad. When arming the system, the user enters their PIN at which time the system will be armed and will generally provide a delay time to enable the user to exit the premises at which the system is located before the system becomes fully armed. Upon entering a premise having an armed security system, the user would enter their PIN at which time the security system would be disarmed. During disarming of the security system, there is generally a delay time to enable the user to enter their PIN before the system will go into alarm mode.

There are many instances where a user will forget their PIN or enter an incorrect PIN into the keypad controller. Many controllers permits multiple attempts to enter the PIN through the keypad. This will allow the user to correctly interact with the system in those circumstances where the user has entered an incorrect PIN. However even allowing multiple attempts will not help a user who has forgotten their PIN. It would be useful in such circumstances to utilize a unique characteristic of the user to identify the user to the security system. Such

characteristic could be a unique biometric characteristic such as a fingerprint, retina scan, voice print etc. In addition there are certain security installations which may require a higher level of security. In such installations the use of unique biometric characteristic in-place of or in addition to a PIN or security card would be of benefit.

SUMMARY OF THE INVENTION

The present invention provides for a biometric input device for a security system. The biometric input device comprises a biometric sensor for sensing and input of biometric data, an image capture module for capturing and storage of the inputted biometric data from the biometric sensor, and an input/output module for passing the captured biometric data to a control panel and receiving data from the control panel.

In an aspect of the invention there is provided a security system for controlling access to a premises. The security system comprises a control panel for overall control of the security system, and one or more input devices for allowing users to interact with the security system. One or more of such input devices is a biometric input device capable of sensing biometric data from a user and capable of passing said sensed biometric data to the control panel for comparison against a database of biometric data of authorized users.

BRIEF DESCRIPTION OF THE DRAWINGS

Preferred embodiments of the present invention are illustrated in the attached drawings, wherein:

Figure 1 is a schematic view of a security system, embodying the input device of the present invention;

Figure 2 is a schematic view of a first embodiment of an input device of the present invention illustrating the operation of the input device;

Figure 3 is a schematic view of a second embodiment of an input device of present invention illustrating the operation of the input device; and

Figure 4 is a schematic view of the fourth embodiment of an input device of the present invention illustrating the interaction between the input device and the control panel.

DETAILED DESCRIPTION OF THE PREFERRED EMBODIMENTS

A typical security system embodying the present invention is illustrated in Figure 1. The security system comprises a control panel 10 which controls the operation of the overall security system. A number of sensors or detection devices 12, utilized for monitoring a zone or area of protection, are connected to the control panel in a typical manner. Detection devices 12 may be any of the commonly utilized detection devices such as motion detectors, door contacts, glass break detectors, shock sensors, fire detectors, water detectors, etc. The detection devices 12 in Figure 1 are illustrated as being hard wired to the control panel 10, however, wireless technology is in common use and any of the detection devices 12 could use wireless communication between the detection devices 12 and the control panel 10. The security system may be capable of reporting to a remote monitoring station 14, utilizing any of the commonly employed methods of communication such as utilizing a telephone dialer 16 sending messages to the remote monitoring station 14 over the local telephone system 18. In some situations, the connection between the control panel 10 and the remote monitoring location 14 may also be wireless, utilizing cellular telephone technology or other means of wireless communication. The system can also use other communication arrangements such as two way cable systems. The control panel also includes an interface 20 for connection to a sounding device 22 for activation in an alarm or emergency situation.

The control panel 10 includes logic and programming modules which control the overall operation of the system including the processing of the biometric data from the input device as will be described below.

An input device for allowing the user to interact with the security system is also connected to the control panel. Many such input devices are presently in use including keypad controllers, card swipe readers, etc. specific to security systems, which may be hardwired to the control panel or may communicate with the control panel using suitable wireless technology. As shown in the figure, in a preferred embodiment, the input device with a biometric input is connected to the control panel 10 for allowing the user to interface with the security system, to program the system and control the operation of the system and for displaying the status of the system and its various components. As noted above while the input device is preferably a keypad controller any suitable input device for allowing a user to interact with and in particular enter access codes for the security system may be utilized.

