(12) INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
10 February 2005 (10.02.2005)

PCT

(10) International Publication Number
WO 2005/013181 A2

(51) International Patent Classification[7]: G06K

(21) International Application Number:
PCT/US2004/024411

(22) International Filing Date: 30 July 2004 (30.07.2004)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
60/490,956 30 July 2003 (30.07.2003) US

(71) Applicant *(for all designated States except US)*: **APPLIED NEURAL COMPUTING LTD.** [US/US]; 2150 Route 38, #352, Cherry Hill, NJ 08002 (US).

(72) Inventors; and
(75) Inventors/Applicants *(for US only)*: **AVNI, Yossi** [IL/IL]; 32 Pinchas Rozen Street, P.O.B. 444, 46103 Herzelia (IL). **SUCHARD, Eytan** [IL/—]; 11a Heshel street, P.O.B. 453, 27104 Kyriut Byalik (IL).

(74) Agent: **WAR, Steven, M.**; Fulbright & Jaworski LLP, 801 Pennsylvania Avenue, N.W., Washington, DC 20004-2623 (US).

(81) Designated States *(unless otherwise indicated, for every kind of national protection available)*: AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BW, BY, BZ, CA, CH, CN, CO, CR, CU, CZ, DE, DK, DM, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MA, MD, MG, MK, MN, MW, MX, MZ, NA, NI, NO, NZ, OM, PG, PH, PL, PT, RO, RU, SC, SD, SE, SG, SK, SL, SY, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, YU, ZA, ZM, ZW.

(84) Designated States *(unless otherwise indicated, for every kind of regional protection available)*: ARIPO (BW, GH, GM, KE, LS, MW, MZ, NA, SD, SL, SZ, TZ, UG, ZM, ZW), Eurasian (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European (AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HU, IE, IT, LU, MC, NL, PL, PT, RO, SE, SI, SK, TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG).

Published:
— *without international search report and to be republished upon receipt of that report*

For two-letter codes and other abbreviations, refer to the "Guidance Notes on Codes and Abbreviations" appearing at the beginning of each regular issue of the PCT Gazette.

(54) Title: SYSTEM AND METHOD FOR INTEGRATING BIOMETRIC READERS INTO SECURITY DEVICES

(57) Abstract: According to one aspect of the invention, the present invention includes an enhanced security device comprising: an access device , a biometric reader attached to the access device, a memory configured to receive data from the biometric reader, where the biometric reader is used in conjunction with a learning mode to store known biometric information for comparison at a later time, and a security device associated with the access device, and a comparator including the learning mode and a utilization mode which performs a comparison in the utilization mode between unknown biometric information obtained from the biometric reader and the known biometric information stored in the memory such that the utility of the access device is dependent on the comparison.

WO 2005/013181 A2

SYSTEM AND METHOD FOR INTEGRATING BIOMETRIC READERS INTO SECURITY DEVICES

RELATED APPLICATIONS

[0001] This application claims priority to U.S. Provisional Patent Application No. 60/490,956 filed July 30, 2003.

BACKGROUND OF THE INVENTION

[0002] The present invention relates to systems and methods that are used to control access and thereby protect property, information, or other valuables. The present invention incorporates the use of biometric information into security devices to ensure access is only granted to authorized personnel. Biometrics which may be used include, but are not limited to, iris recognition, the use of retina blood vessels recognition, palm blood vessels structure recognition, finger print recognition and voice recognition devices and methods, or any other biometric that uniquely identifies a specific individual. Examples of prior art systems and methods are given in the U.S. Patents of Gokcebay, U.S. Patent No. 5,245,329; Feldman, U.S. Patent No. 5,938,706; Bonder et al., U.S. Patent No. 6,078,265; Ostermann et al., U.S. Patent No. 5,774,060; Klebes et al., U.S. Patent No. 6,260,300; Nagao et al., U.S. Patent No. 6,376,930; Sato, U.S. Patent No. 6,474,011; Tatsukawa et al., U.S. Patent No. 6,710,700; and Koo, Patent Application Publication No. US 2004/0021552, "RFD: A Key to Automating Everything" Roy Want, Scientific American (January 2004), *The RFID Handbook: Fundamentals and Applications in Contactless Smart Cards and Identification*, 2nd Edition, Klaus Finkenzeller John Wiley & Sons (May 9, 2003) the disclosures of which are incorporated herein in their entirety.

BRIEF SUMMARY OF THE INVENTION

[0003] According to one aspect of the invention, an enhanced security device includes an access device, a biometric reader attached to the access device where the biometric reader is used in conjunction with a learning mode to store known biometric information for comparison at a later time, a memory configured to receive data from the biometric reader, and a security device associated with the access device. A comparison is performed between the information obtained from the biometric reader and the information stored in the memory. The utility of the access device is dependent on the comparison.

[0004] According to another aspect of the invention, an enhanced security device includes an access device, a biometric reader attached to the access device which is used in a utilization mode and a learning mode, a memory configured to receive and store data from the biometric reader, and a security device associated with the access device as well as a means for denying access to the enhanced security device.

[0005] According to another aspect of the invention, a security device includes a key, a bow portion of the key having attached thereto a biometric sensor operational to collect biometric data from a user, a blade portion for accepting a plurality of cuts therein so as to operate a mechanical lock by insertion of the blade portion into a cylinder portion of the mechanical lock, and a data interface configured to transmit the biometric data to a control circuit wherein the control circuit is operational to selectively enable operation of the cylinder in response to the biometric data. The biometric sensor is used in an utilization mode and a learning mode.

[0006] According to another aspect of the invention, a data input device includes a transducer configured to be manually operated by a user to provide an input signal, a biometric sensor configured to collect biometric data from the user while the user is operating the

transducer, and a controller responsive to the biometric data for selectively enabling the input signal. The biometric sensor is used in a utilization mode and a learning mode.

[0007] According to another aspect of the invention, a method of updating a conventional security device to an enhanced security device includes the steps of replacing a conventional cylinder of the conventional security device with an enhanced cylinder, replacing a conventional key of the conventional security device with an enhanced key wherein the enhanced key included a biometric reader, and locating a comparator card within RFID range to the enhanced security device wherein the comparator card compares information received from the biometric reader to stored biometric information to allow the enhanced security device to be accessed.

