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

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
28 March 2002 (28.03.2002)

PCT

(10) International Publication Number
WO 02/25038 A2

(51) International Patent Classification[7]: E05B

(21) International Application Number: PCT/KR01/01081

(22) International Filing Date: 25 June 2001 (25.06.2001)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
2000/026701(U.M.)
22 September 2000 (22.09.2000) KR

(71) Applicants *(for all designated States except US)*: **KIM, Won-Chol** [KR/KR]; 43-302 Daewoo Sawon Jutaek, 640, Naeson 2-dong, Gyeonggi-do, Uiwang-si 437-082 (KR). **KIM, Yang-Gue** [KR/KR]; 106-1204 Jugong Apartment, 242, Ben 3-dong, Gangbuk-gu, Seoul 142-063 (KR).

(72) Inventor; and
(75) Inventor/Applicant *(for US only)*: **JEONG, Myung-Geun** [KR/KR]; 970-21, Dapsimni 4-dong, Dongdaemun-gu, Seoul 130-034 (KR).

(74) Agents: **KIM, Bong-Hee** et al.; #501 Namdo Building, 823-24 Yeoksam-dong, Gangnam-gu, Seoul 135-933 (KR).

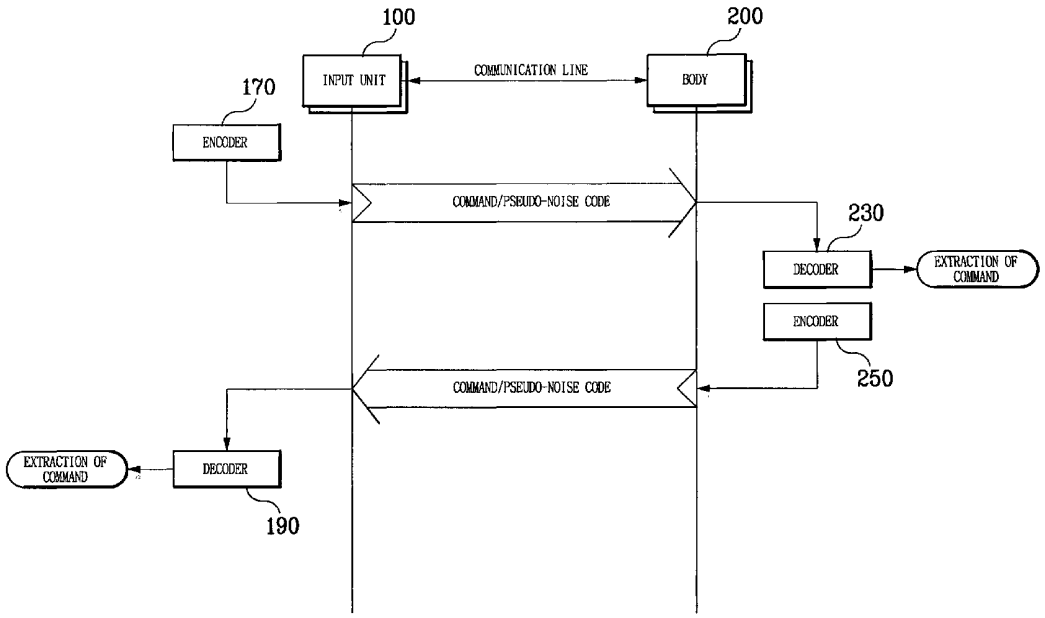
(81) Designated States *(national)*: AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BY, BZ, CA, CH, CN, CR, CU, CZ, DE, DK, DM, DZ, EE, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MA, MD, MG, MK, MN, MW, MX, MZ, NO, NZ, PL, PT, RO, RU, SD, SE, SG, SI, SK, SL, TJ, TM, TR, TT, TZ, UA, UG, US, UZ, VN, YU, ZA, ZW.

(84) Designated States *(regional)*: ARIPO patent (GH, GM, KE, LS, MW, MZ, SD, SL, SZ, TZ, UG, ZW), Eurasian patent (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European patent (AT, BE, CH, CY, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE, TR), OAPI patent (BF, BJ, CF, CG, CI, CM, GA, GN, GW, ML, MR, NE, SN, TD, TG).

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

[Continued on next page]

(54) Title: ELECTRONIC LOCKING APPARATUS AND CONTROL METHOD THEREOF



(57) Abstract: The present invention relates to a locking technology which can be adapted for use with the places requiring installation of an electronic locking apparatus for anti-theft purpose such as doors, safes, filing cabinets, cabinets, etc., and more particularly, an electronic locking apparatus which is divided into an input unit and a body and control method thereof in which an opening/closing (or unlocking/locking) of a door can be effected by a bi-directional communication method or a bi-directional encryption communication method, so that a leakage of password information to the outside is prevented and the electronic locking apparatus as a more powerful security system is implemented.

WO 02/25038 A2

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.

ELECTRONIC LOCKING APPARATUS AND CONTROL METHOD THEREOF

BACKGROUND OF THE INVENTION

Field of the Invention

The present invention relates to a locking technology which can be adapted for use with the places requiring installation of an electronic locking apparatus for anti-theft purpose such as doors, safes, filing cabinets, cabinets, etc., and more particularly, an electronic locking apparatus which is divided into an input unit and a body and control method thereof in which an opening/closing (or unlocking/locking) of a door can be effected by a bi-directional communication method or a bi-directional encryption communication method, so that a leakage of password information to the outside is prevented and the electronic locking apparatus as a more powerful security system is implemented.

Description of the Related Art

In general, it is safes that we have used to safely deposit valuable articles, things that we don't want other people to see, or articles that needs reserving in an unusual method in a living. Safes have commonly been used as deposit boxes for storing valuable articles, but currently, a great number of safes suitable for various purposes have been

manufactured and made available in the market. For example, safes with an excellent fire resistance and security ability according to the need of users, which includes household safes, office safes, hospital safes, wall safes, custom-made safes, etc., are manufactured using a specific material and equipment. Of course, the most important function of such safes is security. An excellent theft-preventing function is the first consideration with users upon the choice of a safe. Each manufacturing company of safes is immersed itself in a manufacture of safes with an excellent anti-theft function and advertises its products widely.

Meanwhile, features of currently used safes is that they are manufactured not to be ruined even when trying to destroy them by applying an intense impact to them or by using a tool such as a drill, etc., due to a development of materials. That is, such safes have a very excellent durability against an external impact. Accordingly, a method in which an external intruder releases a locking device for locking and unlocking a door of a safe rapidly and simply and robs it is to find an original solution of releasing the locking device. Locking devices of safes that have been used widely are implemented in diverse manners such as a dial type, a key inserting type, a button type, etc. Among these, a locking method of the conventional dial-type locking device is widely well known, so that there occur frequent thefts by intruders.

Also, for a locking method of the conventional key inserting-type locking device, a robbery technology is developed so that it becomes difficult to ensure security. A locking method of the conventional button-type locking device in which a user enters a password has an advantage in that he/she frees himself/herself from an inconvenience of having to carrying a key, so he/she enters a password which only he/she memorizes, thereby improving a security. Further, the number of combination-possible passwords can be established optionally so that a security is improved. However, one problem encountered with the conventional button-type locking device using a password is that it employs the fact that a signal for information about password itself is supplied to only a device for locking and unlocking a safe door, so password information is exposed over a communication line. In the event of a use of an identical password over a long period of time, there was a risk of exposing the password being used because the upper surfaces of key buttons corresponding to the password on a keypad, i.e., a key input section is worn by a frequent friction.

An explanation on disadvantages of the conventional safes will be in brief given hereinafter with reference to Figs. 1 and 2.

Fig. 1a is a perspective view illustrating a conventional cryptographic-based safe.

In Fig. 1, as described previously in the locking method of the conventional dial-type locking device, since a safe door unlocking technology used for a theft is widely well known, the cryptographic-based safe has a disadvantage in that there occur frequent thefts by intruders.

Fig. 1b is a perspective view illustrating a conventional digital safe employing an electronic keypad to open a door thereof.

In Fig. 1b, for such a digital safe employing such an electronic keypad, a locking device having both an electronic keypad and a storage battery built therein and a knob are mounted on a door of the digital safe. However, since it is easy to externally identify the position of a latch in the digital safe, an intruder can unlock the safe door in the event of a destruction of a corresponding portion thereof. Also, for a small safe, a user must enter a password with him/her bending down inconveniently, and must depress a reset button attached on the interior part of a safe door to alter the password after opening the safe door, which becomes burdensome. In addition, in the event of a use of an identical password over a long period of time, there was a risk of exposing the password being used because the upper surfaces of key buttons corresponding to the password on a keypad are worn by a frequent friction.

In the meantime, Fig. 2 is a conceptional block diagram

illustrating a unidirectional door unlocking control method used in a conventional button-type locking device of a safe.

Referring to Fig. 2, an input unit 1 and a locking device 3 for locking and unlocking a safe door are connected with each other by a certain number of power source supply lines through which to selectively supply a positive (+) power source and a negative (-) power source. Accordingly, when a user depresses corresponding keys through the input unit 1 to identify a password, the input unit 1 applies a door unlocking power source set by each of power source supply lines (Lines 1 to 4) to the locking device 3 to unlock or open a safe door. As shown in Fig. 2, in the event the input unit 1 and the locking device 3 are connected with each other by four power source supply lines, power source applying signals A01, A02, A03 and A04 for unlocking the safe door is set in such a fashion that a positive (+) power source is applied to the locking device 3 through Lines 1 and 4 and a negative (-) power source is applied thereto. Accordingly, when the input unit 1 identifies an input of a password, it supplies the power source applying signals A01, A02, A03 and A04 to the locking device 3 through the Lines 1 to 4 to open the safe door. As a result, a problem is caused due to the fact that the conventional button-type locking device adopts a unidirectional signal transferring method in which an external intruder can find out and enter a password, or inputs the

power source applying signals preset for the power source supply lines provided between the input unit 1 and the locking device 3 to the locking device 3 to open the safe door.

Further, for a locking device adapted for use with a conventional door, there has been a problem that the same locking schemes as those applied to the conventional safes as mentioned above are employed, so a user cannot free himself/herself from a risk of a theft.

SUMMARY OF THE INVENTION

Therefore, the present invention has been made in view of the above-mentioned problems, and it is an object of the present invention to provide an electronic locking apparatus and control method thereof which can basically prevent an external leakage of password information necessary for unlocking of the electronic locking apparatus mounted to doors, safes, filing cabinets, cabinets, etc., (or necessary for opening of a door), and implement the electronic locking apparatus as a more powerful security system.

It is another object of the present invention is to provide an electronic locking apparatus and control method thereof in which an input unit like a keypad of the electronic locking apparatus for performing an encryption communication is removed from a body thereof to remotely control the input

unit, so it is difficult to externally recognize a locking section, thereby implementing a dual security effect.

It is still another object of the present invention is to provide an electronic locking apparatus and control method thereof which uses a non-repeated optional authentication cipher code to enable an encryption communication between an input unit and a body of the electronic locking apparatus, thereby preventing a risk of password leakage.

It is yet another object of the present invention is to provide an electronic locking apparatus and control method thereof which uses a fractal function to which a chaos theory is applied for an encryption communication between an input unit and a body of the electronic locking apparatus.

It is a further object of the present invention is to provide an electronic locking apparatus and control method thereof in which a control section is provided to an input unit and a body of the electronic locking apparatus to control a bi-directional communication between the input unit and the body, so that an electronic locking of a door and a modification of a password are performed.

According to first aspect of the present invention, there is provided an electronic locking apparatus for performing a bi-directional communication, comprising:

an input unit including:

a key input section having a plurality of numeral keys

and functional keys, the key input section being adapted to generate a corresponding key signal if there is a key input from a user;

a memory adapted to store predefined command information and password information set by a user, the memory being locked to prevent an optional modification of the stored information;

a control section adapted to control a transmission/reception of a password numeral code signal and a command signal between the input unit and a body of the electronic locking apparatus to enable a bi-directional communication between the input unit and the body thereof, the control section being adapted to perform a locking/unlocking of a door and a registration/modification of a password through an identification of signals transmitted/received between the input unit and the body thereof;

a transmitting section adapted to transmit the password numeral code signal and the command signal to the body thereof under the control of the control section of the input unit;

a receiving section adapted to receive signals from the body thereof and supply the received signal to the control section of the input unit; and

a battery adapted to supply a power source required to drive the input unit to each constituent element thereof; and

a body including:

a control section adapted to control a transmission/reception of the password numeral code signal and the command signal between the input unit and the body of the electronic locking apparatus to enable a bi-directional communication between the input unit and the body thereof, the control section being adapted to perform a locking/unlocking of the door and a registration/modification of the password through an identification of the signals transmitted/received between the input unit and the body thereof;

a transmitting section adapted to transmit a password numeral code signal and a command signal to the input unit under the control of the control section of the body;

a receiving section adapted to receive the signals from the input unit and supply the received signals to the control section of the body;

a power source section adapted to supply a power source required to drive the body to each constituent element thereof;

a memory adapted to store the predefined command information and the password information set through the input unit, the memory being locked to prevent an optional modification of the stored information; and

a door locking section adapted to lock/unlock a door when receiving a door control command from the control section of the body.

According to second aspect of the present invention, the electronic locking apparatus may be applied to safes, doors, filing cabinets, cabinets, etc., and the input unit is implemented with a wireless remote control unit.

According to third aspect of the present invention, the electronic locking apparatus is applied to safes, doors, filing cabinets, cabinets, etc., and the input unit is mounted on the door to be connected with the body through a communication line or a cable.

According to fourth aspect of the present invention, the input unit further includes a display section adapted to display the overall states of the input unit according to the performances of a start mode, a door-opening (unlocking) mode and a password-modifying mode to inform the user of it.

According to fifth aspect of the present invention, the transmitting and receiving sections of the input unit implemented with the wireless remote control unit and the body are implemented by employing any one of an infrared communication scheme, a radio frequency (RF) communication scheme and a Bluetooth communication scheme.

According to sixth aspect of the present invention, the input unit and the body further includes a battery level detecting section and a power source level detecting section for detecting a power source level, respectively, to apply the detected power source level to the control sections of the

input unit and the body.

According to seventh aspect of the present invention, the input unit further includes an alarm section employing a buzzer or a speech transmitter to give an alarm to the user with a buzzer or a voice in the event of a detection of a low voltage from the battery, or to give an error alarm signal to the user.

According to eighth aspect of the present invention, there is also provided an electronic locking apparatus for performing a bi-directional encryption communication, comprising:

an input unit including:

a key input section having a plurality of numeral keys and functional keys, the key input section being adapted to generate a corresponding key signal if there is a key input from a user;

a memory adapted to store predefined command information, password information set by the user and a pseudo-noise (PN) code information, the memory being locked to prevent an optional modification of the stored information;

a control section adapted to control both corresponding constituent elements and the overall operation of the input unit to enable a bi-directional encryption communication between the input unit and the body thereof, the control section being adapted to control the input unit so that a

communication for clocking/unlocking a door is performed between the input unit and the body by using an encrypted signal in which a password for locking/unlocking the door is rejected through the authenticating of the password when the user inputs the password through the key input section, and adapted to allow the input unit to perform an encryption communication with the body by encrypting password information of partial digits in all the password information keyed in when the user inputs a new password through the key input section in a password-registering/modifying mode;

an encoder adapted to generate an optional pseudo-noise (PN) code having non-repeated and irregular properties under the control of the control section when a communication is performed between the input unit and the body, and then both mix a specific command signal to be transmitted to the body with the generated pseudo-noise (PN) code to generate an encrypted signal and mix the partial password information with an optional pseudo-noise (PN) code to generate an encrypted signal;

a transmitting section adapted to transmit the encrypted signals generated from the encoder to the body;

a receiving section adapted to receive an encrypted signal from the body; and

a decoder adapted to decode the encrypted signal applied thereto from the receiving section of the input unit in such a

fashion that the decoder rejects a pseudo-noise code from the encrypted signal to extract only pure command information or numeral code information for application to the control section.

a battery adapted to supply a power source required to drive the input unit to each constituent element thereof; and

a body including:

a control section adapted to control both corresponding constituent elements and the overall operation of the body to enable a bi-directional encryption communication between the input unit and the body thereof, the control section being adapted to allow the body to decode the encrypted signal received by the body when receiving it from the input unit and adapted to control a locking/unlocking of the door and a modification of the password through an identification of the decoded signal together with the input unit;

a receiving section adapted to receive the encrypted signals from the input unit;

a decoder adapted to decode the encrypted signals applied thereto from the receiving section of the body in such a fashion that the decoder rejects the pseudo-noise codes from the encrypted signals to extract only pure command information or numeral code information for application to the control section;

an encoder adapted to adapted to generate an optional

pseudo-noise (PN) code having non-repeated and irregular properties under the control of the control section of the body when a communication is performed between the input unit and the body, and then mix a specific command signal or a numeral code with the generated pseudo-noise (PN) code to generate an encrypted signal;

a transmitting section adapted to transmit the encrypted signals generated from the encoder of the body to the input unit;

a power source section adapted to supply a power source required to drive the body to each constituent element thereof, the power source section adapted to be constructed to selectively use a battery voltage and a Direct Current (DC) source adapter;

a memory adapted to store predefined command information, password information set by the user and a pseudo-noise (PN) code information, the memory being locked to prevent an optional modification of the stored information; and

a door locking section adapted to lock/unlock the door when receiving a door control command from the control section of the body.