Figure 2 illustrates a first embodiment of an input device of the present invention 30 for use with a security system. The input device allows the user to interact with the controller 30 using biometric data. The biometric data may be any biometric data which may be easily obtained from the user. Such biometric data may be a finger print, voice recognition, retina scan, or other easily measured biometric characteristic. Preferably, the biometric characteristic is a finger print, more preferably a thumb print. The input device is provided with a scanner capable of capturing an image of the thumb print of the user. One such scanner is that manufactured by Siemens and sold under the trademark FINGERTIP. This scanner is a CMOS sensor which is built around a capacitive sensing circuit with the sensor pixel array being one plate and the surface of the skin of the finger being the other plate. The user would

.place their thumb on the thumb print scanner to activate the controller 30. The thumb print of the user would be scanned in and captured as an image. This image may then be passed to the control panel along the data bus. The control panel in the embodiment illustrated in Figure 2 is provided with a biometric interface module to interact with the input module and pass the image captured by the input module onto the processing circuitry. The image captured from the input module is processed by the sensor data processing and compared by a data comparator against an authorized user account database maintained in non-volatile RAM. If the image captured by the input module matches an image maintained within the authorized user account database than the control processor of control panel carries out the instructions programmed in the control panel. These instructions may include opening the door to allow the user access to the premises at which the security system is installed or may unlock a keypad which then allows the user to interact directly with the security system.

A second embodiment of an input device for a security system of the present invention is illustrated in figure 3. In this embodiment of the invention the input device includes both the biometric sensor such as a thumb print scanner as well as a means for allowing additional user input. One purpose of permitting the additional user input is to increase the security of the system. By requiring additional user input, access to the system can be restricted to situations where both the biometric sensor as well as the additional input correctly identifies an authorized person.

If either of the biometric data or the additional user input matches the stored data, but the other does not, various options may be made available to the user. For example, in these situations, the user may be given limited access to the system. The system may also flay the event

and display a trouble message. This flag and trouble message could also be passed on to a remote monitoring location. The system may also be programmed to store the incomplete access data for future reference and retrieval. The actions which the system could take upon an incomplete authorization could depend upon the needs of the location at which the system is located and those of skill in the art could easily adopt the system and provide it with the required functions and actions.

The means for additional user input may be any means commonly used in the security art. Such means may be a keypad for entering in an access identification number or PIN or may be a card swipe for reading a magnetic stripe on a security access card. Other means for additional user input would be known to those skilled in the security system art.

The input device of the embodiment of Figure 3 takes the image from the biometric sensor and passes it through to the control panel for comparison against the authorized user database similar to the first embodiment. The input device may simply pass the captured image data and the additional user input as separate discrete data. In this type of setup both of the individual elements of data may be compared against the authorized user ID database to determine if both sets of data match entries in the database. Alternatively, the additional user input such as the PIN entered on a keypad may be used as a pointer to point to the location in the database where the image of the user is stored for comparison with the image captured by the biometric sensor. By utilizing the PIN as a data pointer, the comparison of the captured image with the image stored in the database is much simplified and would require less processing power as it would not be necessary for the data comparator to compare the captured image against every image in the database.

To increases the security of the security system the input device may encrypt the data from the biometric sensor for transmission to the control panel. This encryption could utilize an algorithm in which the additional user input is used in the algorithm to encrypt the data. This would be of particular benefit for highly sensitive security installations where any data being transmitted would have to be encrypted. This type of encryption of data would also be useful in situations where the input device and control panel are not hardwired to one another but utilize wireless technology for transmission of data back and forth.

Once the data has been passed to the control panel the control panel could compare the encrypted data with encrypted data stored in the database. Alternatively, the control panel could process the data to decrypt it and then compare the decrypted data with the data in the database. Once again, in order to improve processing capability, the additional user input may be utilized as a pointer to point to the storage location in the database for the stored data which is to be compared with the captured image.