BRIEF DESCRIPTION OF THE DRAWINGS

[0008] The present invention is described in detail below with reference to the following figures, of which:

[0009] FIG. 1 illustrates a key which incorporates a biometric fingerprint reader, contacts and sensors,

[0010] FIG. 2 shows one embodiment of the present invention in which two pairs of contacts located within an enhanced security device are used to ensure biometric information is correct before the lock can be opened,

[0011] FIG. 3 shows a flow chart of the process for which biometric information is checked prior to the opening of the enhanced security device,

[0012] FIG. 4 illustrates how RFID technology may be used with the present invention,

[0013] FIG. 5 illustrates the various components of the present invention which includes the fingerprint reader card, the door circuit, the learning process and the identification process, and

[0014] FIG. 6 illustrates a process to retrofit a conventional lock to become an enhanced security device.

DETAILED DESCRIPTION OF THE INVENTION

[0015] The present invention is now discussed in detail with reference to the figures that were briefly described above. Unless otherwise specified, like parts, systems, and processes are referred to with like reference numerals.

Glossary

[0016] An **RFID (Radio Frequency Identification)** tag is an electronic tag that receives data from marked products through miniature circuits that are attached to products, for example, supermarket products. The RFID tag requires no batteries. The RFID tag derives its energy through induction by a device that is placed nearby and produces electromagnetic energy. For example, a small coil or dipole antenna may be used to charge a capacitor through a diode. Once a sufficient charge is stored in the capacitor, the voltage activates the RFID tag miniature circuit and the circuit sends data through transmission. A receiver which is near the tag, receives and deciphers the transmission from the RFID tag.

[0017] A **Secure RFID tag** is a circuit like RFID tag, that is activated by induction like the RFID tag and that transmits data only to receivers that are in direct contact with the tag. such transmission is used in car keys with immobilizer circuits.

[0018] **Handshaking** is a term which indicates bidirectional serial communication and refers to the process of synchronizing and controlling the communication by using predefined signals such as Request To Send (RTS) etc.

DETAILED DESCRIPTION

[0021] One of the problems with incorporating the use of biometric parameters into a security device to create an Enhanced Security Device (ESD) is that the detection and the use of biometric information may change the manner in which the user accesses the ESD. For example, if an iris or retina reader is incorporated into an ESD, the user would be required to place their eye in close proximity with an iris or retina scanner in order for the ESD to be able to distinguish the identity of the individual attempting to access the ESD. This process would require the individual attempting to access the ESD to modify the manner in which they attempt to gain access to the ESD. A third party observing the individual attempting to access the ESD may then be alerted to the type of biometric information being used to access the ESD. Additionally the user must learn to implement a new task to operate the ESD.

[0022] The present invention incorporates the use of biometric information within the security device in a manner such that the actions taken by the individual accessing the ESD are not noticeably modified and without changing or adding to the normal procedures used to access prior versions of the device. For example, and without limitation, a fingerprint scanner may be incorporated into a conventional appearing key used to access a security device such that biometric information, in this case characteristics of the fingerprint, may be collected from the user and used to determine if the individual is authorized to access the ESD. In this example, the user needs to do nothing more than to use the key in its normal manner, and the ESD will ensure that both the biometric information and the mechanical characteristics of the key are correct before the individual is granted access to the property, information or item of value. In other words, in the case in which the reader of the biometric information can be incorporated into a physical device used to open a security device, such as a key to a lock, the user will not be required to change their procedure for, or manner of accessing, the device and apparent use of

the key to operate the lock to obtain the advantage of the enhanced security features of the present invention. In the case of a fingerprint reader incorporated into a physical key (e.g., into the bow portion of a key or affixed to a conventional key as a snap bow), the individual attempting to access the device would perform the normal action of inserting the key blade into the lock, turning the key after it has been inserted into the cylinder slot and opening the door or container containing the lock. Similarly, a biometric sensor or reader, such as a fingerprint reader, may be incorporated into a transducer (e.g., a keyboard, mouse, trackball, joystick, touchpad, tablet, palm rest, stylus, and similar devices) to identify individuals using the keyboard to access protected information such as classified material; a fingerprint reader may be incorporated into an access card (e.g., a "smartcard"); a fingerprint reader may be incorporated into an access keypad; a palm blood vessel reader may be incorporated into a combination lock such that when a user holds the combination lock in their hand to open it biometric information is obtained and compared to biometric information previously stored in memory. In these cases, biometric information is obtained and used to enhance security while an otherwise conventional device is normally operated and/or used.

[0023] FIG. 1 illustrates a physical key 101 which had been modified to include a biometric reader (or sensor) incorporated into a bow portion of the key, in this case the biometric reader comprising a fingerprint reader 102. Physical key 101 also includes key contacts 103 preferably positioned along or in a blade portion of the key. Key contacts 103 may be used to establish a connection with the security device for which physical key 101 is used to access. The connection between physical key 101 and the security device (e.g., a combination mechanical lock and electrical interface or reader) may be an electrical connection, or may be any type of connection which allows the transfer of information (e.g., biometrics) from physical key 101 to the security device. Additionally physical key 101 may include physical "keying" such that

physical key 101 will only turn or rotate within a security device when the security device has corresponding "keying," such as is used in a conventional key and lock combination as will be familiar to those of ordinary skill in the art.