According to ninth aspect of the present invention, the electronic locking apparatus is applied to safes, doors, filing cabinets, cabinets, etc., and the input unit is

implemented with a wireless remote control unit.

According to tenth aspect of the present invention, the electronic locking apparatus is applied to safes, doors, filing cabinets, cabinets, etc., and the input unit is mounted on the door to be connected with the body through a communication line or a cable.

According to eleventh aspect of the present invention, the input unit further includes a display section adapted to display the overall states of the input unit according to the performances of a start mode, a door opening (unlocking) mode and a password modifying mode to inform the user of it.

According to twelfth aspect of the present invention, the transmitting and receiving sections of the input unit implemented with the wireless remote control unit and the body are implemented with a transmitting section and a receiving section employing any one of an infrared communication scheme, a radio frequency (RF) communication scheme and a Bluetooth communication scheme.

According to thirteenth aspect of the present invention, the input unit and the body further includes a battery level detecting section and a power source level detecting section for detecting a power source level, respectively, to apply the detected power source level to the control sections of the input unit and the body.

According to fourteenth aspect of the present invention,

the input unit further includes an alarm section employing a buzzer or a speech transmitter to give an alarm to the user with a buzzer or a voice in the event of a detection of a low voltage from the battery, or to give an error alarm signal to the user.

According to fifteenth aspect of the present invention, there is also a method of controlling an encryption communication in an electronic locking apparatus including an input unit with a key input section and a body with a door-locking section for opening/closing a door, the input unit and the body each having a control section, an encoder and a decoder, and being adapted to perform a bi-directional encryption communication therebetween, comprising the steps of:

a user password-authenticating step, when the user inputs a password used to open/close the door through the key input section of the input unit, for determining whether or not a user's registered password information stored in the input unit is identical with the password inputted by the user;

an encryption communication step, when the user's registered password information is identical with the password inputted by the user, for allowing the input unit to generate an optional pseudo-noise (PN) code having non-repeated and irregular properties and mix a command signal specified for an

opening/closing of the door with the optional pseudo-noise (PN) code to generate an encrypted signal through the encoder thereof to transmit it to the body, and allowing the body to receive the encrypted signal from the input unit and reject the pseudo-noise (PN) code from the received encrypted signal to extract only pure command information, so that after identifying the rejected pseudo-noise (PN) code and the extracted command information, a command signal indicating an identification of the extracted command information is read out and is mixed with an optional pseudo-noise (PN) code to generate an encrypted signal to transmit it the input unit; and

a door-opening/closing step for allowing the body to search a function specified for the extracted command information to open/close the door.

According to sixteenth aspect of the present invention, the encrypted signal employs a pseudo-noise (PN) code generated according to the encryption communication step based on a fractal function in the following [Expression 3] applied to a chaos theory,

[Expression 3]

$$y_1=f(x_1);$$

$$y_2=f(y_1);$$

$$y_3=f(y_2);$$

$$y_4=f(y_3);$$

. . . . .

$y_n=f(y_{n-1})$,

where f denotes a fractal function, x_1 denotes an initial value, and y_n denotes a pseudo-noise (PN) code value.

According to seventeenth aspect of the present invention, the encryption communication controlling method further includes the step of: when a normal opening/closing of the door is completed by the body, allowing the input unit to perform a display function for indicating that the normal opening/closing of the door has been completed.

According to eighteenth aspect of the present invention, the encryption communication controlling method further includes the step of: a password-registering/modifying step, when the encryption communication is performed for a registration/modification of the password, for allowing the input unit to mix a new password inputted by the user with an optional pseudo-noise (PN) code in such a fashion that numeral codes of the new password is bundled by an optional number upon the mixing of the new password with the optional pseudo-noise (PN) code to generate an encrypted signal which is transmitted to the body, and then allowing the input unit to replace an existing password preset in the body by the new password for registration/modification thereof when all the numeral codes including the first numeral code through the last numeral code of the new password have been transmitted to

the body through an encryption communication between the input unit and the body.

According to nineteenth aspect of the present invention, the encryption communication controlling method further includes the step of: an error displaying step for allowing the input unit to display a generation of an error when an abnormal encrypted signal is received in the encryption communication step or the body does not perform the opening/closing of the door normally.

According to twentieth aspect of the present invention, the command information is previously stored in the input unit and the body in a specific form by each encryption communication step.

According to twenty-first aspect of the present invention, the electronic locking apparatus for controlling the encryption communication is applied to safes, doors, filing cabinets, cabinets and the like.

According to twenty-second aspect of the present invention, there is also provided a method of controlling a bi-directional communication in an electronic locking apparatus including an input unit with a key input section and a body with a door-locking section for opening/closing a door, the input unit and the body each having a control section and being adapted to perform a bi-directional communication therebetween, comprising the steps of: a user password-

authenticating step, when the user inputs a password used to open/close the door through the key input section of the input unit, for determining whether or not a user's registered password information stored in the input unit is identical with the password inputted by the user; an encryption communication step, when the user's registered password information is identical with the password inputted by the user, for allowing the input unit to transmit a door-opening command to the body while allowing the body to receive the door-opening command from the input unit and transmit a door opening-identifying signal to the input unit, and then allowing the input unit to receive the door opening-identifying signal from the body and transmit a door opening-executing signal to the body; and a door-opening/closing step for allowing the body to open/close the door when the body receives the door opening-executing signal from the input unit.

According to twenty-third aspect of the present invention, the bi-directional communication controlling method further includes the step of: when a normal opening/closing of the door is completed by the body, allowing the body to transmit a door opening-displaying command to the input unit while allowing the input unit to perform a display function for indicating that the normal opening/closing of the door has been completed.

According to twenty-fourth aspect of the present invention, the bi-directional communication controlling method further includes the step of: a password-registering/modifying step, when the bi-directional communication is performed for a registration/modification of the password, for allowing the input unit to transmit a new password inputted by the user to the body in such a fashion that numeral codes of the new password is bundled by an optional number upon the transmission of the new password to the body, and then allowing the input unit to replace an existing password preset in the body by the new password for registration/modification thereof when all the numeral codes including the first numeral code through the last numeral code of the new password have been transmitted to the body through a password identifying procedure between the input unit and the body.

According to twenty-fifth aspect of the present invention, the bi-directional communication controlling method further includes the step of: an error displaying step for allowing the input unit to display a generation of an error when an abnormal encrypted signal is received in the bi-directional communication step or the body does not perform the opening/closing of the door normally.

According to twenty-fifth aspect of the present invention, the command information is previously stored in the input unit and the body in a specific form by each bi-

directional communication step.

According to twenty-fifth aspect of the present invention, the electronic locking apparatus for controlling the bi-directional communication is applied to safes, doors, filing cabinets, cabinets and the like.

BRIEF DESCRIPTION OF THE DRAWINGS

The foregoing and other objects, features and advantages of the present invention will become more apparent from the following detailed description when taken in conjunction with the accompanying drawings in which:

Fig. 1a is a perspective view illustrating a conventional cryptographic-based safe.

Fig. 1b is a perspective view illustrating a conventional digital safe employing an electronic keypad to open a door thereof.

Fig. 2 is a schematic conceptional block diagram illustrating a unidirectional door unlocking control method used in a conventional button-type locking device of a safe;

Fig. 3 is a block diagram illustrating an input unit of an electronic locking apparatus according to a preferred embodiment of the present invention;

Fig. 4 is a block diagram illustrating a body of an electronic locking apparatus according to a preferred

embodiment of the present invention;

Fig. 5 is a schematic conceptional block diagram illustrating a bi-directional encryption communication between an input unit and a body of an electronic locking apparatus according to the present invention;

Fig. 6 is a schematic block diagram illustrating a transmitting operation for implementing an encryption when unlocking or opening a door in an electronic locking apparatus according to one preferred embodiment of the present invention;

Fig. 7 is a schematic block diagram illustrating a receiving operation for implementing an encryption when unlocking or opening a door in an electronic locking apparatus according to one preferred embodiment of the present invention;

Fig. 8 is a schematic block diagram illustrating a transmitting operation for implementing an encryption when modifying a password in an electronic locking apparatus according to another preferred embodiment of the present invention;

Fig. 9 is a schematic block diagram illustrating a receiving operation for implementing an encryption when modifying a password in an electronic locking apparatus according to another preferred embodiment of the present invention;

Fig. 10 is a perspective view illustrating a wall incorporating a wall safe equipped with an electronic locking apparatus including an input unit and a body according to one preferred embodiment of the present invention, in which the input unit as a wireless remote control unit controls the body remotely to lock and unlock a safe door;

Fig. 11 is a perspective view illustrating a safe equipped with an electronic locking apparatus including an input unit and a body according to one preferred embodiment of the present invention, in which the input unit as a wireless remote control unit controls the body remotely to lock and unlock a safe door;

Fig. 12 is a plan view illustrating the outside of an input unit as a wireless remote control unit of an electronic locking apparatus according to one preferred embodiment of the present invention;

Fig. 13 is a perspective view illustrating a safe equipped with an electronic locking apparatus including a key input unit mounted on a safe door in an opened position and a body according to another preferred embodiment of the present invention, in which the key input unit as a wired control unit controls the body through a communication line to lock and unlock the safe door;

Fig. 14 is a block diagram illustrating the construction of an electronic locking apparatus which is implemented with a

bi-directional wireless encryption communication scheme according to one preferred embodiment of the present invention;

Fig. 15 is a block diagram illustrating the construction of an electronic locking apparatus which is implemented with a bi-directional wired encryption communication scheme according to another preferred embodiment of the present invention;

Fig. 16 is a flowchart illustrating a process routine of the input unit side for unlocking or opening a door when a user inputs a password through an input unit of an electronic locking apparatus according to one preferred embodiment of the present invention;

Figs. 17a and 17b are flowcharts illustrating process routines of the input unit side for performing an encryption communication between an input unit and a body of an electronic locking apparatus to unlock or open a door after identifying the user's input of the password according to one preferred embodiment of the present invention;

Fig. 18 is a flowchart illustrating a process routine of the input unit side for performing an encryption communication between an input unit and a body of an electronic locking apparatus to modify a password according to one preferred embodiment of the present invention;

Fig. 19 is a schematic block diagram illustrating a transmitting operation for implementing an encryption when

unlocking or opening a door in an electronic locking apparatus according to another preferred embodiment of the present invention;

Fig. 20 is a schematic block diagram illustrating a receiving operation for implementing an encryption when unlocking or opening a door in an electronic locking apparatus according to another preferred embodiment of the present invention;

Fig. 21 is a flowchart illustrating a process routine for unlocking or opening a safe door using an input unit as a wireless remote control unit of an electronic locking apparatus according to another preferred embodiment of the present invention;

Fig. 22 is a flowchart illustrating a process routine for modifying a password using an input unit as a wireless remote control unit of an electronic locking apparatus according to another preferred embodiment of the present invention;

Fig. 23a is a perspective view illustrating a door equipped with an electronic locking apparatus including an input unit and a body according to another preferred embodiment of the present invention, in which the input unit as a wireless remote control unit controls the body remotely to lock and unlock a safe door;

Fig. 23b is a perspective view illustrating a door

equipped with an electronic locking apparatus including a key input unit and a body mounted on the door according to another preferred embodiment of the present invention, in which the key input unit as a wired control unit controls the body through a communication line to lock and unlock the door;

Fig. 24a is a perspective view illustrating a cabinet equipped with an electronic locking apparatus including an input unit and a body according to another preferred embodiment of the present invention, in which the input unit as a wireless remote control unit controls the body remotely to lock and unlock a cabinet door;

Fig. 24b is a perspective view illustrating a cabinet equipped with an electronic locking apparatus including a key input unit and a body mounted on the cabinet according to another preferred embodiment of the present invention, in which the key input unit as a wired control unit controls the body through a communication line to lock and unlock a cabinet door;

Fig. 25a is a perspective view illustrating a filing cabinet equipped with an electronic locking apparatus including an input unit and a body according to another preferred embodiment of the present invention, in which the input unit as a wireless remote control unit controls the body remotely to lock and unlock a cabinet door; and

Fig. 25b is a perspective view illustrating a filing

cabinet equipped with an electronic locking apparatus including a key input unit and a body mounted on the filing cabinet according to another preferred embodiment of the present invention, in which the key input unit as a wired control unit controls the body through a communication line to lock and unlock a cabinet door.

DETAILED DESCRIPTION OF THE PREFERRED EMBODIMENT

Reference will now be made in greater detail to the preferred embodiments of the present invention. Throughout the drawings, it is noted that the same reference numerals or letters will be used to designate like or equivalent elements having the same function even though they are depicted in different drawings. The detailed description of known functions and configurations incorporated herein will be omitted when it may make the subject matter of the present invention rather unclear.

As shown in Figs. 14 and 15, an electronic locking apparatus 300 for a safe of the present invention includes an input unit 100 and an electronic locking apparatus body 200 (hereinafter, referred to as "body"). The input unit 100 and the body 200 are constructed to be controlled by each control section. Also, the input unit 100 of the present invention may be implemented with a bi-directional wireless remote

control unit (i.e., a remote controller) employing an infrared radiation (IrDA), a radio frequency (RF), a Bluetooth, etc., or may be implemented in such a fashion that a key input unit is mounted on a safe door to be connected with the body 200 through a communication line or a cable.

An electronic locking apparatus and control method thereof according to the present invention will be in detail described hereinafter with reference to the accompanying drawings.

First, Fig. 3 is a block diagram illustrating an input unit of an electronic locking apparatus according to a preferred embodiment of the present invention.

Referring to Fig. 3, there is shown an input unit 100 including a control section 110, a key input section 120, a display section 130, a memory 140, a battery level detecting section 150, a battery 160, a encoder 170, a transmitting section 180, a decoder 190 and a receiving section 195.

The control section 110 serves to control the overall operation of the input unit 100 in such a fashion that it controls a corresponding constituent element to perform a start mode, a door-opening (or unlocking) mode, a password-registering/modifying mode according to the present invention, and operates according to a preset program. Also, the control section includes a built-in counter 111 to control a check of the time for setting a key input, a check of the number of

times of setting a key input for re-transmission, etc.

The key input section 120, which includes a plurality of numeral keys and functional keys, serves to transmit a corresponding key signal to the control section 110 if there is a key input form a user.

The display section 130 is implemented with a light emitting diode (LED) or/and a liquid crystal display (LCD), and servers to display overall states according to the performances of a start mode, a door-opening (unlocking) mode and a password-modifying mode to inform a user of it.

The memory 140 serves to store password information set by a user, command information and pseudo-noise (PN) code information, etc. The memory 140 may be a flash memory. Also, the memory 140 may be locked to prevent a leakage of such information to the outside and a modification of them.

The battery level detecting section 150 serves to detect a power source level of the battery 160 for supplying a power source required to drive the input unit 100 to each of the constituent elements thereof to apply the detected power source level to the control section 110. The input unit 100 may include an alarm section employing a buzzer or a speech transmitter which has not been shown in the drawings to give an alarm to a user with a buzzer or a voice at the event of a detection of a low voltage from the batter, or to inform the user of a time for changing the battery through the display

section 130.