A third embodiment of an input device of the present invention is illustrated in figure 4. In the security system illustrated the input device is the combination of a keypad controller and a biometric sensor. The keypad controller 32 is provided with a numeric keypad having individual keys 34 and a status indicating means for providing feedback to a user on the status of the system. The status indicating means can be any of the commonly employed means to provide audio or visual feed back. For example, the status indicating means can be a means of providing audio feedback by providing a speaker to play back prerecorded messages or system generated messages corresponding to the status of the system. Alternatively, the status indicating means can provide visual feedback through the use of indicator lights, LCD or LED displays

capable of displaying alpha-numeric characters or displays capable of displaying graphical images. In the embodiment illustrated in figure 4, the keypad controller 32 is provided with an LCD or LED display area 36 for visual display of system messages and feedback during key entry on the keypad, although as noted above, other status indicating means may be employed.

Similar to the embodiment illustrated in figure 3 described above, the input device of figure 4 utilizes a combination of the biometric data and the additional user input. Once again, preferably the biometric data from the image capture and the user input from the keypad is encrypted to form a unique user ID. This unique user ID is then passed along the data bus to the control panel where the biometric interface module compares the encrypted user ID with an authorized user account database.

The biometric input devices as described above, may be utilized for initialization of the image database. The initial image capture from this thumbprint scanner could be accomplished utilizing a special maintenance or service code to store the scanned image in the image database. The particular and unique access code or PIN associated with this image could then be entered in and stored in the database in the forms as described above.

The use of the combination of a biometric input and the access code may also be utilized to grant different levels of access to individual users. For example, a group of users could be given a common access code, and then the biometric input data would be utilized to differentiate each of the users having the common access code and to regulate the level of access to the system which the user would be allowed.

The embodiments of the invention described above in which the image data is stored at the control panel and the

keypad is merely used for image capture and transfer of the captured image to the control panel provide for numerous other benefits to the security system in addition to the increased level of security. As the image is processed and stored at the control panel, rather than at the keypad, such a security system is amenable to multiple keypads for multiple access points. Each of the keypads would be provided with a biometric input capability with the image from the biometric input being shipped over the data bus to the control panel in the manner as described above. In addition, the control panels generally have much more processing power than keypads and utilizing this processing power of the control panel allows for biometric input at the keypad at a reasonable cost, as it is not necessary to provide each of the individual keypads with increased processing power.

The processing of the image data at the control panel also allows for storage of the original scanned image when the user is attempting to access the security system. This may be of importance in a high security application where it would be of benefit to maintain the raw data from each access of the security system.

The processing and storage of the image data at the control panel also allows for simpler maintenance and upkeep of the image database, as new users could easily be added to the image database in a manner as described above. In addition, users which no longer have access to the security system could have their associated images and access codes deleted from the database by a supervisor having appropriate levels of access. Alternatively, the image may be maintained in the database to enable logging of attempts by the former user to gain access to the system, but the image in the database would be flagged for non-access to the system.

The input device of the present invention with the incorporated biometric sensor allows for increased control over authorization of user access to security systems using the input device. In some installations, such an input device allows for very specific access to the system by utilizing a unique biometric identifier of a user without requiring a user to remember and enter an authorization code. In the installations, increased levels of security access may be provided by requiring a user to input a parameter such as an authorization code or card swipe in addition to the biometric data to gain access to the system. In other situations, the additional parameter may used as a pointer to speed up the process of matching the biometric data from the sensor to the stored biometric data. The additional parameter may also be used in an encryption algorithm to increase the security of the system.

Although various preferred embodiments of the present invention have been described herein in detail, it will be appreciated by those skilled in the art, that variations may be made thereto without departing from the spirit of the invention or the scope of the appended claims.