[0024] FIG. 2 shows one embodiment of the present invention in which two pairs of contacts located within an enhanced security device are used, along with a processor (e.g., microprocessor, controller, PCA, etc.) and memory, to ensure biometric information is correct before the lock can be opened. Referring to FIG. 2, two pairs of contacts, fixed contact 201 and rotating contact 202 are illustrated. Fixed contact 201 may be located on the lock or secured device (such as a door) and rotating contact 202 may be located within lock cylinder 203 as shown. In this configuration, rotating contact 202 rotates together with the lock cylinder 203 as it is rotated. As will be described in detail below, the contacts may be used to permit access to a specific individual if the biometric information read by fingerprint reader 102 (FIG. 1) matches stored biometric information. Conversely, access is denied to any other individual when the biometric information read by fingerprint reader 102 fails to successfully compare to stored biometric information. Additional criteria may also be specified and used to control access (e.g., key identification data, time of day, key expiration information, required quality of biometric match values, etc.). In this configuration when the ESD is locked and physical key 101 is inserted in the key slot, key contacts 103, fixed contacts 201 and rotating contacts 202 are configured to allow information to be transmitted from physical key 101 to a comparator such as a fingerprint recognition chip attached to fixed contacts 201. The term comparator includes any central processing unit, processor, chip, controller or other device which may accomplish the described functions including verification based on biometric sensor information and stored biometric information.

[0025] FIG. 3 shows a flow chart of the process for which biometric information is checked prior to the opening of the ESD. Steps 301 to 307 in FIG. 3 describe how the biometric information obtained by the fingerprint reader 102 (FIG. 1) is used in addition to the traditional physical indentations (i.e., keying or bitting) in the key (not shown). As the user holds physical key 101 with the bow portion of the key between the thumb and the index, fingerprint reader (or scanner) 102 transmits biometric information (uniquely identifying an individual) to a processor (not shown) located in the door or elsewhere. The biometric information collected from fingerprint reader 102 may consist of information regarding a single fingerprint as in the case of a single fingerprint reader being included within physical key 101, or for additional security or convenience, may include biometric information collected from more than one fingerprint reader 102 that has been included within physical key 101. When more than one fingerprint reader 102 is included within physical key 101 additional security may be obtained by requiring that all of the biometric information collected from each fingerprint reader 102 match corresponding biometric information stored in memory 309 before the ESD is opened. For additional convenience, when more than one fingerprint reader 102 has been included within physical key 101, matching information from a single fingerprint may be required for accessing the security device to allow for the possibility that the individual attempting to access the ESD is not making adequate contact with either or both of the fingerprint readers 102 included within physical key 101. Quality of match criteria may also be established so that some combination of fingerprint reader information may be used to collect sufficient data to achieve a desired confidence level. One of ordinary skill in the art would also appreciate that the handle of physical key 101 may be ergonomically designed to ensure that the user grasps physical key 101 in a manner conducive to the gathering of biometric information.

[0026] Fingerprint reader 102 may receive its energy (i.e., operating power) from a power source located in door 308 through flat cable contacts (not shown) or by induction as described with reference to FIG. 4. Additionally, fingerprint reader 102 may transmit the fingerprint data through other flat cable contacts (or by induction without any cable). When a match is obtained between the biometric information obtained by fingerprint reader 102 and the information stored within memory 309, security pin (or latch) 310 may be electromechanically operated and thereby open and allows cylinder 203 of the ESD to be turned by physical key 101. The successful comparison (e.g., satisfaction of one or more criteria) between the fingerprint information obtained from fingerprint reader 102 and the information stored within memory 309 (i.e., resulting in "fingerprint approval") may be used within the ESD as backup data in addition to the physical indentations on the key to ensure that both the key is the correct key and that the individual holding the key is the correct individual to access the security device. In this embodiment rotation of physical key 101 may be inhibited by an electromagnetic release which is only activated by a successful fingerprint comparison.

[0027] Referring again to FIG 3, in Step 301 door 308 is secured closed and protected by an ESD. In Step 302 the individual attempting to access the door protected by an ESD holds physical key 101 between their fingers in a manner in which one or more of their fingers are in physical contact with one or more fingerprint readers 102 contained on or in a bow portion of physical key 101. Alternatively, fingerprint reader 102 may be part of a snap bow affixed to an underlying bow portion of the key. Use of a snap bow provides for retrofitting of a biometric reader device and/or other transponder technology to conventional keys for use in access control systems. In Step 303, the individual attempting to access the door protected by the ESD then inserts physical key 101 into key slot 311. As physical key 101 is fully inserted into key slot 311, key contacts (fixed on physical key 101) may physically touch and/or engage

rotating contacts 202 (FIG. 2) at or along the opening of cylinder 203. Rotating contacts 202 (FIG. 2) are engaged with fixed contacts 201 when the ESD is in the locked position. Fixed contacts 201 are communicatively joined to a comparator, such as a fingerprint recognition card. The exchange of information from physical key 101 to fingerprint recognition card may also be achieved by wireless or contactless means such as inductive, magnetic, electromagnetic (i.e., R.F.), capacitive, optical or other couplings without any physical connection between physical key 101 and fingerprint recognition card (this is similar to the RFID "immobilizer" chips that may be included within an automobile key). In Step 304 the biometric information obtained from fingerprint reader 102 is compared to stored biometric information by a Fingerprint Recognition (FR) chip unit. In Step 305, if the information obtained from fingerprint reader 102 successfully matches the stored biometric information, security pin (or latch) 310 is electromechanically retracted in a manner which permits the cylinder of the ESD to be turned by physical key 101. In Step 306 the individual attempting to access the ESD turns physical key 101 and cylinder 203 is turned in the process. In Step 307 the ESD is disengaged and door 308 may be opened.

[0028] In a preferred embodiment of the present invention, three sets of contacts are used, key contacts 103, fixed contacts 201 and rotating contacts 202. As described above, key contacts 103 are located on physical key 101 and make a physical connection with fingerprint scanner 102. Rotating contacts 202 may be physically located on the lock cylinder. Rotating contacts 202 makes a physical connection with key contacts 103 when physical key 101 is inserted into the key slot which is included within the lock cylinder. Fixed contacts 201 makes a physical connection with a comparator such as fingerprint recognition card. When the lock cylinder is in the locked position, biometric information obtained by fingerprint scanner 102 can be transmitted from fingerprint scanner 102 to the comparator through key contacts 103, rotating contacts 202 and fixed contacts 201. Two of the wires of key contacts 201 supply voltage to

fingerprint reader 102 and three other wires may be used for communication (e.g., a common or "ground", data transmit and receive connections). When the fingerprints of the individual attempting to access the ESD are scanned the information may be sent by way of key contacts 103, through rotating contacts 202, through fixed contacts 201 to a processing unit (not shown). The processing unit may be implemented as an appropriately programmed and configured microprocessor, controller, programmed logic array (PLA) or other dedicated device and/or software. In appropriate situations, this functionality may be provided by software running on a general purpose platform such as a personal computer. One of ordinary skill in the art would appreciate that the processing unit need not be installed in door 308 itself but may be located remotely. One of ordinary skill in the art would appreciate that when the present invention is implemented using RFID these the key contact, the fixed contact and the rotating contact may not be required.