The encoder 170 serves to substitute an optional pseudo-noise (PN) code (having non-repeated and irregular properties) into a fractal function applied to a chaos theory under the control of the control section and multiply a command signal to be transmitted to the body 200 by a result of substituting the pseudo-noise code into the fractal function to generate an encoded or encrypted signal to supply the encoded or encrypted signal to the transmitting section 180 which transmits it to the body 200.

In the event the input unit 100 is a wireless remote control unit, for example, the transmitting section 180 is implemented with an infrared transmitter when the input unit 100 is a remote control unit using an infrared radiation, with a radio transmitter when it is a remote control unit using a radio frequency (RF), and with a Bluetooth chip when it is a remote control unit using a Bluetooth, respectively. Also, in the event the input unit 100 is mounted on a door, the transmitting section 180 may be a connector to which a communication line or a cable is connected.

The decoder 190 functions to decode an encrypted signal received by the receiving section 195 from the body 200, and reject a pseudo-noise code from the encrypted signal to extract only pure command information for application to the control section 110.

The receiving section 195 is constructed to correspond to the transmitting section 180.

Herein, an explanation on the encoder 170 and the decoder 190 will be in detail given with reference to Figs. 6 to 9 and Figs. 19 and 20 as will be described later.

Next, Fig. 4 is a block diagram illustrating a body of an electronic locking apparatus according to a preferred embodiment of the present invention.

Referring to Fig. 4, there is shown a body 200 including a control section 210, a receiving section 220, a decoder 230, a transmitting section 240, a encoder 250, a battery level detecting section 260, a power source section 270, a door locking section 280 and a memory 290.

The feature of the body 200 is that constituent elements such as a key input section and a display section are not mounted on the outside of the body. The control section 210 serves to control the overall operation of the body 200 in such a fashion that it controls a corresponding constituent element to perform a start mode, a door-opening (or unlocking) mode, a password-modifying mode according to the present invention to enable a bi-directional encryption communication between the input unit 100 and the body 200. Also, the control section includes a built-in counter 211.

The receiving section 220, the decoder 230, the transmitting section 240 and the encoder 250 of the body 200

are implemented to correspond to those of the input unit 100. The power source level detecting section 260 serves to detect a power source level of the power source section 270 for supplying a power source required to drive the body 200 to apply the detected power source level to the control section 210. The power source section 270 may be constructed so that both a battery and a Direct Current (DC) adapter are used as the power source section 270. At this time, the DC adapter converts an AC power source into a DC power source needed to internally drive of the body 200.

The door locking section 280 serves to actuate a solenoid coil when receiving a door-opening (or unlocking) command from the control section 210 to release a gear unit, spring or cam-structured latch so as to open or unlock a safe door. Also, the door locking section 280 serves to actuate the solenoid coil when receiving a door-closing (or locking) command from the control section 210 to lock the gear unit, spring or cam-structured latch so as to close or lock the safe door.

The memory 290 serves to store password information, command information and pseudo-noise (PN) code information, etc., received by the body 200 from the input unit 100. The memory 290 may be a flash memory. Also, the memory 290 may be locked to prevent a leakage of such information to the outside and a modification of them.

The command information and contents stored in the memory 290, and a bi-directional communication flow between the input unit 100 and the body 200 can be expressed like the following [table 1].

[Table 1]

Section	Order	Command number	Contents	Remarks
Door-opening mode	1	1	Open a door	Input unit → body
	2	2	Identify opening of a door	Input unit ← body
	3	3	Perform opening of a door	Input unit → body
	4	4	Door opening LED	Input unit ← body
Password-modifying mode	1	11	Modify a password	Input unit → body
	2	12	Identify modification of a password	Input unit ← body
	3	13	Existing password 1	Input unit → body
	4	14	Identify existing password 1	Input unit ← body
	5	15	Existing password 2	Input unit → body
	6	16	Identify existing password 2	Input unit ← body
	7	17	Existing password 3	Input unit → body

	8	18	Identify existing password 3	Input unit ← body
	9	19	Existing password 3	Input unit → body
	10	20	Identify existing password 4	Input unit ← body
	11	21	New password 1	Input unit → body
	12	22	Identify new password 1	Input unit ← body
	13	23	New password 2	Input unit → body
	14	24	Identify new password 2	Input unit ← body
	15	25	New password 3	Input unit → body
	16	26	Identify new password 3	Input unit ← body
	17	27	New password 4	Input unit → body
	18	28	Check Sum	Input unit ← body
	19	29	Store	Input unit → body
	20	30	Complete storing	Input unit ← body
Master key	1	41	Master serial	Input unit → body
	2	42	Identify master serial	Input unit ← body
	3	43	Password 1	Input unit → body
	4	44	Identify password 1	Input unit ← body
	5	45	Password 2	Input unit → body
	6	46	Identify password 2	Input unit ← body
	7	47	Password 3	Input unit → body
	8	48	Identify password 3	Input unit ← body
	9	49	Password 4	Input unit → body

	10	50	Identify password 4	Input unit ← body
Error	1	61	Mismatch of password	Input unit ← body
	2	62	Check Sum	Input unit → body
	3	63	Identify error	Input unit ← body

As shown in Figs. 3 and 4, the electronic locking apparatus is constructed in such a fashion that it includes the encoder/decoder and the transmitter/receiving sections for performing a bi-directional encryption communication between the input unit 100 and the body 200 so that the input unit 100 can transmit/receive a non-repeated and irregular encryption signal obtained by mixing a preset command signal with a pseudo-noise (PN) code used in an encryption technology to/from the body 200 to perform a door-opening mode, a password-registering/modifying mode, etc.

Fig. 5 is a schematic conceptional block diagram illustrating a bi-directional encryption communication between an input unit and a body of an electronic locking apparatus according to the present invention.

Referring to Fig. 5, a wireless or wired communication line is established between the input unit 100 and the body 200. When the input unit 100 allows the encoder 170 to mix a specific command signal with an optional pseudo-noise (PN) code to transmit a mixed encrypted signal to the body 200, the decoder 230 of the body 200 rejects the pseudo-noise (PN) code

from the encrypted signal received by the body 200 to extract only a pure command signal. Also, the body 200 may transmit an encrypted signal to the input unit 100. When the body 200 allows the encoder 250 to mix a specific command signal with an optional pseudo-noise (PN) code to transmit a mixed encrypted signal to the body 200, the decoder 190 of the input unit 100 rejects the pseudo-noise (PN) code from the encrypted signal received by the body 200 to extract only a pure command signal. Like this, the bi-directional encryption communication between the input unit 100 and the body 200 utilizes an irregular optional authentication cipher code called a pseudo-noise (PN) code, so that although an external measuring instrument or a signal monitor monitors the encrypted signal transmitted and received between the input unit 100 and the body 200, different signals always appears, and although an identical signal is monitored, a password is not exposed.

Now, an encryption scheme applied to a bi-directional communication between the input unit 100 and the body 200 of the electronic locking apparatus according to the present invention will be in detail described hereinafter with reference to Figs. 6 to 9.

First, a main principle of the encryption scheme according to the present invention is that when the input unit 100 requests the body to open or unlock a door, it does not

directly transmit password information itself to the body 200, but mixes a corresponding command signal with an optional pseudo-noise (PN) code to generate an encrypted or encoded signal for transmission to the body 200, and the pseudo-noise (PN) code is generated non-repeatedly and irregularly so that it can be modified and updated each time a door is opened or unlocked in order to keep the password information from being exposed by an external signal monitor.

Fig. 6 is a schematic block diagram illustrating a transmitting operation for implementing an encryption when unlocking or opening a door in an electronic locking apparatus according to one preferred embodiment of the present invention, and Fig. 7 is a schematic block diagram illustrating a receiving operation for implementing an encryption when unlocking or opening a door in an electronic locking apparatus according to one preferred embodiment of the present invention.

As shown in Figs. 6 and 7, in order to prevent a risk of a password exposure which can be occurred at the time of transmitting/receiving data between the input unit 100 and the body 200 of the electronic locking apparatus, when a transmitting end or one of the input unit 100 and the body 200 multiplies a command signal C01 by an optional pseudo-noise (PN) code C03 and a carrier (wave) signal C05 to generate an encrypted or encoded signal with a noise for transmission to a

receiving end or the other of the input unit 100 and the body 200, the receiving end rejects the carrier signal D03 and the pseudo-noise (PN) code D05 from the encrypted signal with a noise received by the receiving end to extract a pure command signal D06 so that a user can know desired command contents. The pseudo-noise (PN) code applied to the present invention may be configured to be modified each time a signal is transmitted/received between the input unit 100 and the body 200, and once a pseudo-noise (PN) code is set by both the input unit 100 and the body 200, the set pseudo-noise (PN) code may be used. The these two cases is more excellent than the case where an existing password information itself is transmitted/received between the input unit 100 and the body 200 in terms of a communication security. In particular, the former of the two cases will be more effective for a security. The implementation of the encryption as shown in Figs. 6 and 7 shows transmission/reception of an optional encrypted signal in which password information itself is concealed between the input unit 100 and the body 200 in a door-opening mode.

It is the most important for an encryption that an encoder 170 or 250 for generating the pseudo-noise (PN) code is incorporated in the input unit 100 and the body 200 of the electronic locking apparatus according to the present invention. The conditions of the encoder applied to the present invention must include non-repeated and irregular

properties. This becomes a primary factor making a security of the electronic locking apparatus according to the present invention more excellent. As previously mentioned, the present invention employs a chaos theory-based communication technology. As an example, a fractal function applied to the present invention can be defined by [Expression 1] as follows:

[Expression 1]

$y_1=f(x_1)$;

$y_2=f(y_1)$;

$y_3=f(y_2)$;

$y_4=f(y_3)$;

. . . . .

$y_n=f(y_{n-1})$,

where f denotes a fractal function, x_1 denotes an initial value, and y_n denotes a pseudo-noise (PN) code value.

The fractal function represented in the [Expression 1] can be re-written by a function such as the following [Expression 2].

[Expression 2]

$y_1=Cx(x-1)$;

$y_2=Cy_1(y_1-1)$;

$y_3=Cy_2(y_2-1)$;

$y_4=Cy_3(y_3-1)$;

. . . . .

$y_n=Cy_n(y_{n-1}-1)$,

where C denotes a fractal function, x denotes an initial value, and y_n denotes a pseudo-noise (PN) code value. 2

The fractal function like [Expression 1] and [Expression 2] makes the pseudo-noise (PN) code value (y_n) to be an optional irregular variable.

Also, in a chaos encryption communication, the encoder and the decoder of both the input unit and the body must store a fractal function (f), an initial value (x) and a pseudo-noise (PN) code value (y_n) of n-th communication each time a communication is performed between the input unit 100 and the body 200. Accordingly, as can be seen from the following [Table 2], a first communication performs a generation of a cipher code, i.e., an encoding operation (encryption) and a decoding operation (decryption) using y_1, a second communication performs an encoding operation (encryption) and a decoding operation (decryption) using y_2, and a n-th communication performs an encoding operation (encryption) and a decoding operation (decryption) using y_n.

[Table 2]

Number of times of communications	PN generator of input unit	PN generator of body
1	$Y_1=f(x_1)$	$y_1=f(x_1)$
2	$Y_2=f(y_1)$	$y_2=f(y_1)$
3	$Y_3=f(y_2)$	$y_3=f(y_2)$
4	$Y_4=f(y_3)$	$y_4=f(y_3)$
. . . .	. . . .	. . . .
n	$y_n=f(y_{n-1})$	$y_n=f(y_{n-1})$

That is, the input unit 100 and the body 200 include a pseudo-noise (PN) code generator to always generate an identical pseudo-noise (PN) code conforming to a corresponding communication to synchronize the generated pseudo-noise (PN) code so that the input unit 100 and the body 200 identify an encryption signal together therewith.

Accordingly, as shown in Figs. 6 and 7, an encrypted signal according to a preferred embodiment of the present invention is generated by modulating a command signal to be transmitted by using a pseudo-noise (PN) code which is a chaos signal determined by the fractal function and is transmitted to a receiving end. At this time, the receiving end receives the modulated encrypted (chaos) signal and then demodulates

the received encrypted signal to decode it so that the command signal is decrypted.

In the meantime, in the event it is desired to register/modify a password, the input unit 100 must transmit password information to the body 200. For this reason, an encrypted signal generated in a password-registering/modifying mode is constructed unlike that generated in a door-opening mode as shown in Figs. 6 and 7. That is, in the password-registering/modifying mode, a user mixes password information (a numeral code) inputted by himself/herself with an optional pseudo-noise (PN) code while generating the encrypted (chaos) signal as mentioned above with reference to Figs. 6 and 7 for transmission to the body 200. This will be described hereinafter with reference to Figs. 8 and 9.

Fig. 8 is a schematic block diagram illustrating a transmitting operation for implementing an encryption when modifying a password in an electronic locking apparatus according to another preferred embodiment of the present invention, and Fig. 9 is a schematic block diagram illustrating a receiving operation for implementing an encryption when modifying a password in an electronic locking apparatus according to another preferred embodiment of the present invention.

As shown in Figs. 8 and 9, in the event of a modification of a password when transmitting/receiving data

between the input unit 100 and the body 200, the input unit 100 may transmit a numeral code consisting of a set of numerals or password information inputted by the user at a time to the body 200, but may convert the set of numerals of the numeral code into an encrypted signal one by one or by bundling them together by about two numerals at a time for security purposes for transmission to the body 200. This is a kind of method for preventing a password from being exposed to the outside. As shown in Figs. 8 and 9, in the event of transmitting a command signal along with a numeral code, when a transmitting end or one of the input unit 100 and the body 200 multiplies a numeral code E01 by an optional pseudo-noise (PN) code E02 and a carrier (wave) signal E04 to generate an encrypted or encoded signal with a noise for transmission to a receiving end or the other of the input unit 100 and the body 200, the receiving end rejects the carrier signal F03 and the pseudo-noise (PN) code F05 from the encrypted signal F01 with a noise received by the receiving end to extract a pure command signal D06 so that a user can know desired command contents.

Of course, also in the event of a modification of a password as shown in Figs. 8 and 9, a numeral code is modulated into an encrypted chaos signal for transmission.

Fig. 10 is a perspective view illustrating a wall incorporating a wall safe equipped with an electronic locking

apparatus including an input unit and a body according to one preferred embodiment of the present invention, in which the input unit as a wireless remote control unit controls the body remotely to lock and unlock a safe door.

Referring to Fig. 10, when a body of the wall safe is mounted to the wall 10, a keypad through which to input a password to unlock or open a safe door, a knob or any indication for suggesting a safe is not attached on the outside of the safe. The aim of this is to make it difficult to distinguish the safe from the wall when viewed from the outside to obtain a dual security effect. That is, the electronic locking apparatus as shown in Fig. 10 is composed of a body 200 mounted on the inside of a wall safe embedded into a wall 10 in a house or an office and an input unit 100 used as a wireless remote control unit for remotely controlling the body 200 through a radio communication scheme such as an infrared communication scheme, a radio frequency (RF) communication scheme and a Bluetooth communication scheme. As a result, where a user (or a safe manager) always carries the wireless remote control unit, it becomes difficult for an intruder to readily find the safe embedded into the wall 10. Further, although the intruder locates the safe, since a key inserting section, a key button input section or a knob has not been attached on the outside of the body 200 of the safe, it is difficult for him/her to forcibly unlock the

safe door.

Fig. 11 is a perspective view illustrating a safe equipped with an electronic locking apparatus according to one preferred embodiment of the present invention.

Referring to Fig. 11, as shown in Fig. 8, the electronic locking apparatus includes a body 200 mounted on the inside of the safe and an input unit 100 used as a portable wireless remote control unit for remotely controlling the body 200 through a radio communication scheme such as an infrared communication scheme, a radio frequency (RF) communication scheme and a Bluetooth communication scheme.

Fig. 12 is a plan view illustrating the outside of an input unit 100 as a wireless remote control unit of an electronic locking apparatus according to one preferred embodiment of the present invention.

The input unit 100 is an example of the wireless remote control unit implemented with a remote controller employing an infrared ray which is widely used in our daily life. The main difference between the wireless remote control unit 100 and a remote controller used at home is that the wireless remote control unit 100 can communicate bi-directionally with the body 200 of the safe as shown in Figs. 10 and 11. Since the detailed explanation on this has been given previously, it will be omitted hereinafter.