THE EMBODIMENTS OF THE INVENTION IN WHICH AN EXCLUSIVE PROPERTY OR PRIVILEGE IS CLAIMED ARE DEFINED AS FOLLOWS:

1. A biometric input device for a security system comprising a biometric sensor for sensing and input of biometric data,

an image capture module for capturing and storage of the inputted biometric data from the biometric sensor, and

an input/output module for passing the captured biometric data to a control panel and receiving data from the control panel.

2. A biometric input device for a security system according to claim 1, wherein the biometric data is one or more selected from the group consisting of a finger print, a hand print, voice print, a hand geometry, a facial feature geometry or a retina scan.

3. A biometric input device for a security system according to claim 1, wherein the biometric data is a thumb print and the biometric sensor is a thumb print scanner.

4. A biometric input device according to claim 3, wherein the input device further includes a keypad for allowing a user to input alphanumeric characters.

5. A security system for controlling access to a premises, the security system comprising a control panel for overall control of the security system, and one or more input devices for allowing users to interact with the security system one or more of such input devices being a biometric input device capable of sensing biometric data from a user and capable of passing said sensed biometric data to the control panel for comparison against a database of biometric data of authorized users.

6. A security system according to claim 5, wherein the biometric input device is provided with a security system comprising a biometric sensor for sensing and input of biometric data,

an image capture module for capturing and storage of the inputted biometric data from the biometric sensor, and

an input/output module for passing the captured biometric data to a control panel and receiving data from the control panel.

7. A security system according to claim 6, wherein the biometric data is one or more selected from the group consisting of a finger print, a hand print, a voice print, a hand geometry, a facial feature geometry or a retina scan.

8. A security system according to claim 6, wherein the biometric data is a thumb print and the biometric sensor is a thumb print scanner.

9. A security system according to claim 8, wherein the input device further includes a keypad for allowing a user to input alphanumeric characters.

10. A security system according to claim 9, wherein the control panel maintains an authorized user database of images, the control panel further including a data comparator for comparing the captured image from the input device with the images from the database.

11. A security system according to claim 10, wherein the alphanumeric characters input by a user comprises an access code.

12. A security system according to claim 11, wherein each of the access code and captured image are passed to the control panel by the input device for comparison

against an authorized user database of images and access codes.

13. A security system according to claim 11, wherein the access code is utilized by the control panel as a pointer to the location in the image database where the image of the biometric data of the user is stored.

14. A security system according to claim 11 wherein the input device includes an encryption module for encrypting the access code and captured image prior to outputting the data to the control panel.

15. A security system according to claim 14 wherein the access code is utilized by the encryption module as a variable in the encryption of the image data.