[0029] FIG. 4 illustrates how RFID technology may be used with the present invention. In Step 401 the ESD is locked. In Step 402 the individual attempting to access the door protected by an ESD holds physical key 101 between their fingers in a manner in which one or more of their fingers are in physical contact with and/or close proximity to one or more fingerprint readers 102 contained on physical key 101. In Step 403, biometric information from fingerprint reader 102 is transmitted by RFID to a receiver which is attached to, or in communication with, the lock cylinder of the ESD. This information may be transmitted when the individual accessing the system approach the ESD or when the individual inserts physical key 101 into key slot of the ESD. In Step 404 the biometric information obtained from fingerprint reader 102 is stored into the Random Access Memory (RAM) of the ESD. In Step 405, the biometric information received from fingerprint reader 101 is compared to biometric information stored in Read Only Memory (ROM) of authorized users. One of ordinary skill in

the art would appreciate that the information may be stored in other types of memory. In step 406, if the information obtained from fingerprint reader 102 successfully matches the stored biometric information, security pin (or latch) is retracted in a manner which permits the cylinder of the ESD to be turned by physical key 101. In Step 407 the individual attempting to access the ESD turns physical key 101 and the cylinder of the ESD is turned in the process and the authorized user disengages the ESD.

[0030] FIG. 5 illustrates the various components of the present invention which includes the fingerprint reader card, the door circuit, the learning process and the identification process. As shown therein, physical key 501 includes fingerprint reader 502 that is capable of collecting biometric information from contact with a user. Physical key 501 also contains contacts 503 and may include an RFID transmitter 504.

[0031] Door circuit 505 may include an energy transmitter (not shown), electromagnetic pin 506, a lock decoder/encoder, a key decoder/encoder and a key fingerprint scanner. For example, the energy transmitter may be an oscillator that causes a low frequency (several KHz) magnetic flux change in a small coil. Electromagnetic pin 506 is pulled by an electromagnet (e.g., comprises a solenoid) which may receive its energy from a switch, such as solid state power switch IRF830 available from International Rectifier, Inc. or may be a conventional electromechanical relay. The power switch may receive its signal from fingerprint recognition card (or chip) when a successful comparison is performed between the information obtained by fingerprint reader 102 and the fingerprint information stored in memory 507. The lock decoder/encoder is similar to the immobilizer circuits which may be installed within vehicle security and ignition systems.

[0032] The decoder may be connected by hardwiring to the lock. In this configuration the analog signal that is transmitted from the key may be converted by an analog to

digital chip into a digital signal. The digital signal may then be further translated into bits by an additional chip and may be processed as desired. The decoder may also transmit the digital information received from the fingerprint recognition card through the lock into the key. The key decoder is operational for encoding the scanner data and of sending it into the door lock. It is also capable of decoding data for serial handshaking communication. The key fingerprint scanner may be used to scan the thumb that holds the key and send the data to the key decoder/encoder.

[0033] A learning mode may also be included to provide the ability to record new biometric information so that additional individuals may be authorized to access the ESD. The learning mode may be initiated by the user by pressing a learning button contained on the comparator or the fingerprint recognition card or in a similarly secured area near or contained within the ESD. One of ordinary skill in the art would appreciate that appropriate security procedures would be incorporated to insure the new user is authorized to access the ESD prior to their biometric information being stored in memory 507. Once the learning process is initiated, the user may place the center of their thumb on the fingerprint scanner that is attached to the fingerprint recognition card until the fingerprint recognition card informs the user that information corresponding to their thumb has been successfully stored within memory 507. This information may be conveyed by the system to the user by illumination of one or more LEDS or by generation of an acknowledgement sound. Alternatively, the user may grasp the key in a manner which allows their biometric information to be determined and use the fingerprint reader 102 included in physical key 101 to enter their biometric information into the system when the fingerprint recognition card is in the learn mode. A second mode, such as an operational mode, would also be available such that when the fingerprint recognition card is in the operation mode

it would only perform comparisons between information read by fingerprint reader 102 and stored biometric information.

[0034] As described above, the identification process begins when a physical key is inserted into the key slot of the ESD. In one embodiment, a capacitor may be charged by an inductively coupled voltage source and may be used to provide power to fingerprint scanner 102. The key fingerprint scanner scans the user's thumb. The key encoder/decoder translates the fingerprint data into a serial signal. The serial signal is received by the door's encoder/decoder and is translated into a series of bits. The series of bits is sent to the fingerprint recognition card for approval. The fingerprint recognition card searches for a match. Once a match is found, the card signals the approval to a power switch such as IRF830. The power switch closes the pin electromagnet circuit, disengaging the pin thus allowing the lock's bolt to rotate (assuming any physical keying requirements, e.g., mechanical lock activation are also satisfied). The user turns the key and the door opens.

[0035] Referring to FIG. 6, another novel aspect of the present invention is that a conventional lock may be retrofitted to become an ESD. In this case the removable cylinder of the conventional lock and the key from the conventional lock would be replaced with an ESD cylinder and an ESD key. The ESD cylinder may include a security pin (or similar device such as built-in locking pins) which would be used in conjunction with the ESD key and the comparator to ensure that access to the ESD is denied until the appropriate biometric information is successfully compared. The ESD key would include a biometric sensor, such as a fingerprint reader. In addition a comparator, included in card unit of FIG 6, such as a fingerprint recognizer chip or a similar device may be required to ensure access to the ESD device is only obtained when a successful comparison is performed between the biometric information that is read and the stored biometric information. In this configuration biometric information gathered by

fingerprint reader is sent via RFID to the fingerprint recognizer chip. If the comparison between the biometrics reader (or sensor) and the stored biometrics is successful, fingerprint recognizer chip (or Card Unit of FIG. 6) sends a RFID signal to the security pin included on the ESD cylinder (lock cylinder of FIG. 6) to disengage the security pin. Once the security pin has been disengaged, the ESD key may be used to access the room, property or object protected by the ESD. One of ordinary skill in the art would appreciate that the present invention may be implemented in a central system to affect access to a number of ESDs. For example, a fingerprint recognition card could be located within a building and each lock cylinder within each conventional lock may be replaced with an ESD cylinder. Now only authorized individuals would have access to each of the retrofitted locks (now ESDs) and would use an ESD key to gain access.