The wireless remote control unit 100 includes an

infrared ray-emitting section 180 or a transmitting section, an LED display section 130 and a key input section 120 consisting of 3*4 keys and a number of functional keys. Although not shown in Fig. 12, in addition to the LED display section 130, an LCD display screen may be provided so that a user can identify the operation state.

Fig. 13 is a perspective view illustrating a safe equipped with an electronic locking apparatus including an input unit 100 implemented with a key input unit mounted on a safe door in an opened position and a body 200 according to another preferred embodiment of the present invention, in which the input unit 100 as a wired control unit controls the body 200 through a communication line to lock and unlock the safe door.

Referring to Fig. 13, the key input unit 100 attached on the outside of a safe door and the body 200 mounted on the inside of the safe 300 are connected with each other through a cable or a communication line 301. The main difference between the electronic locking apparatus as shown in Fig. 13 and the conventional button-type locking device as previously mentioned is that a bi-directional communication and an encrypted chaos signal as shown in Figs. 4 to 7 are used to perform a communication between the key input unit 100 and the body 200 of the electronic locking apparatus, so that it has a more excellent advantage in terms of a communication security.

Meanwhile, the electronic locking apparatus will be effective in applying to both safes taken as an example in the above description and doors. For example, an input unit is provided to only a specified person and a separate door-locking device such as a knob is not mounted to a door, which makes it difficult for an intruder to unlock or open the door.

Fig. 14 is a block diagram illustrating the construction of an electronic locking apparatus which is implemented with a bi-directional wireless encryption communication scheme according to one preferred embodiment of the present invention, and Fig. 15 is a block diagram illustrating the construction of an electronic locking apparatus which is implemented with a bi-directional wired encryption communication scheme according to another preferred embodiment of the present invention.

Referring to Figs. 14 and 15, the bi-directional encryption communication schemes has been described previously, and the input unit 100 is implemented with a portable remote control unit (see Fig. 12) separated from the body 200 of the electronic locking apparatus or is implemented with an key input unit 100 connected, through a communication line or a cable, with the body 200 mounted on the inside of the safe so as to perform a bi-directional encryption communication between the input unit 100 and the body 200.

An encryption locking method according to a preferred

embodiment of the present invention as shown in Figs. 3 to 15 will be described hereinafter Figs. 16 to 18.

Fig. 16 is a flowchart illustrating a process routine of the input unit side for unlocking or opening a door in a start mode when a user inputs a password through an input unit 100 of an electronic locking apparatus according to one preferred embodiment of the present invention.

First, a program of the process routine starts in a start mode 400 and proceeds to step 401 in which the control section 110 of the input unit 100 determines whether or not a password input start key (for example, "S"(START) key button) is depressed through the key input section 120 of the input unit so that a corresponding key signal is inputted into the input unit 100. If it is determined at step 401 that there is a key input of "S" which serves as the password input start key, the program proceeds to step 403 where the control section 110 determines if there is an input of a numeral key corresponding to a password. If it is determined at step 403 that the input of the numeral key exists, the program proceeds to step 406. If, on the other hand, is determined at step 401 that there is no key input of "S" which serves as the password input start key, the program proceeds to step 402 where the control section 110 maintains a wait mode. At step 403, if it is determined that the key input of the numeral key does not exist, the program proceeds to step 404 where the control

section 110 controls a driving of a built-in counter 111 and determines whether or not a numeral key inputting time exceeds a predetermined time. If it is determined at step 404 that the numeral key inputting time exceeds the predetermined time, the program proceeds to step 405 where the control section 110 performs a reset mode for resetting an input of the password, and then returns to step 410 where the control section 110 performs the step 401 repeatedly. On the other hand, if is determined at step 404 that the numeral key inputting time does not exceed the predetermined time, the program returns to step 403 where the control section 110 waits for an input of the numeral key.

At step 403, if it determined that an input of the numeral key, the program proceeds to step 406 where the control section 110 determines whether or not a clear key for clearing the inputted numeral key is depressed. If it is determined at step 408 that the clear key is depressed by a user, the program proceeds to step 407 where the control section 110 resets the inputted numeral and returns to step 403 again.

On the other hand, if it is determined at step 406 that the clear key is not depressed, the control section 110 temporarily stores the corresponding inputted numeral in a corresponding storing area of the memory 140, and then the program proceeds to step 408. At step 408, the control

section 110 determines whether or not a password input end key for completing an input of the password is depressed. If it is determined at step 408 that there is an input of the password input end key, the program proceeds to step 411 where the control section 110 stores the inputted password in the corresponding storing area of the memory 140, and then proceeds to step 412 where the control section 110 carries out a door-opening mode. If, on the other hand, it is determined at step 408 that there is no input of the password input end key, the program proceeds to step 409 where the control section 110 determines whether or not the numeral key inputting time exceeds the predetermined time. If it is determined at step 409 that the numeral key inputting time exceeds the predetermined time, the program proceeds to step 410 where the control section 110 performs a reset mode for resetting an input of the password, and then returns to step 401 where the control section 110 performs the step 401 repeatedly. On the other hand, if it is determined at step 409 that the numeral key inputting time does not exceed the predetermined time, the program returns to step 403 where the control section 110 waits for an input of a numeral key corresponding to the next numeral in the password. The input of a password to the input unit 100 by the user is completed through the above process routine. At this time, the password may be configured with numbers of six to eight digits. The

routine of step 403 to step 410 is performed repeatedly until an input of numbers to the first digit through the last digit of the password is completed. Consequently, when an input of the password is completed and the password input end key is depressed through the key input section at step 408, the program proceeds to step 411 where the control section 110 stores the inputted password in the corresponding storing area of the memory 140, and then proceeds to step 412 where the control section 110 performs the door-opening mode. The above-mentioned flowchart as shown in Fig. 16 is a process in which a user inputs a password for unlocking or opening a door through the input unit 100. That is, this is an authentication process of the password from the user. When the user accomplishes a password-inputting process as shown in Fig. 16 through the input unit 100, the input unit 100 carries out an encryption communication with the body 200 to effect an opening of a door, which will be described hereinafter with reference to Figs. 17a and 17b.

Figs. 17a and 17b are flowcharts illustrating process routines of the input unit side for performing an encryption communication between an input unit and a body of an electronic locking apparatus to unlock or open a door after identifying the user's input of the password according to one preferred embodiment of the present invention.

Once the start mode is completed and a user's password

is inputted to the input unit 100, the program starts in a door-opening mode 500 and proceeds to step 501 in which the control section 110 of the input unit 100 reads out the password inputted by the user and a preset password from the memory 140 and then, determines whether or not they are identical with each other. If it is determined at step 501 that the two passwords are not identical with each other, the program proceeds to step 502 where the control section 110 allows the display section 130 to display a flickering indicative of error, and then proceeds to step 503 where the control section 110 allows the program to return to the start mode. The error indication flickering is performed using an LED indicator of a remote control unit as shown in Fig. 12. But, in the case of using an LCD device, an error for a mismatch between the two passwords may be displayed in the form of a message or an icon. In addition to this, a user may be informed of the mismatch error through a voice message.

If it is determined at step 501 that the two passwords are identical with each other, the program proceeds to step 504 where the control section 110 reads out a first command for requesting an opening of a door as shown in the above [Table 1] from the memory 140 and allows the encoder 170 to generate a first pseudo-noise (PN) code y_1 by substituting an initial value x_1 into the fractal function as shown in the above [Expression 1]. At subsequent step 505, the control

section 110 allows the encoder 170 to combine the first door-opening command signal with the first pseudo-noise (PN) code to generate an encrypted door-opening signal and to transmit the generated encrypted signal to the body 200 through the transmitting section 180. At this time, the encrypted door-opening signal becomes a noise-type signal (encrypted signal or chaos signal) into which [first command signal * first pseudo-noise (PN) code * carrier signal] as shown in Fig. 6 is combined. Like this, when the encrypted signal for requesting an opening of a door is transmitted from the input unit 100 to the body 200, the body 200 receives it through the receiving section 220 for application to the decoder 230 which, in turn, decodes it in such a fashion that the first command signal is extracted by rejecting the first pseudo-noise (PN) code from the encrypted door-opening signal. Then, when the control section 210 of the body 200 identifies a reception of the door-opening signal, it reads out a second command signal indicating an identification of an opening of a door from the memory 290, and then allows the encoder 250 to generate an encrypted door opening-identifying signal and to transmit it to the input unit 100 through the transmitting section 240. At subsequent step 506, the control section 110 determines whether or not the door opening-identifying signal is received by the input unit 100 through a reception of the receiving section 195, and then, a decoding process of the decoder 190.

If it is determined at step 506 that the input unit 100 receives the door opening-identifying signal, the program proceeds to step 512. On the other hand, if it is determined at step 506 that the input unit 100 does not receive the door opening-identifying signal, the program proceeds to step 507 where the control section 110 drives the built-in counter 111 and determines whether or not a predetermined time elapses. If it is determined at step 507 that the predetermined time does not elapse, the program returns to step 506 where the control section 110 performs the step 506 repeatedly. On the other hand, if it is determined at step 507 that the predetermined time elapses, the program proceeds to step 508 where the control section 110 determines whether or not the number of times of transmitting the encrypted door-opening signal is within a predetermined number of times of re-transmission. If it is determined at step 508 that the number of times of transmitting the encrypted door-opening signal is within the predetermined number of times of re-transmission, the program returns to at step 504 where the control section 110 performs the subsequent steps repeatedly. If, on the other hand, it is determined at step 508 that the number of times of transmitting the encrypted door-opening signal exceeds the predetermined number of times of re-transmission, the program proceeds to step 509 where the control section 110 initializes a pseudo-noise (PN) code, and then proceeds to

step 510 where the control section 110 allow the display section 130 to display a flickering indicative of an error. Then, the program proceeds to next step 511 where the control section 110 returns to the start mode. On the other hand, if it is determined at step 506 that the command information which has been received by the input unit 100 and has been decoded by the decoder 190 is the door opening-identifying signal, the program proceeds to step 512 where the control section 110 allow the encoder 170 to generate a new pseudo-noise (PN) code or a second pseudo-noise (PN) code y_2 by substituting the first new pseudo-noise (PN) code value y_1 for a dependent variable of the fractal function as shown in the above [Expression 1] and [Expression 2].

Subsequently, at step 513, it is determined whether or not a pseudo-noise (PN) code extracted from the encrypted signal received from the body 200 is identical with the second pseudo-noise (PN) code generated by the encoder 170. If the answer at step 513 is NO, the program proceeds to step 514 where the control section 110 determines whether or not the number of times of transmitting the encrypted door-opening signal is within a predetermined number of times of re-transmission. If it is determined at step 514 that the number of times of transmitting the encrypted door-opening signal is within the predetermined number of times of re-transmission, the program returns to step 504 where the control section 110

performs the subsequent steps 504 through 513 repeatedly. If, on the other hand, it is determined at step 514 that the number of times of transmitting the encrypted door-opening signal exceeds the predetermined number of times of re-transmission, the program proceeds to step 515 where the control section 110 initializes a pseudo-noise (PN) code, and then proceeds to step 516 where the control section 110 allow the display section 130 to display a flickering indicative of an error. Then, the program proceeds to next step 517 where the control section 110 returns to the start mode.

On the other hand, if it is determined at step 513 that the pseudo-noise (PN) code extracted from the encrypted signal received from the body 200 is identical with the second pseudo-noise (PN) code, the program proceeds to step 518 where the control section 110 determines whether or not the command signal received from the body 200 is the second command signal indicating an identification of an opening of a door. If it is determined at step 518 that the received command signal is not the second (door opening-identifying) command signal, the program proceeds to step 514 where the control section performs the steps 514 through 517. On the other hand, if it determined at step 518 that the received command signal is the second command signal, the program proceeds to step 519 where the control section 110 reads out a third command indicating execution of an opening of a door as shown in the above [Table

1] from the memory 140 and allow the encoder 170 to generate a new pseudo-noise (PN) code or a third pseudo-noise (PN) code y_3 by substituting the second new pseudo-noise (PN) code value y_2 for a dependent variable of the fractal function as shown in the above [Expression 1] and [Expression 2]. Subsequently, at step 521, the control section 110 allows the encoder 170 to combine the third door opening-executing command signal with the third pseudo-noise (PN) code to generate an encrypted door opening-executing signal and to transmit the generated encrypted signal to the body 200 through the transmitting section 180. At this time, the encrypted door opening-executing signal becomes a noise-type signal (encrypted signal or chaos signal) into which [third command signal * third pseudo-noise (PN) code * carrier signal] as shown in Fig. 6 is combined. Like this, when the encrypted signal for requesting an execution of a door-opening is transmitted from the input unit 100 to the body 200, the body 200 receives it through the receiving section 220 for application to the decoder 230 which, in turn, decodes it in such a fashion that the third command signal is extracted by rejecting the third pseudo-noise (PN) code from the encrypted door opening-executing signal. Then, when the control section 210 of the body 200 identifies a reception of the door opening-executing signal, it reads out a fourth command signal indicating an identification of an execution of an opening of a door from

the memory 290, and then allows the encoder 250 to generate an encrypted door opening-executing-identifying signal and to transmit it to the input unit 100 through the transmitting section 240. At subsequent step 521, the control section 110 determines whether or not the door opening-executing-identifying signal is received by the input unit 100 through a reception of the receiving section 195, and then, a decoding process of the decoder 190. If it is determined at step 521 that the input unit 100 receives the door opening- executing-identifying signal, the program proceeds to step 527. On the other hand, if it is determined at step 521 that the input unit 100 does not receive the door opening-executing-identifying signal, the program proceeds to step 522 where the control section 110 drives the built-in counter 111 and determines whether or not a predetermined time elapses. If it is determined at step 522 that the predetermined time does not elapse, the program returns to step 521 where the control section 110 performs the step 521 repeatedly. On the other hand, if it is determined at step 521 that the predetermined time elapses, the program proceeds to step 523 where the control section 110 determines whether or not the number of times of transmitting the encrypted door opening-executing signal is within a predetermined number of times of re-transmission. If it is determined at step 523 that the number of times of transmitting the encrypted door opening-executing

signal is within the predetermined number of times of re-transmission, the program returns to at step 519 where the control section 110 performs the subsequent steps 519 through 521 repeatedly. If, on the other hand, it is determined at step 523 that the number of times of transmitting the encrypted door opening-executing-signal exceeds the predetermined number of times of re-transmission, the program proceeds to step 524 where the control section 110 initializes a pseudo-noise (PN) code, and then proceeds to step 525 where the control section 110 allow the display section 130 to display a flickering indicative of an error. Then, the program proceeds to next step 526 where the control section 110 returns to the start mode.

On the other hand, if it is determined at step 521 that the command information which has been received by the input unit 100 and has been decoded by the decoder 190 is the door opening—executing-identifying signal, the program proceeds to step 527 where the control section 110 allow the encoder 170 to generate a new pseudo-noise (PN) code or a fourth pseudo-noise (PN) code y_4 by substituting the third new pseudo-noise (PN) code value y_3 for a dependent variable of the fractal function as shown in the above [Expression 1] and [Expression 2]. Subsequently, at step 528, it is determined whether or not a pseudo-noise (PN) code extracted from the encrypted signal received from the body 200 is identical with the fourth

pseudo-noise (PN) code generated by the encoder 170. If the answer at step 513 is NO, the program proceeds to step 514 where the control section 110 determines whether or not the number of times of transmitting the encrypted door opening-executing signal is within a predetermined number of times of re-transmission. If it is determined at step 529 that the number of times of transmitting the encrypted door opening-executing signal is within the predetermined number of times of re-transmission, the program returns to step 519 where the control section 110 performs the subsequent steps 519 through 528 repeatedly. If, on the other hand, it is determined at step 529 that the number of times of transmitting the encrypted door opening-executing signal exceeds the predetermined number of times of re-transmission, the program proceeds to step 530 where the control section 110 initializes a pseudo-noise (PN) code, and then proceeds to step 531 where the control section 110 allow the display section 130 to display a flickering indicative of an error. Then, the program proceeds to next step 532 where the control section 110 returns to the start mode.