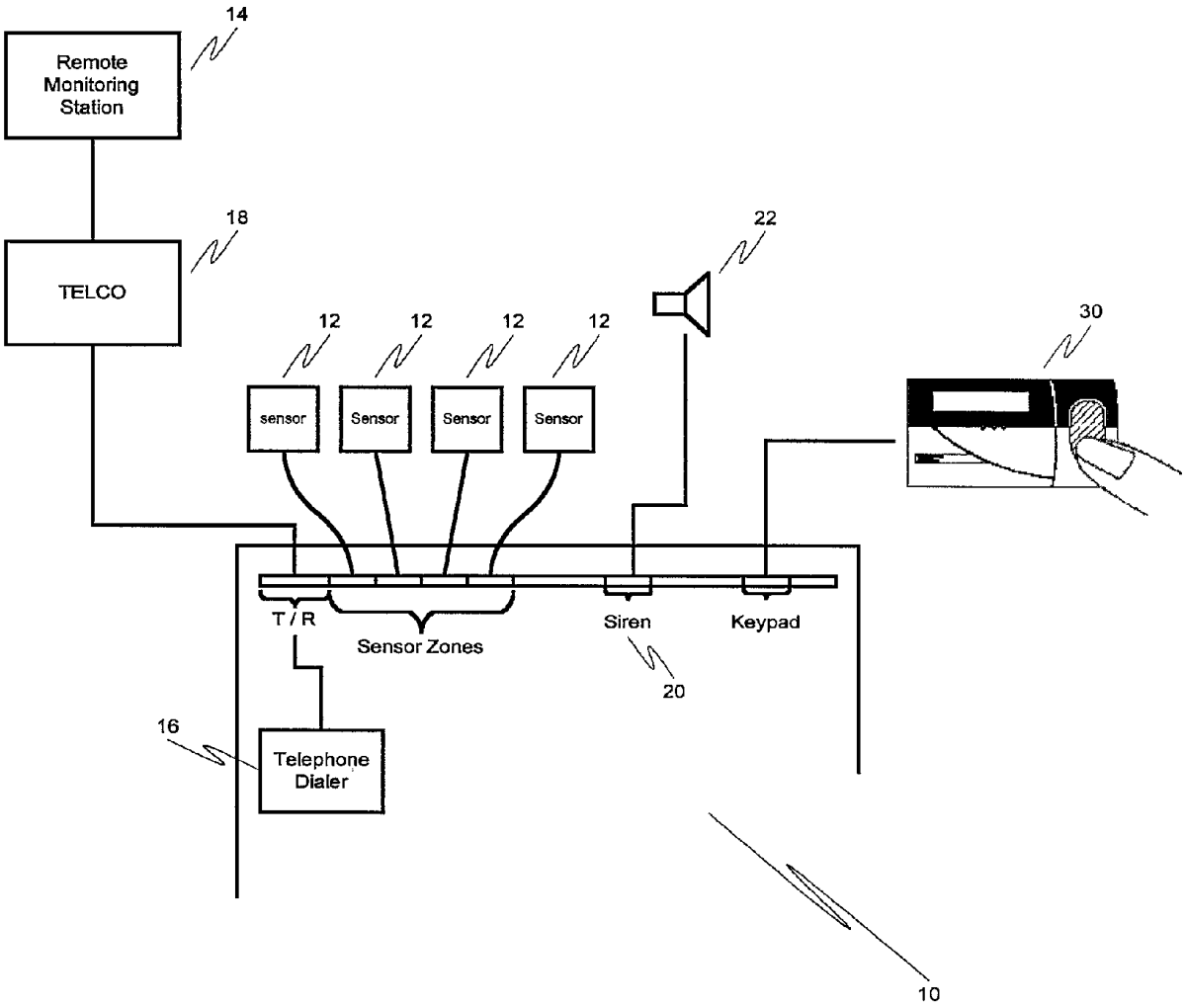

14
Remote Monitoring Station
18
TELCO
22
12
12
12
12
sensor
Sensor
Sensor
Sensor
30
T / R
Sensor Zones
Siren
Keypad
20
16
Telephone Dialer
10