[0036] While the present invention has been described through the use of a fingerprint reader on a physical key which is inserted into the key slot of a cylinder of a ESD, one of ordinary skill in the art would appreciate that the current invention includes the use of other biometric information used in other security devices. Additionally, while the present invention has been described with the memory and the fingerprint recognition chip unit being separated from the physical key, additional and alternative configurations are possible and one of ordinary skill in the art would appreciate that as the size of memory, processing units and chips continue to decrease, the present invention would also include the integration of the biometric reader, the memory and the processing of the information in one location, e.g., within and/or as part of a physical key.

CLAIMS

What is claimed is:

1. An enhanced security device includes:

an access device ,

a biometric reader attached to said access device,

a memory configured to receive data from said biometric reader,

wherein said biometric reader is used in conjunction with a learning mode to store known biometric information for comparison at a later time, and

a security device associated with said access device,

a comparator including said learning mode and a utilization mode which performs a comparison in said utilization mode between unknown biometric information obtained from said biometric reader and said known biometric information stored in said memory such that the utility of said access device is dependent on said comparison.

2. The enhanced security device of claim 1 wherein said access device is a physical key.

3. The enhanced security device of claim 1 wherein said biometric reader is a fingerprint reader.

4. The enhanced security device of claim 1 wherein said comparison is performed by a processor.

5. The enhanced security device of claim 4 wherein said information is transmitted from said biometric reader to said processor through electrical contacts.

6. The enhanced security device of claim 4 wherein said information is transmitted from said biometric reader to said processor by inductive coupling.

7. The enhanced security device of claim 1 wherein said access device includes a set of contacts.

8. The enhanced security device of claim 7 wherein said set of contacts includes a key contact, a rotating contact and a fixed contact.

9. The enhanced security device of claim 8 wherein said rotating contact is located on a lock cylinder.

10. The enhanced security device of claim 8 wherein information is transmitted from said key contact to said rotating contact to said fixed contact when said enhanced security device is in a locked position.

11. The enhanced security device of claim 1 wherein said security device is a mechanically operated lock.

12. The enhanced security device of claim 11 wherein said mechanically operated lock includes a cylinder.

13. The enhanced security device of claim 12 wherein said cylinder includes a plurality of electrical contacts configured to engage a corresponding set of contacts upon insertion of a key into said cylinder.

14. The enhanced security device of claim 1 wherein said utility of said access device is the disengagement of said security device.

15. The enhanced security device of claim 1 wherein said biometric reader obtains its operating voltage through a radio frequency voltage transmission.

16. The enhanced security device of claim 15 wherein said RFID voltage transmission is secure.

17. The enhanced security device of claim 1 further including an immobilizer key.

18. The enhanced security device of claim 1 further including a security pin.

19. The enhanced security device of claim 18 wherein said security pin is used to determine the utility of said access device.

20. An enhanced security device comprising:

an access device ,

a biometric reader attached to said access device wherein said biometric reader is used in a utilization mode and in a learning mode,

a memory configured to receive and store data from said biometric reader,

a security device associated with said access device, and

means for denying access to said enhanced security device.

21. The enhanced security device of claim 20 wherein said access device is a physical key.

22. The enhanced security device of claim 20 wherein said biometric reader is a fingerprint reader.

23. The enhanced security device of claim 20 wherein said access device includes a set of contacts.

24. The enhanced security device of claim 20 wherein said security device is a physical lock.

25. The enhanced security device of claim 24 wherein said physical lock includes a cylinder.

26. The enhanced security device of claim 25 wherein said cylinder includes contacts.

27. The enhanced security device of claim 20 wherein said utility of said access device is the disengagement of said security device.

28. The enhanced security device of claim 20 wherein said biometric reader obtains its operating voltage through RFID voltage transmission.

29. The enhanced security device of claim 28 wherein said RFID voltage transmission is secure.

30. The enhanced security device of claim 1 further including an immobilizer key.

31. The enhanced security device of claim 1 further including a security pin.

32. The enhanced security device of claim 31 wherein said security pin is used to determine the utility of said access device.

33. A security device comprising:

a key including

(i) a bow portion having attached thereto a biometric sensor operational to collect biometric data from a user wherein said biometric sensor is used in a utilization mode and in a learning mode,

(ii) a blade portion for accepting a plurality of cut therein so as to operate a mechanical lock by insertion of said blade portion into a cylinder portion of said mechanical lock, and

(iii) a data interface configured to transmit said biometric data to a control circuit wherein said control circuit is operational to selectively enable operation of the cylinder in response to said biometric data.

34. A biometric sensor of claim 33 wherein a biometric sensor comprises a sensor selected from the group consisting of a fingerprint reader, pressure transducer, palm blood vessel reader, iris recognition and voice recognition devices.

35. A data input device comprising:

a transducer configured to be manually operated by a user to provide an input signal,

a biometric sensor configured to collect biometric data from the user while the user is operating said transducer wherein said biometric sensor is used in a utilization mode and in a learning mode; and

a controller responsive to the biometric data for selectively enabling said input signal.

36. A biometric sensor of claim 35 wherein a biometric sensor comprises a sensor selected from the group consisting of a fingerprint reader, pressure transducer, palm blood vessel reader, iris recognition and voice recognition devices.

37. A transducer of claim 35 wherein a transducer comprises an input device selected from the group consisting of a keyboard, mouse, trackball, joystick, touchpad, tablet, palm rest and stylus.