On the other hand, if it is determined at step 528 that the pseudo-noise (PN) code extracted from the encrypted signal received from the body 200 is identical with the fourth pseudo-noise (PN) code, the program proceeds to step 533 where the control section 110 determines whether or not the command

signal received from the body 200 is the fourth command signal indicating an identification of an execution of a door opening. If it is determined at step 533 that the received command signal is not the fourth command signal, the program returns to step 529 where the control section 110 performs the subsequent steps 529 through 532 repeatedly. On the other hand, if it is determined at step 533 that the received command signal is the fourth command signal, the program proceeds to step 534 where the control section 110 allows the display section 130 to display a flickering of a door-opening LED indicating that the door has been opened for a user, and then proceeds to step 535 where the control section 110 concludes the door-opening mode according to the present invention.

Fig. 18 is a flowchart illustrating a process routine of the input unit 100 for performing an encryption communication between an input unit and a body of an electronic locking apparatus to modify a password according to another preferred embodiment of the present invention. Here, the password-modifying mode represents a process in which when it is necessary that a user should modify his/her password being used, the input unit 100 transmits new password information to the body 200 which, in turn, stores it therein through a bi-directional encryption communication between the input unit 100 and the body 200.

First, at step 601, the control section 110 of the input unit 100 determines whether or not a user selects a modification of a password. At this time, a method in which the user selects the modification of the password through the key input section 120 of the input unit 100 is to use a separate mode-setting key or to depress ["S" key + "E" key] for the input unit as shown in Fig. 10. If it is determined at step 601 that the modification of the password is not selected, the program proceeds to step 602 in which the control section 110 performs a corresponding function. On the other hand, if it is determined at step 601 that the modification of the password is selected, the program proceeds to step 603. Like this, when the modification of the password is selected, the control section 110 may allow the display section 130 to, for a few seconds, display a flickering of LED indicating to the user that the modification of the password has been selected. At step 603, the control section 110 allows the user to input an existing password through the key input section 120. Subsequently, at step 604 the control section determines whether or not the existing password inputted by the user is identical with a preset password stored in the memory 140. If it is determined at step 604 that there is no accord between the inputted password and the preset password, the program proceeds to step 605 where the control section 110 determines whether or not the number of

times of inputting the existing password is within a predetermined number of times of re-inputting password. If it is determined at step 605 that whether or not the number of times of inputting the existing password is within the predetermined number of times of re-inputting password, the program returns to step 603 where the control section 110 performs the subsequent steps 603 and 604. On the other hand, if it is determined at step 605 that whether or not the number of times of inputting the existing password exceeds the predetermined number of times of re-inputting password, the program proceeds to step 606 where the control section 110 allows the display section 130 to display a flickering of an error indication, and proceeds to step 607 where the control section 110 returns to the start mode.

On the other hand, if it is determined at step 604 that there is an accord between the inputted password and the preset password, the program proceeds to step 608 where the control section 110 allows the user to input a new password and stores the inputted new password in a password-storing area of the memory 140. At subsequent step 609, like in a password modifying process as shown in [Table 1], the new password inputted by the user is encrypted or encoded by an encryption method as shown in Fig. 8 to generate an encrypted password signal which is transmitted to the body 200. At this time, the encrypted password signal becomes a noise signal

(chaos signal) into which [first digit of password * second digit of password * pseudo-noise (PN) code * carrier signal] as shown in Fig. 8 is combined in such a fashion that digits of the newly inputted password is encrypted or encoded two by two. At step 609, first, the control section 110 allows the transmitter 180 of the input unit 100 to transmit a signal indicating a modification of a password to the body 200. Then, the program proceeds to step 610 where the control section 110 determines whether or not a password modification-identifying signal is received by the input unit 100 from the body 200 through a reception of the receiving section 195, and then, a decoding process of the decoder 190. If it is determined at step 610 that the password modification-identifying signal is not received by the input unit 100 from the body 200, the program proceeds to step 611 where the control section 110 determines whether or not the number of times of transmitting the encrypted password-modifying signal is within a predetermined number of times of re-transmission. If it is determined at step 611 that the number of times of transmitting the encrypted password-modifying signal is within the predetermined number of times of re-transmission, the program returns to at step 609 where the control section 110 performs the subsequent steps 609 and 610 repeatedly. If, on the other hand, it is determined at step 611 that the number of times of transmitting the encrypted password-modifying

signal exceeds the predetermined number of times of re-transmission, the program proceeds to step 612 where the control section 110 initializes a pseudo-noise (PN) code, and then proceeds to step 613 where the control section 110 allow the display section 130 to display a flickering indicative of an error. Then, the program proceeds to next step 614 where the control section 110 returns to the start mode.

In the meantime, at step 610, if it is determined that the password modification-identifying signal is received by the input unit 100 from the body 200, the program proceeds to step 615 where the control section 110 performs an encryption-identifying procedure for an existing password between the input unit 100 and the body 200 through a series of processes corresponding to the command numbers 13 to 20 in a password-modifying mode in the above [Table 1]. In this case, for the initial signal indicating a modification of a password, i.e., the initial password-modifying signal and a signal identifying the initial signal, i.e., the password modification-identifying signal (respectively, the command numbers 11 and 12), the control section 110 of the input unit 100 allows the encoder 170 to generate an encrypted signal incorporating a command signal without a numeral code which is transmitted to the body 200 as shown in Fig. 6, and the control section 210 of the body 200 allows the decoder 230 to extract the pure command signal indicating the modification of the password

from the encrypted signal received by the body 200 from the input unit 100. Then, each of the command numbers 13 to 20 in the above [Table 1] does not incorporate the command signal involved in the transmitted/received encryption signal, but incorporates an encrypted signal having a numeral code for identifying the existing password like in the encrypted transmission/reception procedures as shown in Figs. 8 and 9. At this time, digits of the encrypted signal having the numeral code is transmitted/received, two by two, between the input unit 100 and the body 200.

Subsequently, at step 616, when the encryption-identifying procedure for the existing password is completed, the control section 110 performs the encryption-identifying procedure (a series of process corresponding to command numbers 21 to 27 in the above [Table 1]) for new password information to be modified, and then encrypts or encodes the new password information stored in the memory 140 of the input unit 100 according to the encrypted transmission/reception procedures as shown in Fig. 8 in such a fashion that the numeral codes (i.e., digits) of the new password are encrypted one by one or two by two to generate successive encrypted signals to repeatedly perform the transmission of the encrypted signal. At subsequent step 617, the control section 110 of the input unit 100 determines whether or not a checksum signal identifying a completion of reception of the new

password is received in an encrypted form from the body 200. If it is determined at step 617 that although all the digits (the first digit through the last digit) of the new password have been transmitted, in an encrypted form, to the body 200, the checksum signal is not received during a predetermined period of time, the program proceeds to step 618 where the control section 110 allows the display section 130 to display a flickering of an error indication, and then proceeds to step 619 where the control section 110 returns to the start mode. On the other hand, if it is determined at step 617 that a command signal indicating the checksum signal is received through a decoding of the encrypted checksum signal, the program proceeds to step 620 where the control section 110 allows the encoder 170 to generate an encrypted signal requesting a storing of the new password for transmission to the body 200. Subsequently, at step 621, the control section 110 determines whether or not a storage-completing signal identifying a completion of storage of the new password is received from the body 200 so that a corresponding command signal is identified, the program proceeds to step 622 where the control section 110 concludes the present password-modifying mode.

In the meantime, in Fig. 18, the new password inputting/storing process has been performed at step 608, but may be performed after step 615 in which the encryption-

identifying procedure for the existing password is completed. That is, a user may input the new password after a completion of the encryption-identifying procedure for the existing password, or may previously input the new password to replace the existing password before a completion of the encryption-identifying procedure.

Further, although the present invention has been shown and described so that the door-opening mode and the password-modifying mode are performed in two different modes in Figs. 16 to 18, it may be implemented so that a user performs either the door-opening mode or the password-modifying modes selectively after all the door-opening and password-modifying modes start in a start mode.

As can be seen from the embodiments previously described, an electronic locking apparatus according to present invention may be implemented so that an input unit and a body are constructed to be driven under the control of each separate control section in the places requiring installation of an locking device, and then a communication between the input unit and the body is effected more safely and effectively using an encrypted signal modified always without directly transmitting a password in a password-authenticating process for releasing the locking apparatus through an encoder and a decoder.

Moreover, although having not been described in the

foregoing, a master key mode as shown in [Table 1] may be carried out. Herein, "the master key" refers to a mode which a manufacturer of a locking device or only an authorized one person can manage as well as a mode which can open or unlock a door with an aid of a specific password assigned at the time of manufacturing the locking device without undergoing an authentication of a preset password in the event it is impossible to drive the electronic locking apparatus due to a loss of the input unit or other reasons.

An example of its detailed process is like a procedure of a master key mode shown in the above [Table 1].

Another embodiment of the present invention will be described with reference to Figs. 19 and 22.

Fig. 19 is a schematic block diagram illustrating a transmitting operation for implementing an encryption when unlocking or opening a door in an electronic locking apparatus according to another preferred embodiment of the present invention, and Fig. 20 is a schematic block diagram illustrating a receiving operation for implementing an encryption when unlocking or opening a door in an electronic locking apparatus according to another preferred embodiment of the present invention.

Referring to Fig. 19, a fixed cipher code H02 is one which is inputted to a wireless remote control unit (an input unit) 100 and a wireless remote electronic locking apparatus

(a body) 200 at the time of manufacturing the electronic locking apparatus. In the event of a transmission of an encrypted signal when opening a safe door or registering/modifying a password, a command H01 is mixed with the fixed cipher code H02, an optional authentication cipher code H04 generated by a fractal function (for example, pseudo-noise code) and a carrier signal H06 to generate an encrypted signal H08. At this time, H03, H05 and H07 of Fig. 19 denote each mixed signal. On the contrary, In the event of a reception of the encrypted signal, as shown in Fig. 20, a carrier J02 and an optional authentication signal J04 are rejected from the received-encrypted signal to extract a fixed cipher code J06 and a command J08. At this time, J03, J05 and J07 of Fig. 20 denote each rejected signal.

Fig. 21 is a flowchart illustrating a process routine for unlocking or opening a safe door using an input unit as a wireless remote control unit of an electronic locking apparatus according to another preferred embodiment of the present invention.

First, a user depresses a key input button of the wireless remote input unit 100 such as a remote controller as shown in Fig. 12, for example, in the order of [open]+[password]+[open]. Then, at the input unit side 100, the program proceeds to step 701 where the control section 110 performs a password authentication procedure for determining

whether or not a password inputted by the user is identical with a registered password stored in the input unit 100. If the inputted password is not identical with the registered password in the password authentication procedure, the control section 110 allows the display section 130 to flicker "error" LED three to five times, and then allows the program to return to an initial state, i.e., the start mode. On the other hand, if the inputted password is identical with the registered password in the password authentication procedure 701, the program proceeds to step 703 where the control section 110 of the input unit 100 allows the encoder 170 to convert a door-opening signal into an encrypted signal according to the encrypted transmission procedure of Fig. 19 for transmission to the body 200. Then, at step 705, if it is determined that the body 200 receives the door-opening signal through the decoding of the encrypted signal received from the input unit 100, the program proceeds to step 707 where the control section 210 allows the body 200 to transmit an optional authentication cipher code to be modified to the input unit 100. Then, the input unit 100, at step 709, receives the optional authentication cipher code from the body 200, and at step 711, stores it in the memory 140. After that, at step 713, the input unit 100 transmits a signal indicative of a completion of storage of the optional authentication cipher code to the body 200. If it is determined at step 715 that

the body 200 receives the storage-completing signal from the input unit 100, the program proceeds to step 717 where the control section 110 transfers the door-opening signal to an electronic locking circuit for actuating a solenoid coil. Then, the solenoid coil is actuated so that a gear unit, spring or cam-structured latch is released to open or unlock a safe door. At this time, the body 200, at step 721, transmits a door opening-completing signal indicating an opening of the safe door to the input unit 100. Then, if it is determined at step 723 that the input unit 100 receives the door opening-completing signal from the body 200, the program proceeds to step 725 where the control section 110 allows the display section 130 to flicker "door-opening" LED to inform the user of an opening of the safe door.

A password modifying process according to another embodiment of the present invention will be described with reference to Fig. 22.

Fig. 22 is a flowchart illustrating a process routine for modifying a password using an input unit as a wireless remote control unit of an electronic locking apparatus according to another preferred embodiment of the present invention.

First, at step 801, the control section 110 of the input unit 100 determines whether or not if there is a request for a modification of a password from a user, a password-modifying

mode is selected. If it is determined at step 801 that the password-modifying mode is selected, the program proceeds to step 803 where the control section 130 performs the password authentication procedure. Then, at step 805, the input unit 100 transmits a password modifying-requesting signal to the body 200. At subsequent step 807, if it is determined that the body 200 receives the password modifying-requesting signal form the input unit 100, the program proceeds to step 809 where the control section 210 of the body 200 transmits a signal requesting a transmission of an existing password to the input unit 100. Then, if it is determined at step 811 that there is a request for a transmission of the existing password by the body 200, the program proceeds to step 813 where the control section 110 allows the encoder 170 to convert existing password information into an encrypted signal for transmission to the body 200. If it is determined at step 815 that the body 200 receives the encrypted existing password signal form the input unit 100, the program proceeds to step 817 where the control section 210 allows the decoder to decode the encrypted existing password signal received from the input unit 100, and then determines whether or not the decoded existing password is identical with a password stored in the body 200. If it is determined at step 817 that the decoded existing password is identical with the stored password, the program proceeds to step 819 where the control section 210

allows the body 200 to transmit a password modifying-approving signal to the input unit 100. Then, if it is determined at step 821 the input unit 100 receives the password modifying-approving signal from body 200, the program proceeds to step 823 where the control section 110 allows the display section 130 to turn a "modify" LED on to inform the user of an approval of the password modification. After that, at step 825, the control section 110 allows the user to input a new password into the input unit 100. At step 825, if an input of the new password is completed by the user, the program proceeds to step 827 where the control section 110 allows the display section 130 to turn the "modify" LED on, and then proceeds to step 829 where the control section 110 requests a re-input of the password from the user to identify a correct input of the new password. Then, at step 833, the control section of the input unit 100 determines whether or not the re-inputted new password is identical with the first inputted new password, and then stores the new password in the memory 140 if the re-inputted new password is identical with the first inputted new password. At subsequent step 833, the input unit 100 transmits the new password to the body 200. The body 200 receives the new password from the input unit 100 and stores it in the memory 290. Then, at step 837, the body 200 transmits a signal indicating a completion of storage of the new password to the input unit 100. At this time, at step

839, the input unit 100 receives the new password storage-completing signal from the body 200, and then flickers three LEDs simultaneously to inform the user of a successful completion of a modification of the password.

In the meantime, the electronic locking apparatus according to the present invention has more excellent security ability than a conventional locking device which employs a unidirectional communication scheme providing an unlocking/locking signal from the input 100 to the body 200 without a password-identifying procedure in that it enables a bi-directional communication between the input unit 100 and the body 200 through only a password-identifying procedure between the input unit 100 and the body 200 even without the above described encryption converting process. In the event the input unit and the body according to present invention are implemented with only a bi-directional communication scheme, the encoders 170 and 250 and the decoders 190 and 230 will be omitted from the construction of the input unit 100 and the body 200 in Figs. 3 and 4, and a procedure (for example, a process for generating an optional pseudo-noise code using a fractal function) for generating an encrypted signal upon the transmission/reception of a signal will also be omitted. Also, in this case, a bi-directional communication between the input unit and the body enables an identification of a password through a command signal according to information

about a password itself under the control of the control section included in both the input unit and the body, so that a door can be opened or unlocked for only a password identified.

The application examples of the electronic locking apparatus according to the present invention are shown in Figs. 23 to 25. Fig. 23a is a perspective view illustrating a door equipped with an electronic locking apparatus including an input unit and a body according to another preferred embodiment of the present invention, in which the input unit as a wireless remote control unit controls the body remotely to lock and unlock a safe door, Fig. 23b is a perspective view illustrating a door equipped with an electronic locking apparatus including a key input unit and a body mounted on the door according to another preferred embodiment of the present invention, in which the key input unit as a wired control unit controls the body through a communication line to lock and unlock the door, Fig. 24a is a perspective view illustrating a cabinet equipped with an electronic locking apparatus including an input unit and a body according to another preferred embodiment of the present invention, in which the input unit as a wireless remote control unit controls the body remotely to lock and unlock a cabinet door, Fig. 24b is a perspective view illustrating a cabinet equipped with an electronic locking apparatus including a key input unit and a

body mounted on the cabinet according to another preferred embodiment of the present invention, in which the key input unit as a wired control unit controls the body through a communication line to lock and unlock a cabinet door, Fig. 25a is a perspective view illustrating a filing cabinet equipped with an electronic locking apparatus including an input unit and a body according to another preferred embodiment of the present invention, in which the input unit as a wireless remote control unit controls the body remotely to lock and unlock a cabinet door, and Fig. 25b is a perspective view illustrating a filing cabinet equipped with an electronic locking apparatus including a key input unit and a body mounted on the filing cabinet according to another preferred embodiment of the present invention, in which the key input unit as a wired control unit controls the body through a communication line to lock and unlock a cabinet door.