Fig. 1

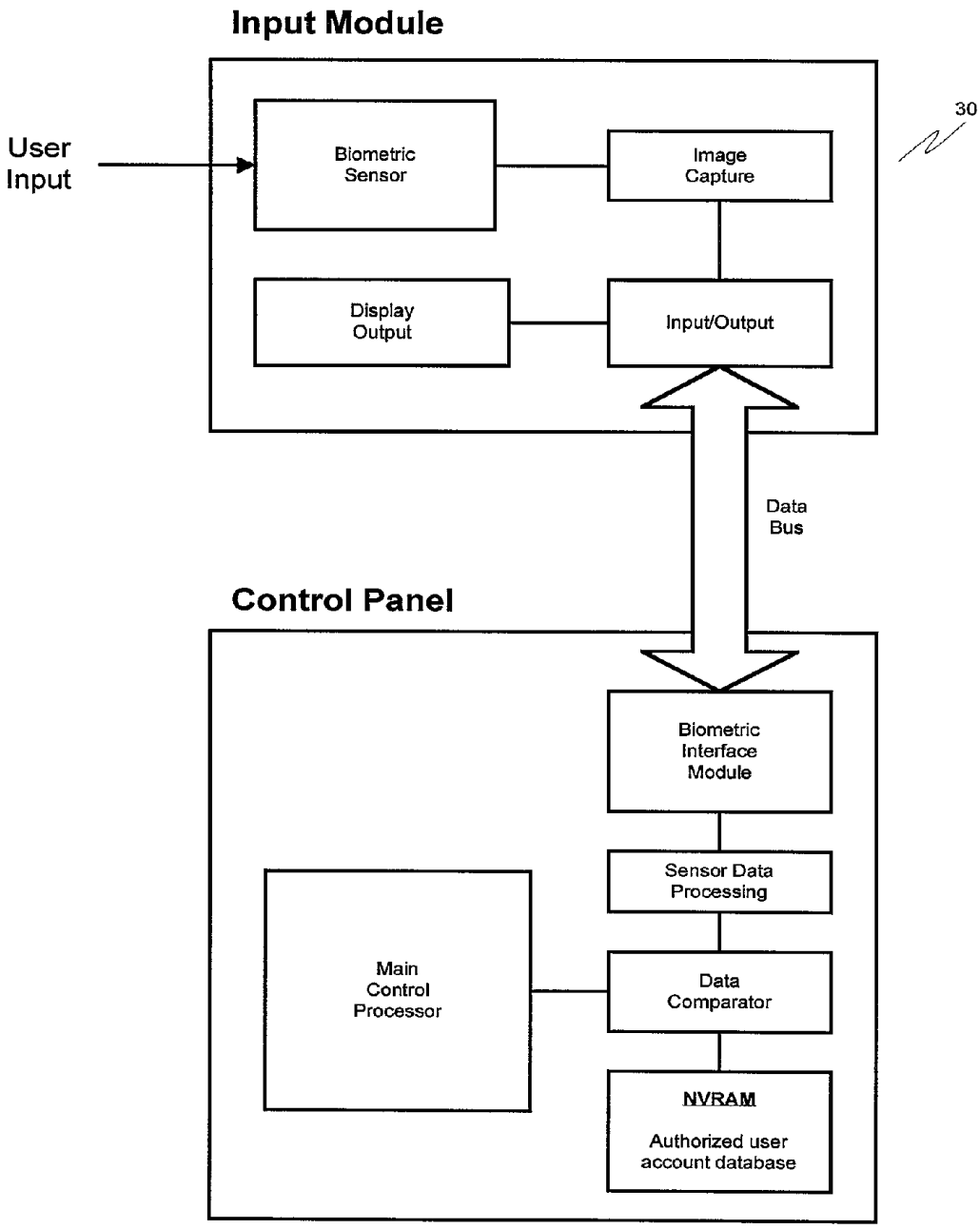

Input Module
User Input
Biometric Sensor
Image Capture
30
Display Output
Input/Output
Data Bus
Control Panel
Biometric Interface Module
Sensor Data Processing
Main Control Processor
Data Comparator
NVRAM
Authorized user account database