38. A method of updating a conventional security device to an enhanced security device comprising the steps of:

replacing a conventional cylinder of said conventional security device with an enhanced cylinder,

replacing a conventional key of said conventional security device with an enhanced key wherein said enhanced key included a biometric reader,

locating a comparator card within RFID range to said enhanced security device wherein said comparator card compares information received from said biometric reader to stored biometric information to allow said enhanced security device to be accessed.

39. The method of claim 38 wherein communications between said enhanced key and said comparator card are RFID communications.

40. The method of claim 38 wherein communications between said comparator and said enhanced cylinder are RFID communications.

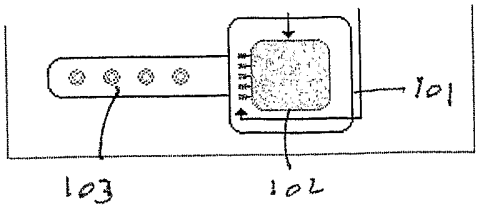


Fig 1

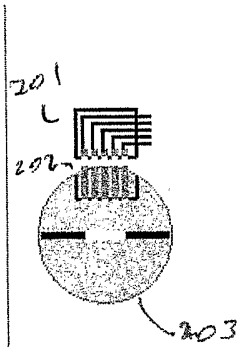


FIG 2.

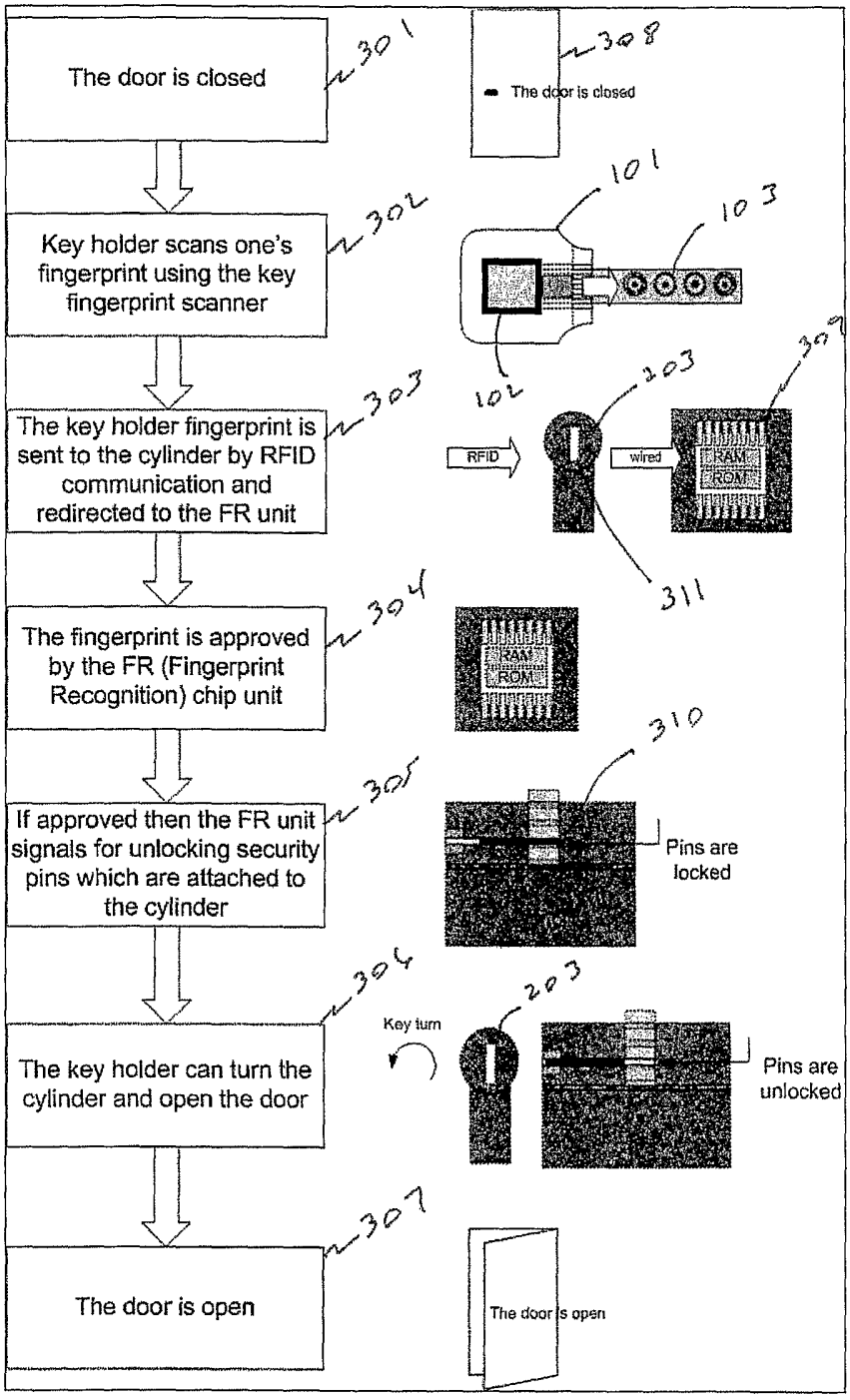
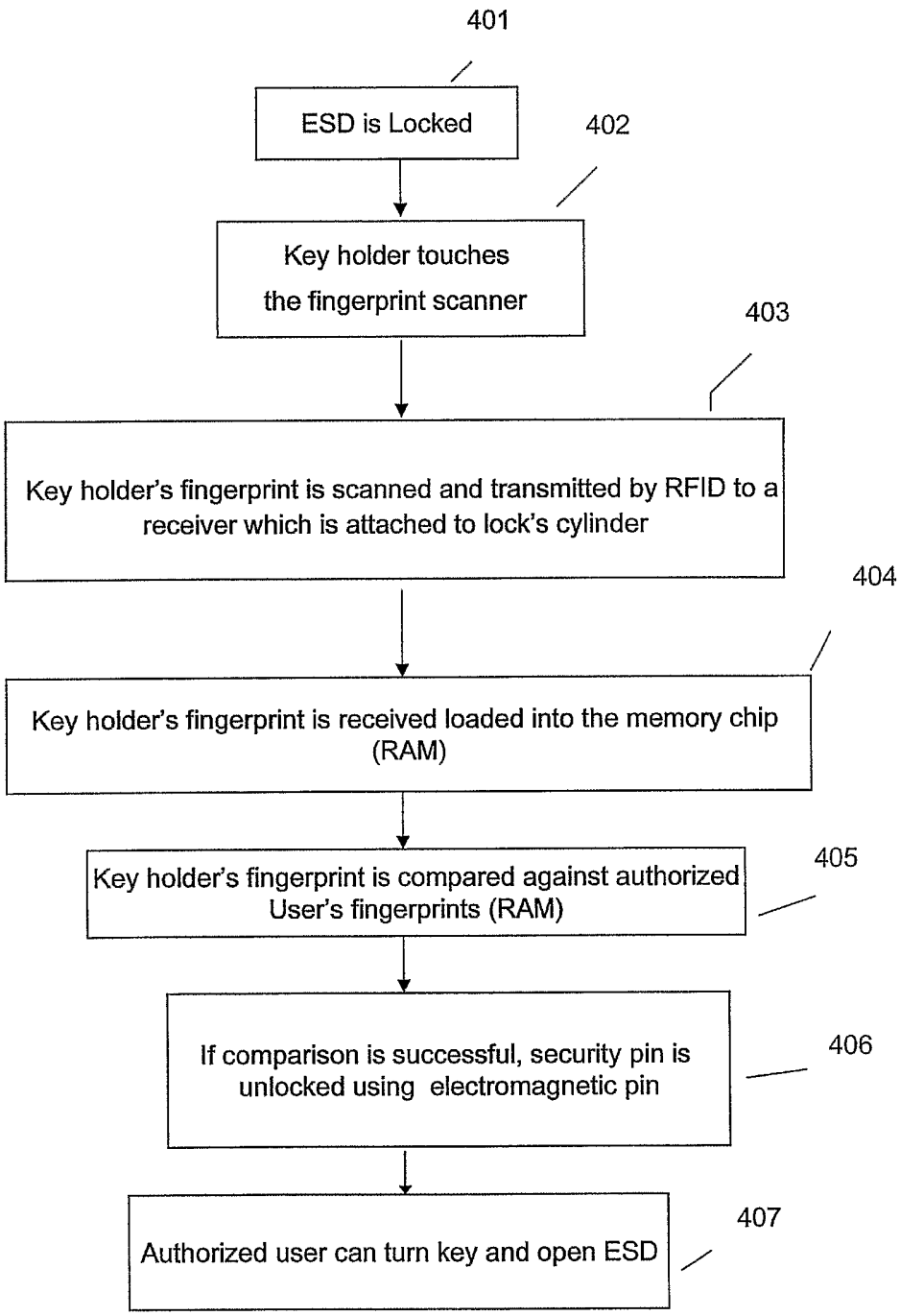