As can be seen from the foregoing, the present invention has the following various advantages:

The present invention is implemented in such as fashion that the electronic locking apparatus thereof is constructed to be divided into an input unit and a body, and when a user inputs a password through the input unit, the authentication of the password between the input unit and the body is performed by using an encrypted signal from which password information is rejected, thereby basically preventing an

external leakage of password information and implementing a more powerful security system.

Also, the present invention is implemented in such a fashion that the input unit like a keypad of the electronic locking apparatus for performing an encryption communication is removed from the body thereof to remotely control the input unit, so it is difficult to externally recognize a locking section, thereby implementing a dual security effect.

Further, the present invention employs an optional non-repeated authentication cipher code (a pseudo-noise code generated by a fractal function) to enable an encryption communication between the input unit and the body of the electronic locking apparatus, thereby preventing a risk of password leakage.

In addition, the present invention is implemented in such a fashion that the input unit and the body thereof are provided with the control section, respectively, to perform a bi-directional communication therebetween, so that an authentication of a password is effected through an password identification procedure between the input unit and the body, thereby improving a security.

While this invention has been described in connection with what is presently considered to be the most practical and preferred embodiment, it is to be understood that the invention is not limited to the disclosed embodiment, but, on

the contrary, it is intended to cover various modifications, variations or equivalents within the spirit and scope of the appended claims.

WHAT IS CLAIMED IS:

1. An electronic locking apparatus for performing a bi-directional communication, comprising:

an input unit including:

a key input section having a plurality of numeral keys and functional keys, the key input section being adapted to generate a corresponding key signal if there is a key input from a user;

a memory adapted to store predefined command information and password information set by a user, the memory being locked to prevent an optional modification of the stored information;

a control section adapted to control a transmission/reception of a password numeral code signal and a command signal between the input unit and a body of the electronic locking apparatus to enable a bi-directional communication between the input unit and the body thereof, the control section being adapted to perform a locking/unlocking of a door and a registration/modification of a password through an identification of signals transmitted/received between the input unit and the body thereof;

a transmitting section adapted to transmit the password numeral code signal and the command signal to the body thereof under the control of the control section of the input unit;

a receiving section adapted to receive signals from the body thereof and supply the received signal to the control section of the input unit; and

a battery adapted to supply a power source required to drive the input unit to each constituent element thereof; and

a body including:

a control section adapted to control a transmission/reception of the password numeral code signal and the command signal between the input unit and the body of the electronic locking apparatus to enable a bi-directional communication between the input unit and the body thereof, the control section being adapted to perform a locking/unlocking of the door and a registration/modification of the password through an identification of the signals transmitted/received between the input unit and the body thereof;

a transmitting section adapted to transmit a password numeral code signal and a command signal to the input unit under the control of the control section of the body;

a receiving section adapted to receive the signals from the input unit and supply the received signals to the control section of the body;

a power source section adapted to supply a power source required to drive the body to each constituent element thereof;

a memory adapted to store the predefined command

information and the password information set through the input unit, the memory being locked to prevent an optional modification of the stored information; and

a door locking section adapted to lock/unlock a door when receiving a door control command from the control section of the body.

2. The electronic locking apparatus according to claim 1 wherein the electronic locking apparatus is applied to safes, doors, filing cabinets, cabinets and the like, and the input unit is implemented with a wireless remote control unit.

3. The electronic locking apparatus according to claim 1 wherein the electronic locking apparatus is applied to safes, doors, filing cabinets, cabinets and the like, and the input unit is mounted on the door to be connected with the body through a communication line or a cable.

4. The electronic locking apparatus according to claim 2 or 3 wherein the input unit further includes a display section adapted to display the overall states of the input unit according to the performances of a start mode, a door-opening (unlocking) mode and a password-modifying mode to inform the user of it.

5. The electronic locking apparatus according to claim 2 wherein the transmitting and receiving sections of the input unit implemented with the wireless remote control unit and the body are implemented by employing any one of an infrared communication scheme, a radio frequency (RF) communication scheme and a Bluetooth communication scheme.

6. The electronic locking apparatus according to claim 4 wherein the input unit and the body further includes a battery level detecting section and a power source level detecting section for detecting a power source level, respectively, to apply the detected power source level to the control sections of the input unit and the body.

7. The electronic locking apparatus according to claim 6 wherein the input unit further includes an alarm section employing a buzzer or a speech transmitter to give an alarm to the user with a buzzer or a voice in the event of a detection of a low voltage from the battery, or to give an error alarm signal to the user.

8. An electronic locking apparatus for performing a bi-directional encryption communication, comprising:

an input unit including:

a key input section having a plurality of numeral keys

and functional keys, the key input section being adapted to generate a corresponding key signal if there is a key input from a user;

a memory adapted to store predefined command information, password information set by the user and a pseudo-noise (PN) code information, the memory being locked to prevent an optional modification of the stored information;

a control section adapted to control both corresponding constituent elements and the overall operation of the input unit to enable a bi-directional encryption communication between the input unit and the body thereof, the control section being adapted to control the input unit so that a communication for clocking/unlocking a door is performed between the input unit and the body by using an encrypted signal in which a password for locking/unlocking the door is rejected through the authenticating of the password when the user inputs the password through the key input section, and adapted to allow the input unit to perform an encryption communication with the body by encrypting password information of partial digits in all the password information keyed in when the user inputs a new password through the key input section in a password-registering/modifying mode;

an encoder adapted to generate an optional pseudo-noise (PN) code having non-repeated and irregular properties under the control of the control section when a communication is

performed between the input unit and the body, and then both mix a specific command signal to be transmitted to the body with the generated pseudo-noise (PN) code to generate an encrypted signal and mix the partial password information with an optional pseudo-noise (PN) code to generate an encrypted signal;

a transmitting section adapted to transmit the encrypted signals generated from the encoder to the body;

a receiving section adapted to receive an encrypted signal from the body; and

a decoder adapted to decode the encrypted signal applied thereto from the receiving section of the input unit in such a fashion that the decoder rejects a pseudo-noise code from the encrypted signal to extract only pure command information or numeral code information for application to the control section.

a battery adapted to supply a power source required to drive the input unit to each constituent element thereof; and

a body including:

a control section adapted to control both corresponding constituent elements and the overall operation of the body to enable a bi-directional encryption communication between the input unit and the body thereof, the control section being adapted to allow the body to decode the encrypted signal received by the body when receiving it from the input unit and

adapted to control a locking/unlocking of the door and a modification of the password through an identification of the decoded signal together with the input unit;

a receiving section adapted to receive the encrypted signals from the input unit;

a decoder adapted to decode the encrypted signals applied thereto from the receiving section of the body in such a fashion that the decoder rejects the pseudo-noise codes from the encrypted signals to extract only pure command information or numeral code information for application to the control section;

an encoder adapted to adapted to generate an optional pseudo-noise (PN) code having non-repeated and irregular properties under the control of the control section of the body when a communication is performed between the input unit and the body, and then mix a specific command signal or a numeral code with the generated pseudo-noise (PN) code to generate an encrypted signal;

a transmitting section adapted to transmit the encrypted signals generated from the encoder of the body to the input unit;

a power source section adapted to supply a power source required to drive the body to each constituent element thereof, the power source section adapted to be constructed to selectively use a battery voltage and a Direct Current (DC)

source adapter;

a memory adapted to store predefined command information, password information set by the user and a pseudo-noise (PN) code information, the memory being locked to prevent an optional modification of the stored information; and

a door locking section adapted to lock/unlock the door when receiving a door control command from the control section of the body.

9. The electronic locking apparatus according to claim 8 wherein the electronic locking apparatus is applied to safes, doors, filing cabinets, cabinets and the like, and the input unit is implemented with a wireless remote control unit.

10. The electronic locking apparatus according to claim 8 wherein the electronic locking apparatus is applied to safes, doors, filing cabinets, cabinets and the like, and the input unit is mounted on the door to be connected with the body through a communication line or a cable.

11. The electronic locking apparatus according to claim 9 or 10 wherein the input unit further includes a display section adapted to display the overall states of the input unit according to the performances of a start mode, a door

opening (unlocking) mode and a password modifying mode to inform the user of it.

12. The electronic locking apparatus according to claim 9 wherein the transmitting and receiving sections of the input unit implemented with the wireless remote control unit and the body are implemented by employing any one of an infrared communication scheme, a radio frequency (RF) communication scheme and a Bluetooth communication scheme.

13. The electronic locking apparatus according to claim 11 wherein the input unit and the body further includes a battery level detecting section and a power source level detecting section for detecting a power source level, respectively, to apply the detected power source level to the control sections of the input unit and the body.

14. The electronic locking apparatus according to claim 13 wherein the input unit further includes an alarm section employing a buzzer or a speech transmitter to give an alarm to the user with a buzzer or a voice in the event of a detection of a low voltage from the battery, or to give an error alarm signal to the user.

15. A method of controlling an encryption communication

in an electronic locking apparatus including an input unit with a key input section and a body with a door-locking section for opening/closing a door, the input unit and the body each having a control section, an encoder and a decoder, and being adapted to perform a bi-directional encryption communication therebetween, comprising the steps of:

a user password-authenticating step, when the user inputs a password used to open/close the door through the key input section of the input unit, for determining whether or not a user's registered password information stored in the input unit is identical with the password inputted by the user;

an encryption communication step, when the user's registered password information is identical with the password inputted by the user, for allowing the input unit to generate an optional pseudo-noise (PN) code having non-repeated and irregular properties and mix a command signal specified for an opening/closing of the door with the optional pseudo-noise (PN) code to generate an encrypted signal through the encoder thereof to transmit it to the body, and allowing the body to receive the encrypted signal from the input unit and reject the pseudo-noise (PN) code from the received encrypted signal to extract only pure command information, so that after identifying the rejected pseudo-noise (PN) code and the extracted command information, a command signal indicating an

identification of the extracted command information is read out and is mixed with an optional pseudo-noise (PN) code to generate an encrypted signal to transmit it the input unit; and

a door-opening/closing step for allowing the body to search a function specified for the extracted command information to open/close the door.

16. The encryption communication controlling method according to claim 15 wherein the encrypted signal employs a pseudo-noise (PN) code generated according to the encryption communication step based on a fractal function in the following [Expression 3] applied to a chaos theory,

[Expression 3]

$y_1=f(x_1)$;

$y_2=f(y_1)$;

$y_3=f(y_2)$;

$y_4=f(y_3)$;

. . . . .

$y_n=f(y_{n-1})$,

where f denotes a fractal function, x_1 denotes an initial value, and y_n denotes a pseudo-noise (PN) code value.

17. The encryption communication controlling method according to claim 16 further comprising the step of:

when a normal opening/closing of the door is completed by the body, allowing the input unit to perform a display function for indicating that the normal opening/closing of the door has been completed.

18. The encryption communication controlling method according to claim 17 further comprising the step of:

a password-registering/modifying step, when the encryption communication is performed for a registration/modification of the password, for allowing the input unit to mix a new password inputted by the user with an optional pseudo-noise (PN) code in such a fashion that numeral codes of the new password is bundled by an optional number upon the mixing of the new password with the optional pseudo-noise (PN) code to generate an encrypted signal which is transmitted to the body, and then allowing the input unit to replace an existing password preset in the body by the new password for registration/modification thereof when all the numeral codes including the first numeral code through the last numeral code of the new password have been transmitted to the body through an encryption communication between the input unit and the body.

19. The encryption communication controlling method according to claim 18 further comprising the step of:

an error displaying step for allowing the input unit to display a generation of an error when an abnormal encrypted signal is received in the encryption communication step or the body does not perform the opening/closing of the door normally.

20. The encryption communication controlling method according to claim 19 wherein the command information is previously stored in the input unit and the body in a specific form by each encryption communication step.

21. The encryption communication controlling method according to claim 20 wherein the electronic locking apparatus for controlling the encryption communication is applied to safes, doors, filing cabinets, cabinets and the like.

22. A method of controlling a bi-directional communication in an electronic locking apparatus including an input unit with a key input section and a body with a door-locking section for opening/closing a door, the input unit and the body each having a control section and being adapted to perform a bi-directional communication therebetween, comprising the steps of:

a user password-authenticating step, when the user inputs a password used to open/close the door through the key

input section of the input unit, for determining whether or not a user's registered password information stored in the input unit is identical with the password inputted by the user;

an encryption communication step, when the user's registered password information is identical with the password inputted by the user, for allowing the input unit to transmit a door-opening command to the body while allowing the body to receive the door-opening command from the input unit and transmit a door opening-identifying signal to the input unit, and then allowing the input unit to receive the door opening-identifying signal from the body and transmit a door opening-executing signal to the body; and

a door-opening/closing step for allowing the body to open/close the door when the body receives the door opening-executing signal from the input unit.

23. The bi-directional communication controlling method according to claim 22 further comprising the step of:

when a normal opening/closing of the door is completed by the body, allowing the body to transmit a door opening-displaying command to the input unit while allowing the input unit to perform a display function for indicating that the normal opening/closing of the door has been completed.

24. The bi-directional communication controlling method according to claim 23 further comprising the step of:

a password-registering/modifying step, when the bi-directional communication is performed for a registration/modification of the password, for allowing the input unit to transmit a new password inputted by the user to the body in such a fashion that numeral codes of the new password is bundled by an optional number upon the transmission of the new password to the body, and then allowing the input unit to replace an existing password preset in the body by the new password for registration/modification thereof when all the numeral codes including the first numeral code through the last numeral code of the new password have been transmitted to the body through a password identifying procedure between the input unit and the body.

25. The bi-directional communication controlling method according to claim 24 further comprising the step of:

an error displaying step for allowing the input unit to display a generation of an error when an abnormal encrypted signal is received in the bi-directional communication step or the body does not perform the opening/closing of the door normally.

26. The bi-directional communication controlling method

according to claim 25 wherein the command information is previously stored in the input unit and the body in a specific form by each bi-directional communication step.

27. The bi-directional communication controlling method according to claim 26 wherein the electronic locking apparatus for controlling the bi-directional communication is applied to safes, doors, filing cabinets, cabinets and the like.