Fig. 2

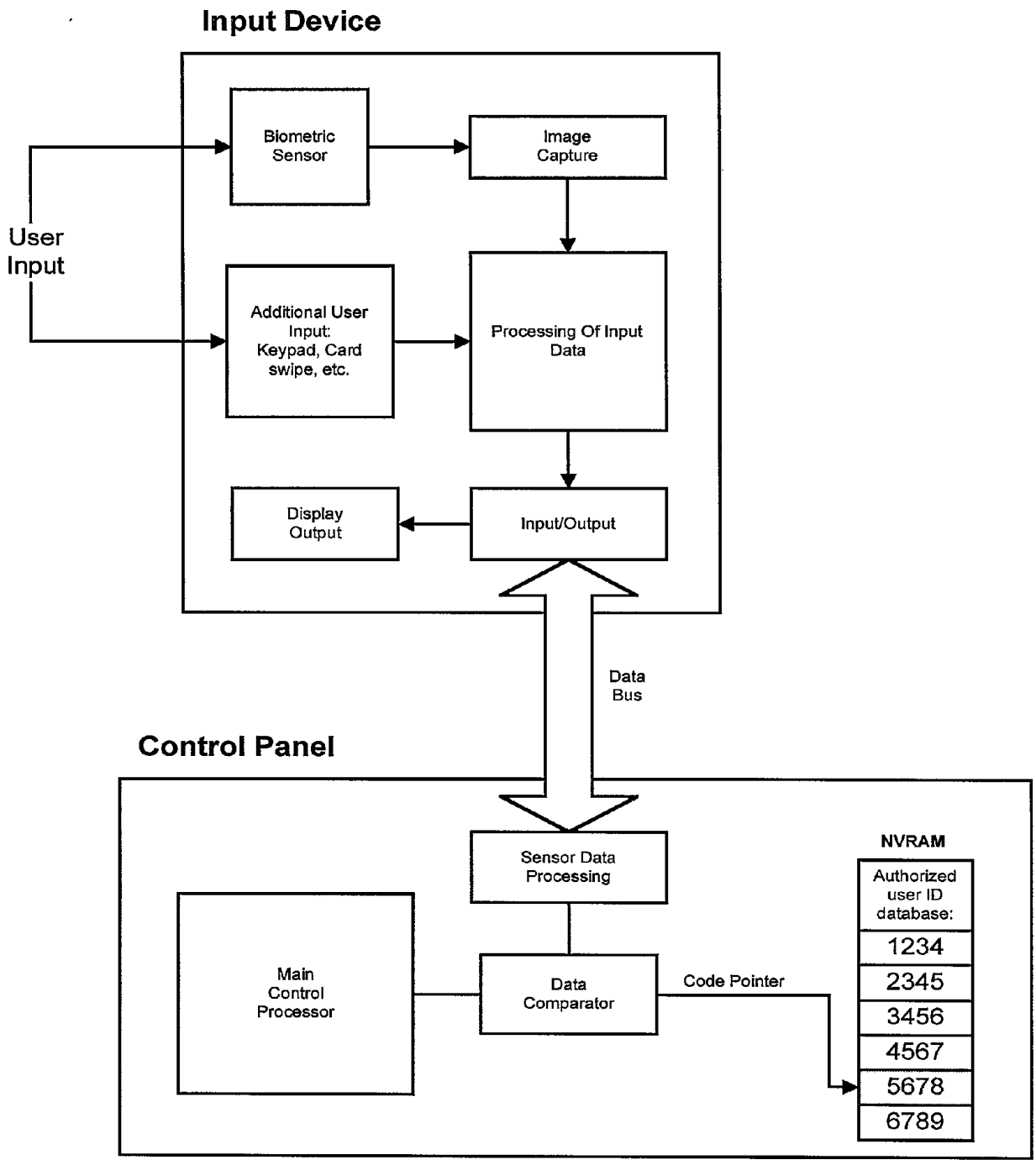

Input Device
Biometric Sensor
Image Capture
User Input
Additional User Input: Keypad, Card swipe, etc.
Processing Of Input Data
Display Output
Input/Output
Data Bus
Control Panel
Sensor Data Processing
NVRAM
Authorized user ID database:
1234
2345
3456
4567
5678
6789
Main Control Processor
Data Comparator
Code Pointer