The door is closed
301
Key holder scans one's fingerprint using the key fingerprint scanner
302
The key holder fingerprint is sent to the cylinder by RFID communication and redirected to the FR unit
303
The fingerprint is approved by the FR (Fingerprint Recognition) chip unit
304
If approved then the FR unit signals for unlocking security pins which are attached to the cylinder
305
The key holder can turn the cylinder and open the door
306
The door is open
307
308
The door is closed
101
103
102
203
309
RFID
wired
RAM
ROM
311
RAM
ROM
310
Pins are locked
Key turn
203
Pins are unlocked
The door is open

FIG. 3

FIGURE 4


401
ESD is Locked
402
Key holder touches the fingerprint scanner
403
Key holder's fingerprint is scanned and transmitted by RFID to a receiver which is attached to lock's cylinder
404
Key holder's fingerprint is received loaded into the memory chip (RAM)
405
Key holder's fingerprint is compared against authorized User's fingerprints (RAM)
406
If comparison is successful, security pin is unlocked using electromagnetic pin
407
Authorized user can turn key and open ESD

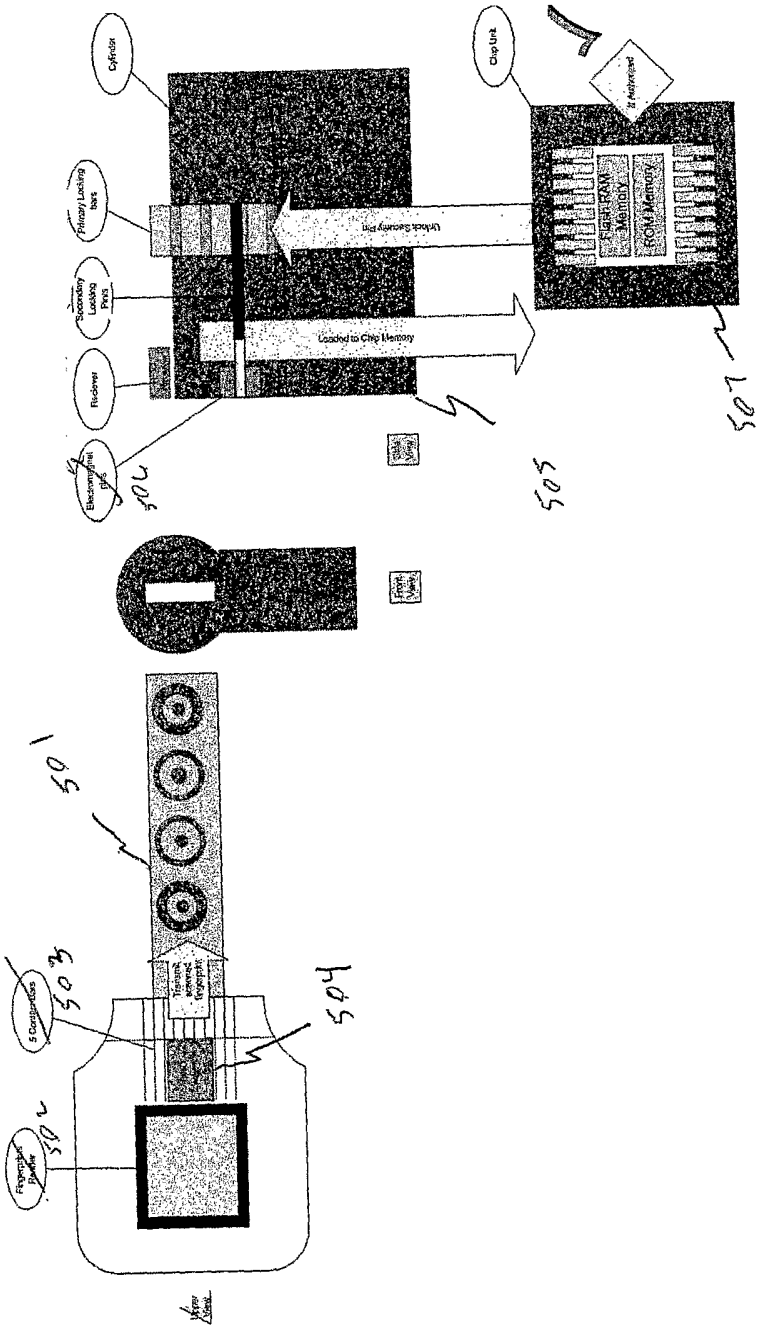

Cylinder
Primary Locking bars
Secondary Locking Pins
Fin driver
Electromagnet pins
Chip Unit
If Authorized
Unlock Security Pin
Loaded to Chip Memory
501
502
503
504
505
507

FIG 5.

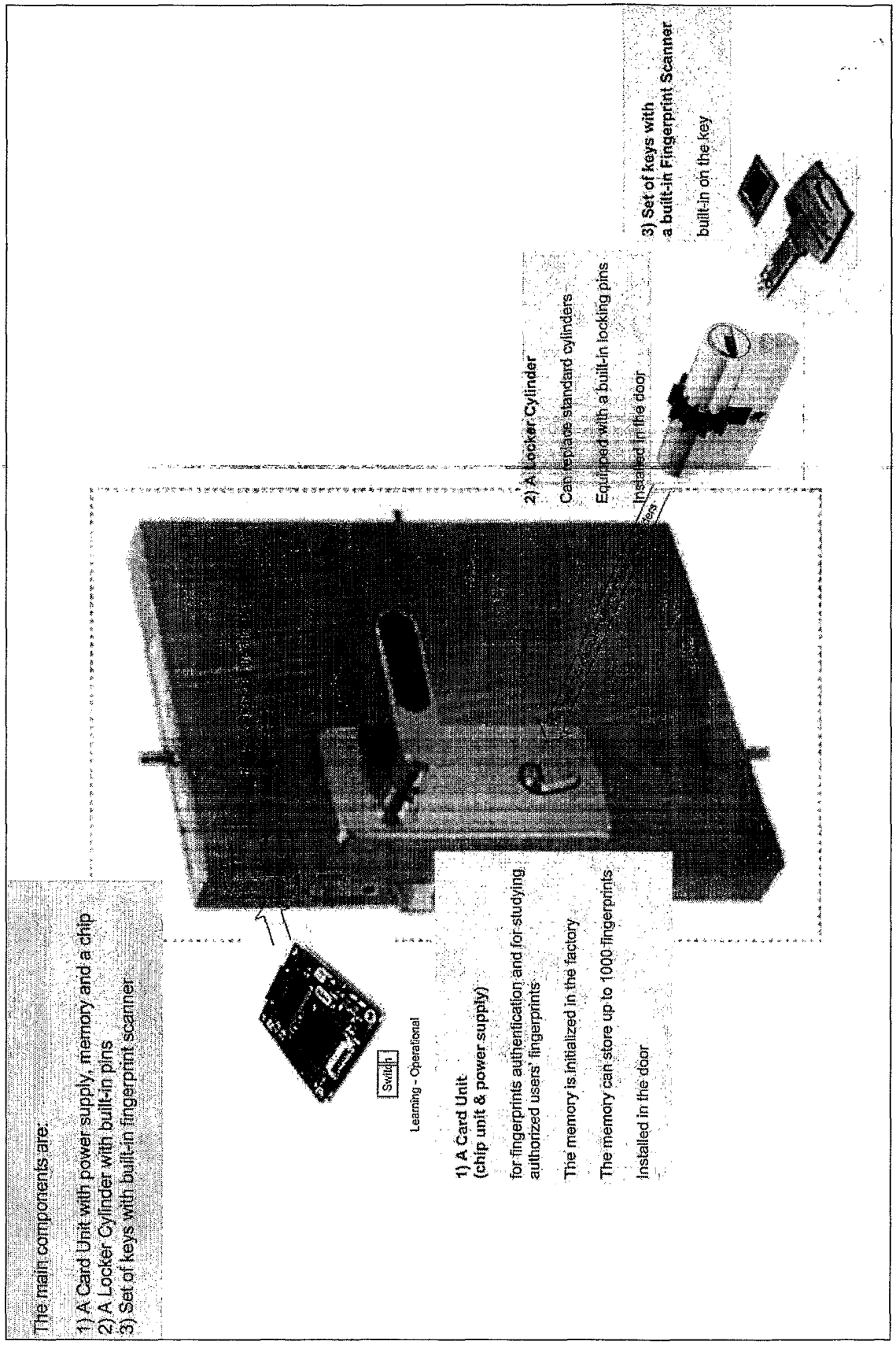

The main components are:
1) A Card Unit with power supply, memory and a chip
2) A Locker Cylinder with built-in pins
3) Set of keys with built-in fingerprint scanner
Switch
Learning - Operational
1) A Card Unit
(chip unit & power supply)
for fingerprints authentication and for studying authorized users' fingerprints
The memory is initialized in the factory
The memory can store up to 1000 fingerprints
Installed in the door
2) A Locker Cylinder
Can replace standard cylinders
Equipped with a built-in locking pins
Installed in the door
3) Set of keys with a built-in Fingerprint Scanner
built-in on the key

FIG 6.