FIG. 1a

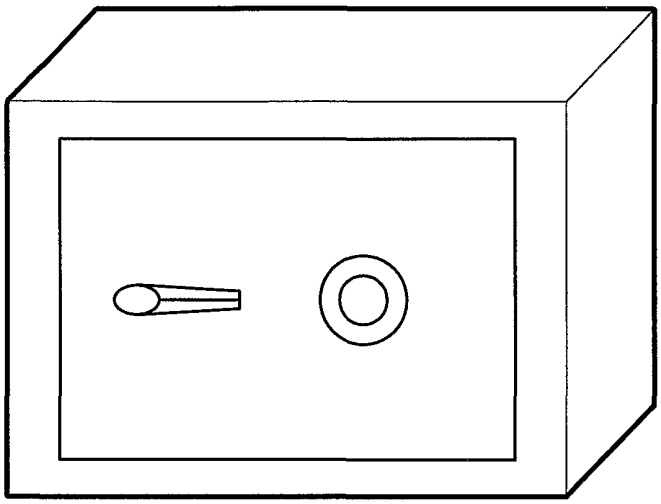


FIG. 1b

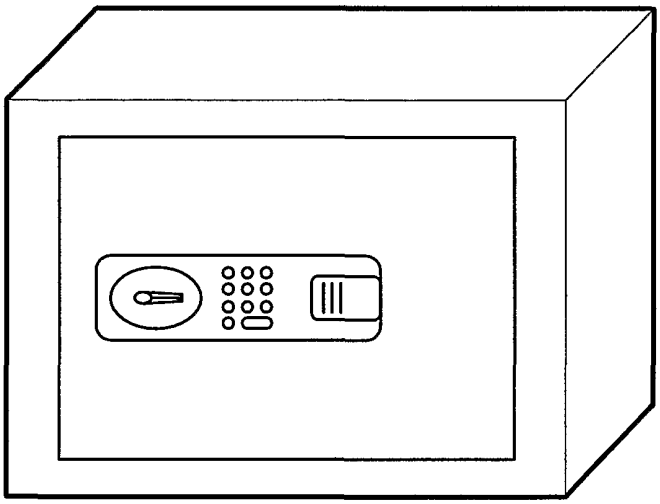


FIG. 2

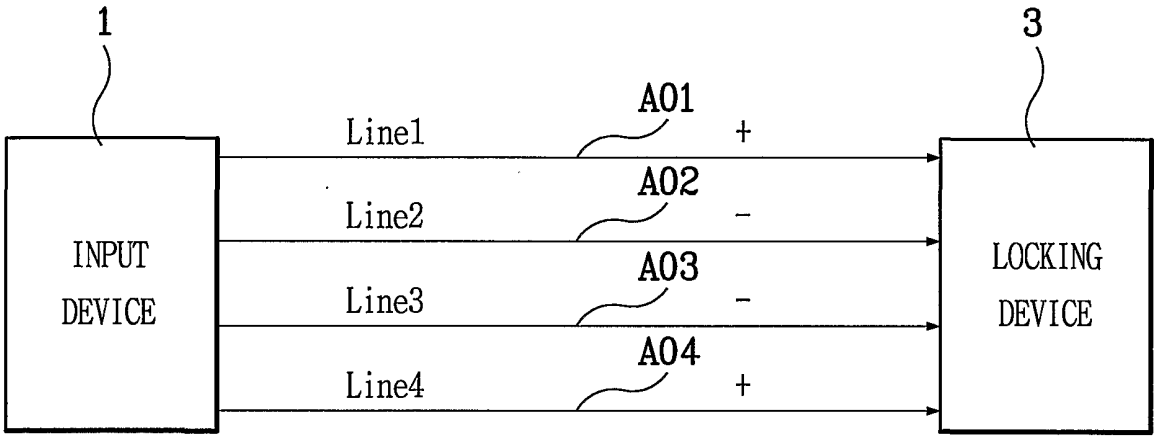

1
3
A01
Line1
+
A02
Line2
-
A03
Line3
-
A04
Line4
+
INPUT DEVICE
LOCKING DEVICE

FIG. 3

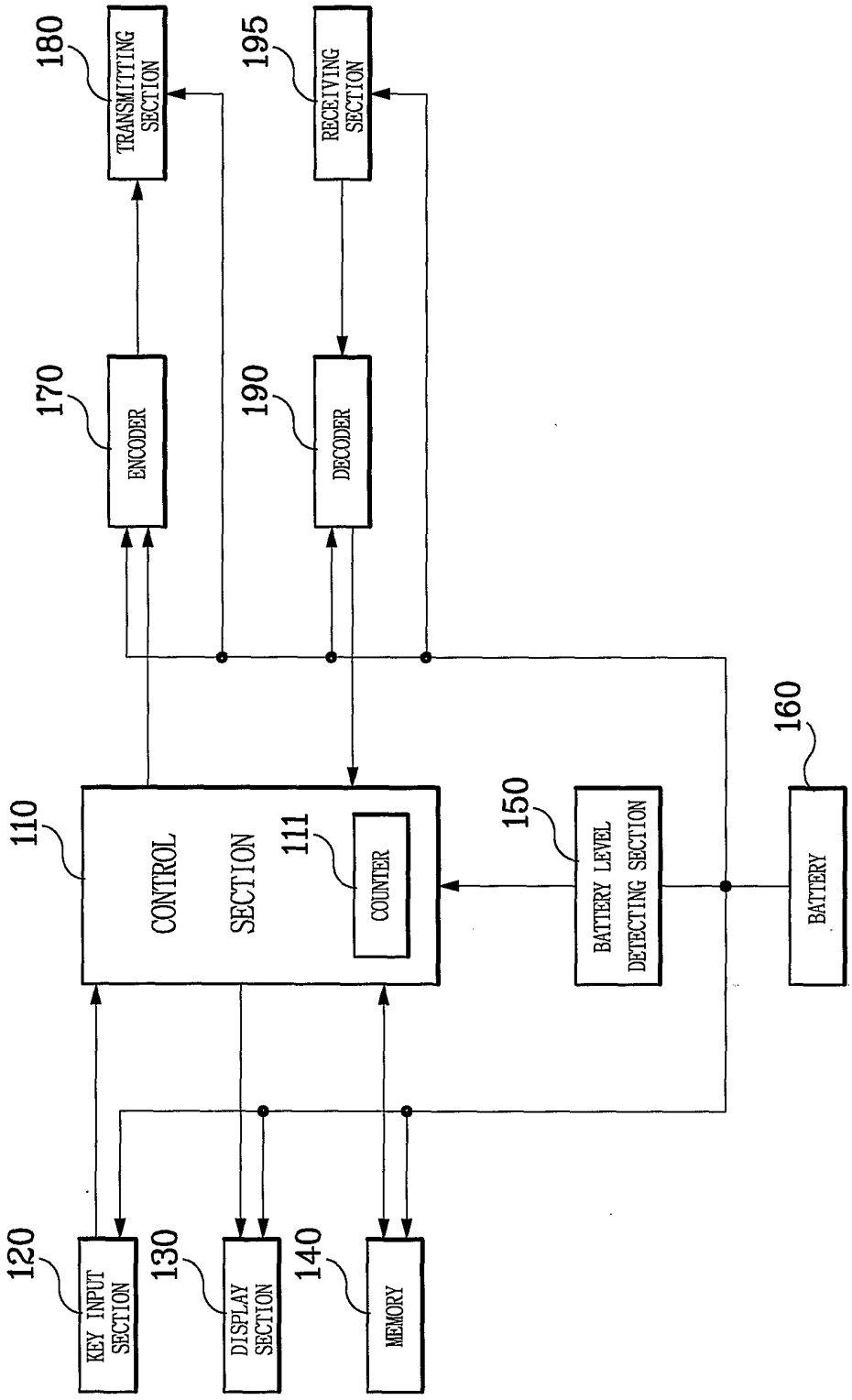

180
TRANSMITTING SECTION
195
RECEIVING SECTION
170
ENCODER
190
DECODER
110
CONTROL SECTION
111
COUNTER
150
BATTERY LEVEL DETECTING SECTION
160
BATTERY
120
KEY INPUT SECTION
130
DISPLAY SECTION
140
MEMORY

FIG. 4

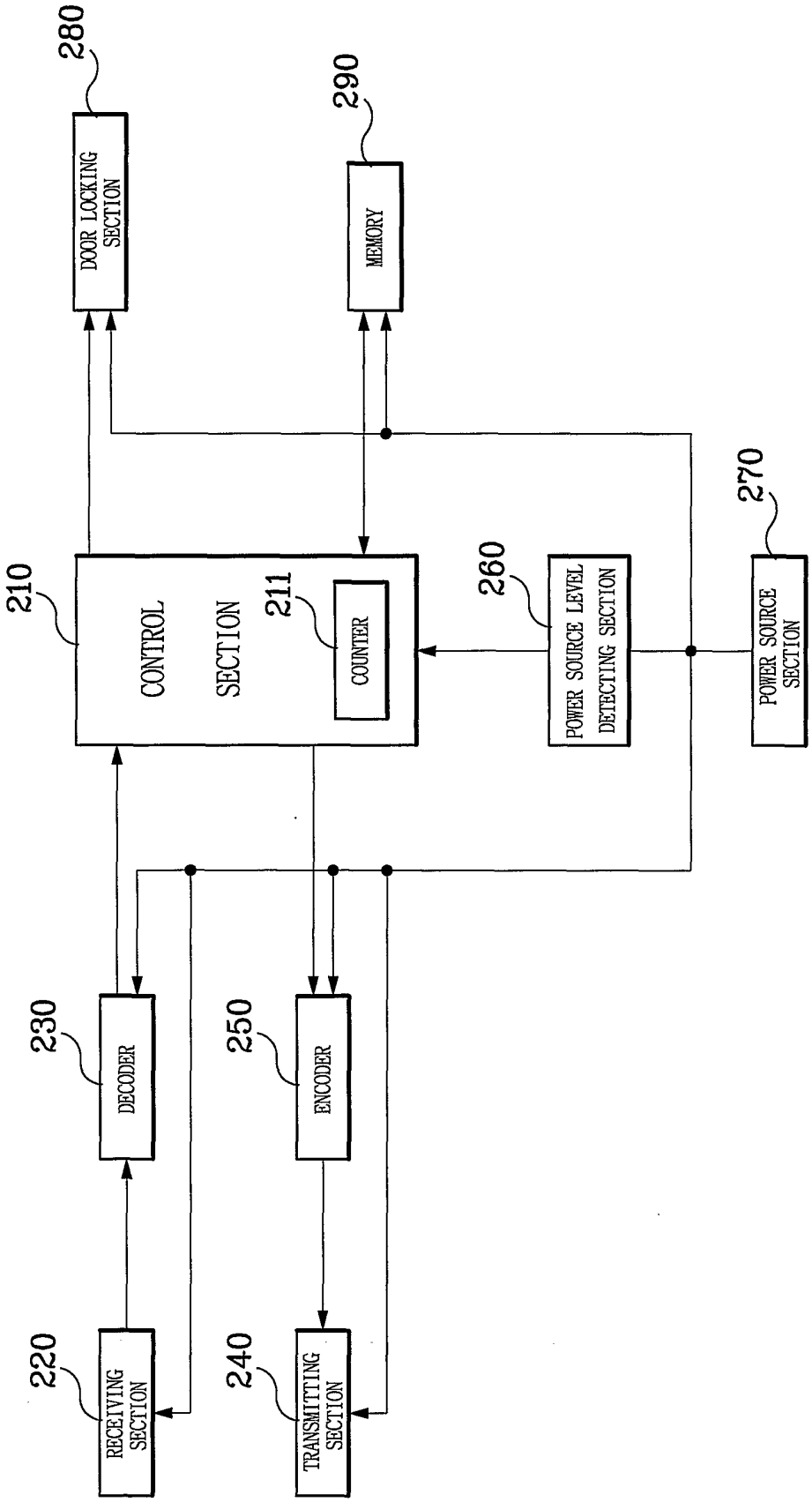

280
DOOR LOCKING SECTION
290
MEMORY
270
210
CONTROL SECTION
211
COUNTER
260
POWER SOURCE LEVEL DETECTING SECTION
POWER SOURCE SECTION
230
DECODER
250
ENCODER
220
RECEIVING SECTION
240
TRANSMITTING SECTION

FIG. 5

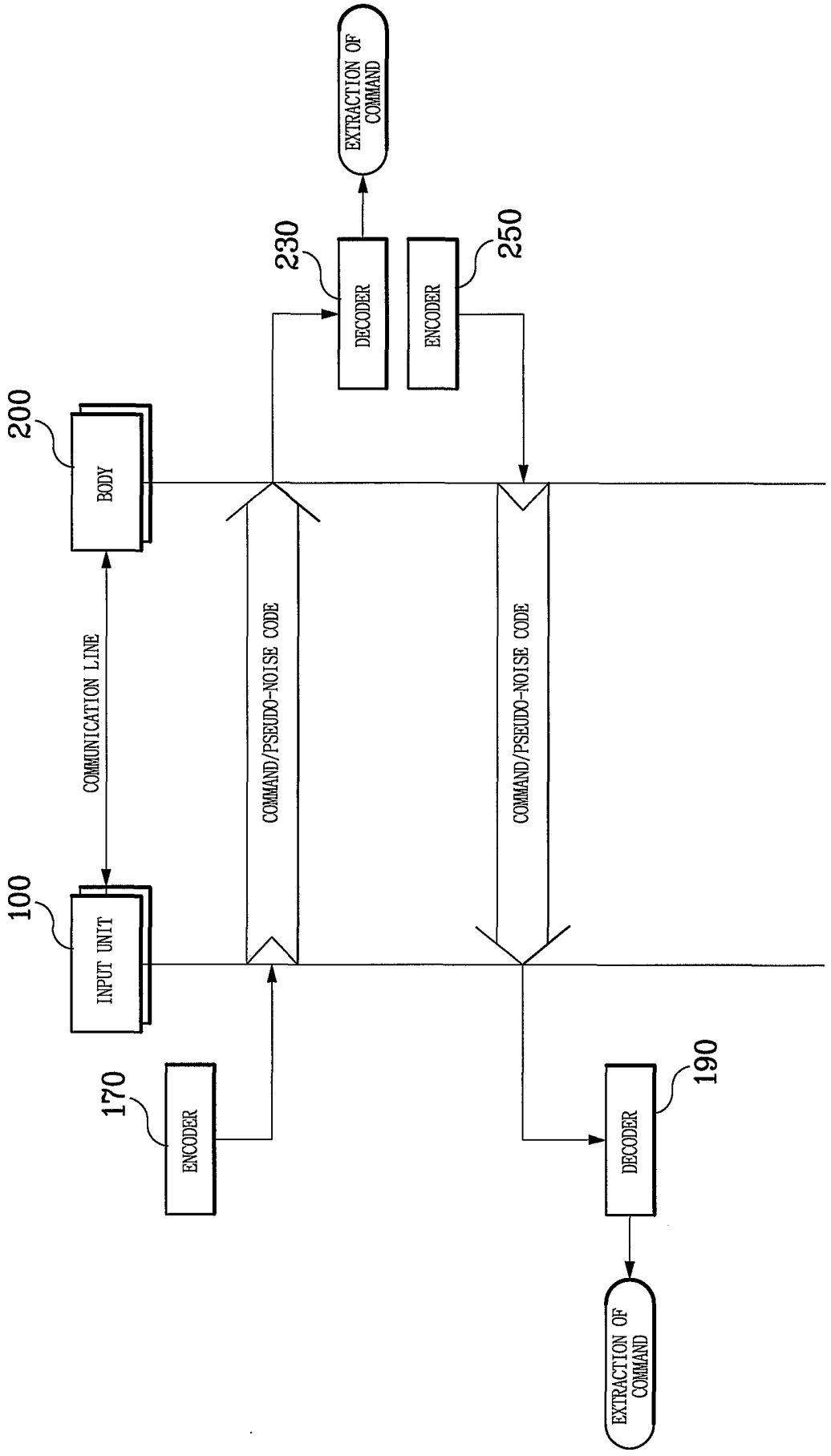

EXTRACTION OF COMMAND
230
DECODER
250
ENCODER
200
BODY
COMMUNICATION LINE
COMMAND/PSEUDO-NOISE CODE
COMMAND/PSEUDO-NOISE CODE
100
INPUT UNIT
170
ENCODER
190
DECODER
EXTRACTION OF COMMAND