Fig. 3

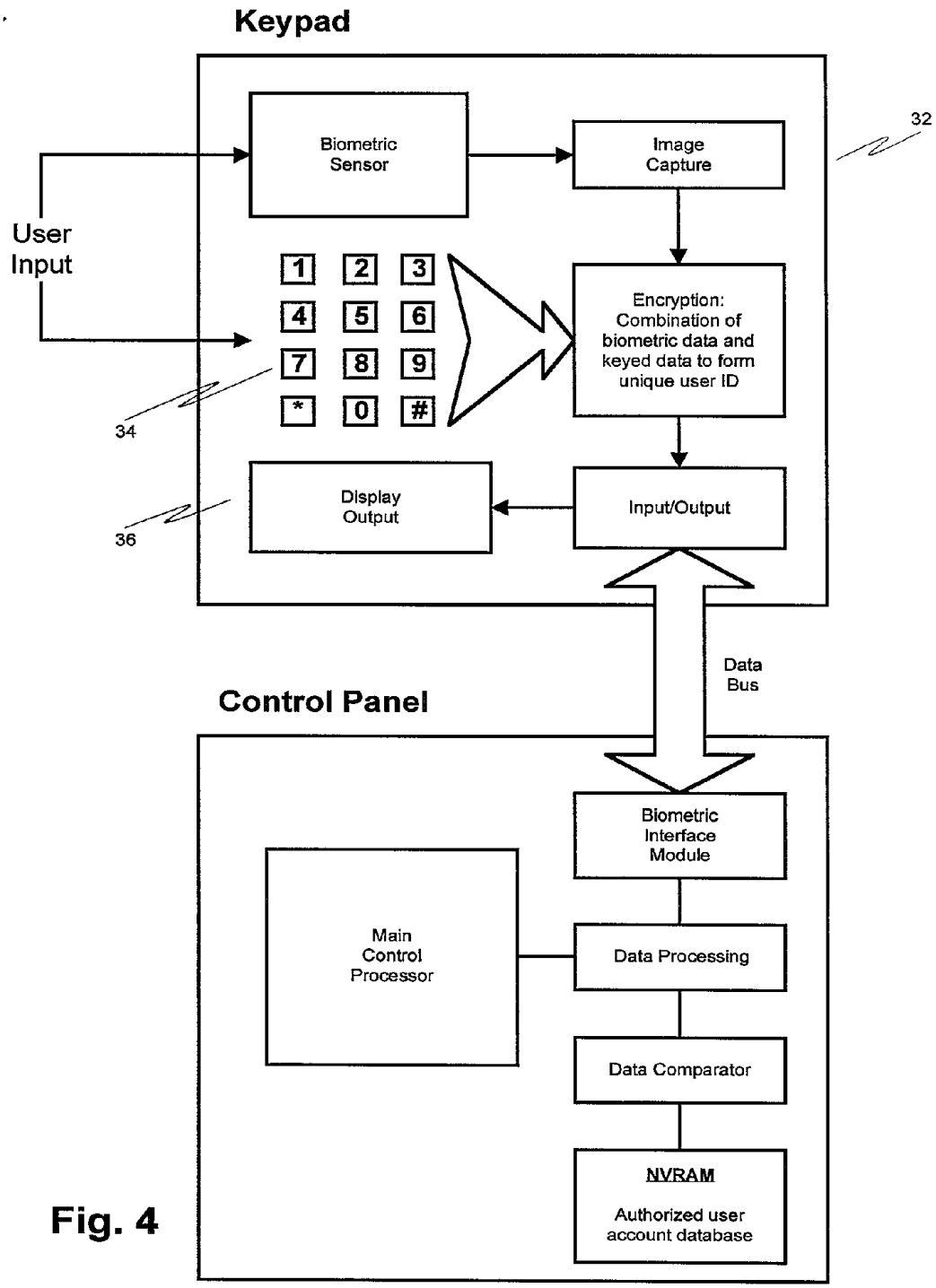

Keypad
Biometric Sensor
Image Capture
32
User Input
1
2
3
4
5
6
7
8
9
*
0
#
34
Encryption: Combination of biometric data and keyed data to form unique user ID
Display Output
36
Input/Output
Data Bus
Control Panel
Biometric Interface Module
Main Control Processor
Data Processing
Data Comparator
NVRAM
Authorized user account database

Fig. 4