FIG. 6

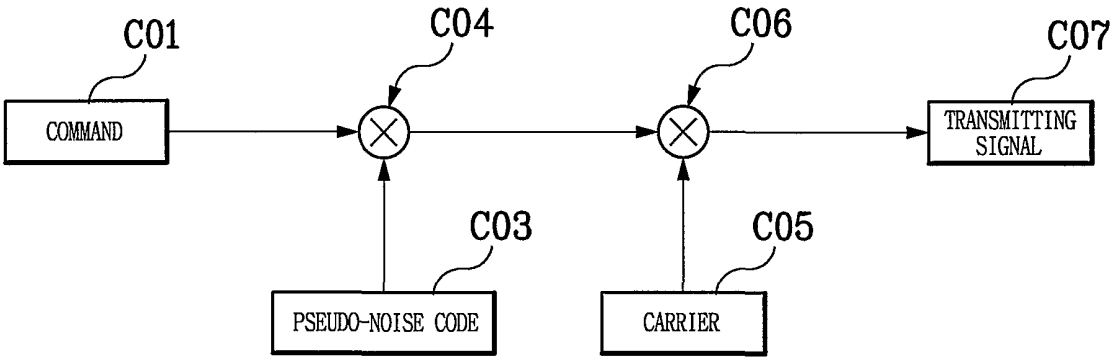

C01
C04
C06
C07
COMMAND
TRANSMITTING SIGNAL
C03
C05
PSEUDO-NOISE CODE
CARRIER

FIG. 7

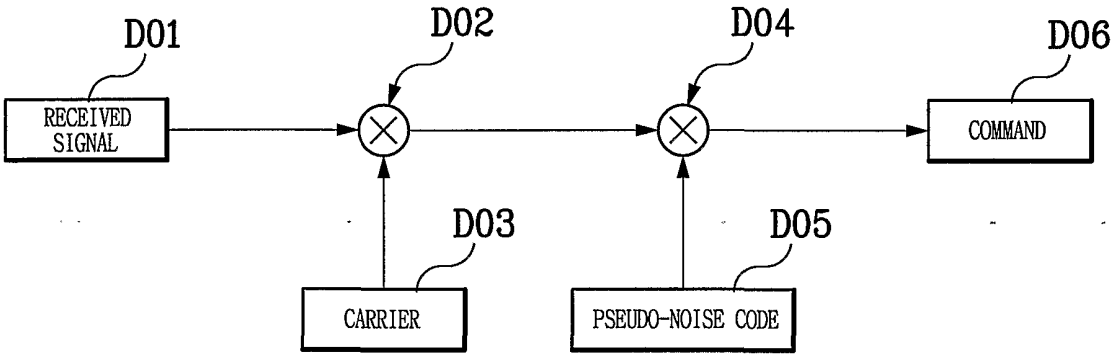

D01
D02
D04
D06
RECEIVED SIGNAL
COMMAND
D03
D05
CARRIER
PSEUDO-NOISE CODE

FIG. 8

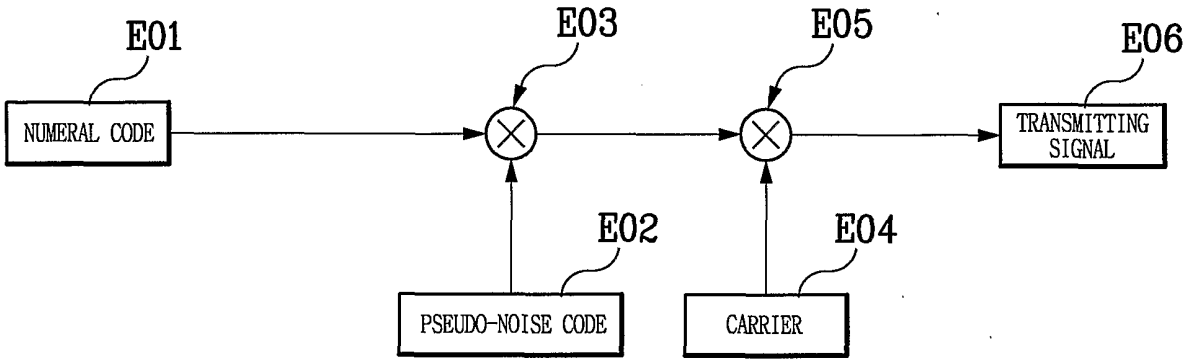

E01
NUMERAL CODE
E03
E05
E06
TRANSMITTING SIGNAL
E02
PSEUDO-NOISE CODE
E04
CARRIER

FIG. 9

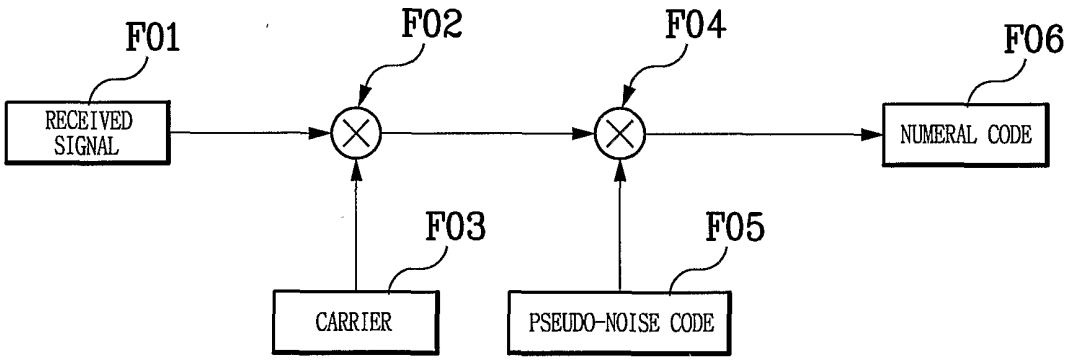

F01
RECEIVED SIGNAL
F02
F04
F06
NUMERAL CODE
F03
CARRIER
F05
PSEUDO-NOISE CODE

FIG. 10

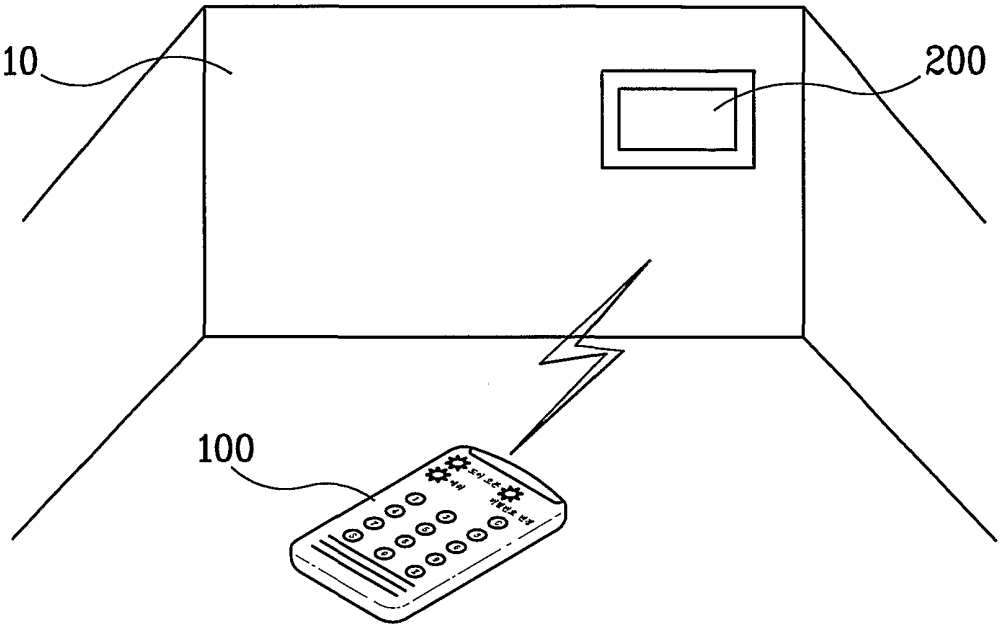


FIG. 11

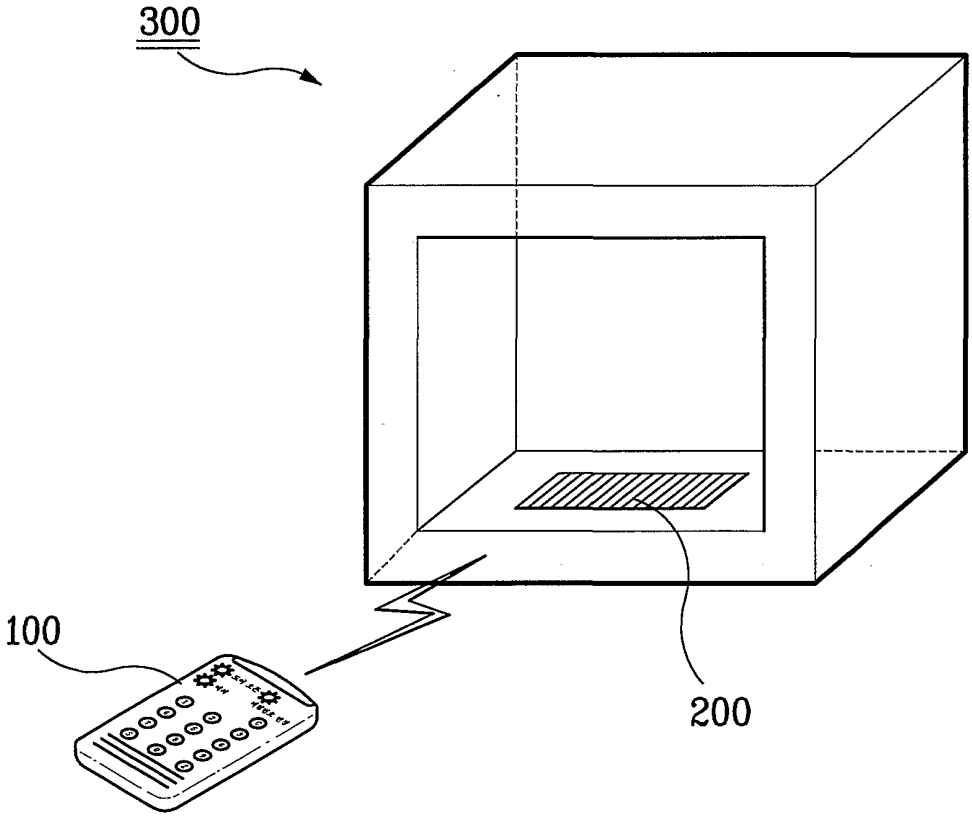


FIG. 12

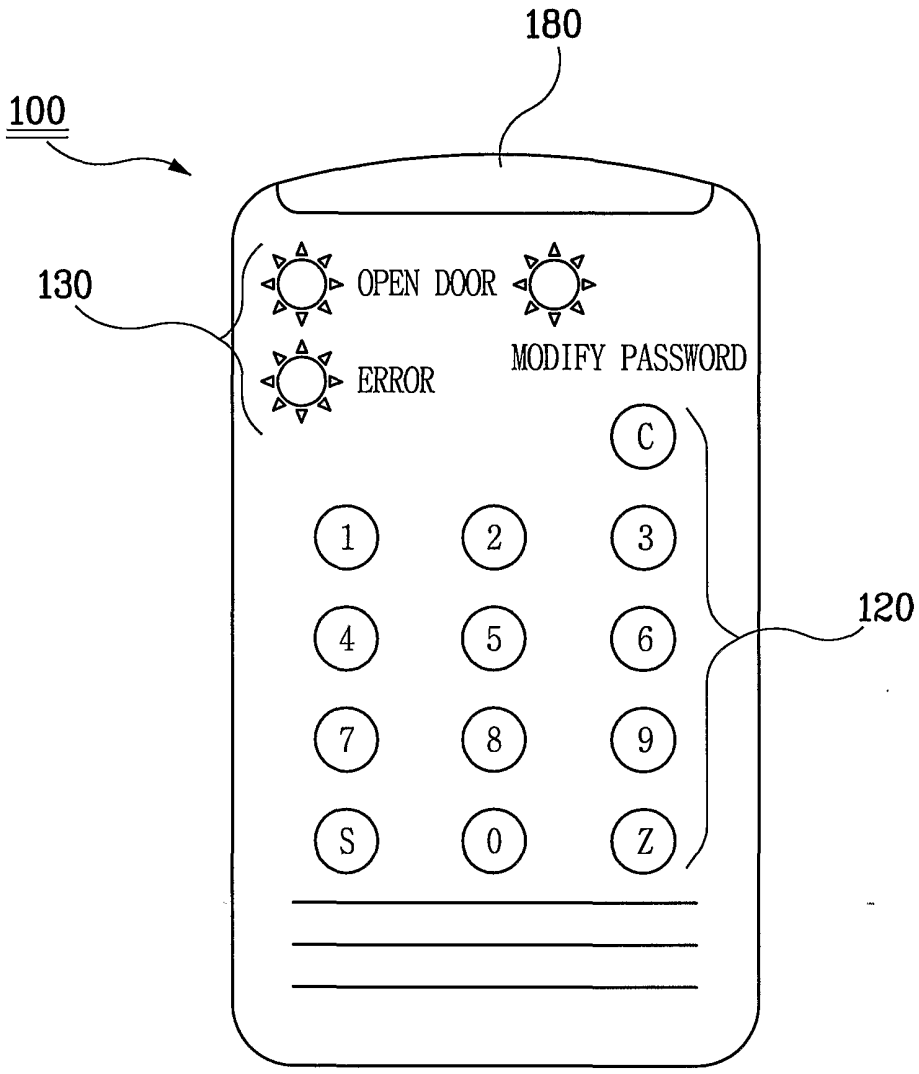

180
100
130
OPEN DOOR
ERROR
MODIFY PASSWORD
C
1
2
3
4
5
6
7
8
9
S
0
Z
120

FIG. 13

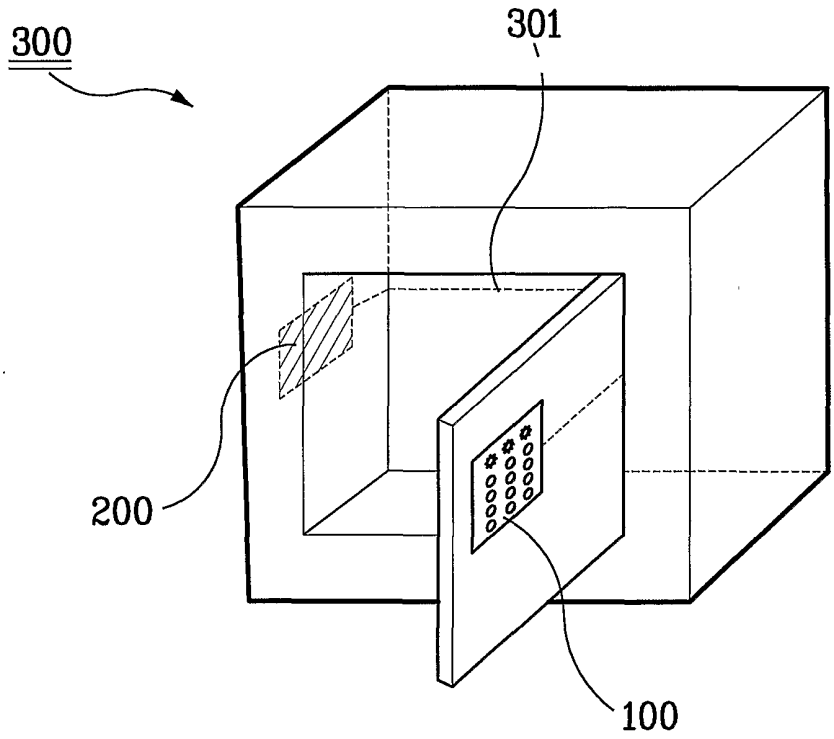


FIG. 14

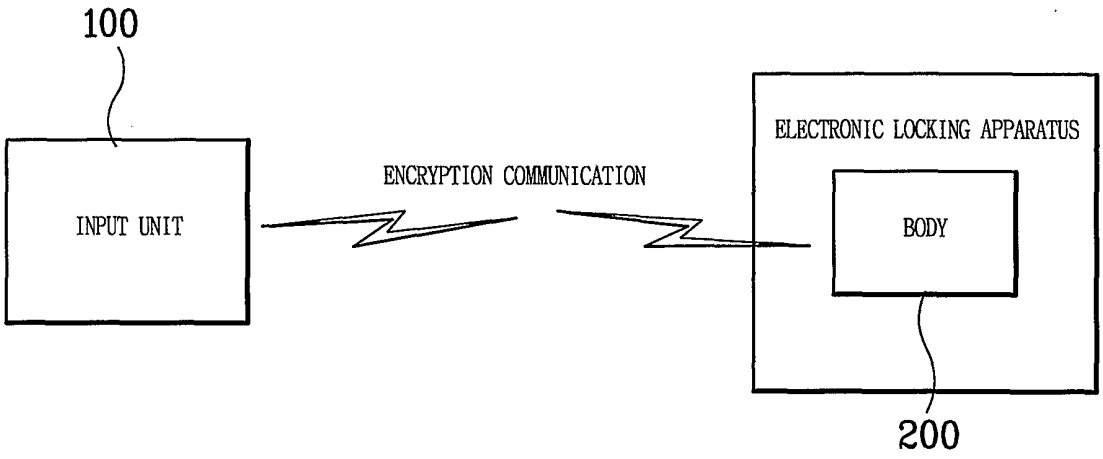

100
INPUT UNIT
ENCRYPTION COMMUNICATION
ELECTRONIC LOCKING APPARATUS
BODY
200

FIG. 15

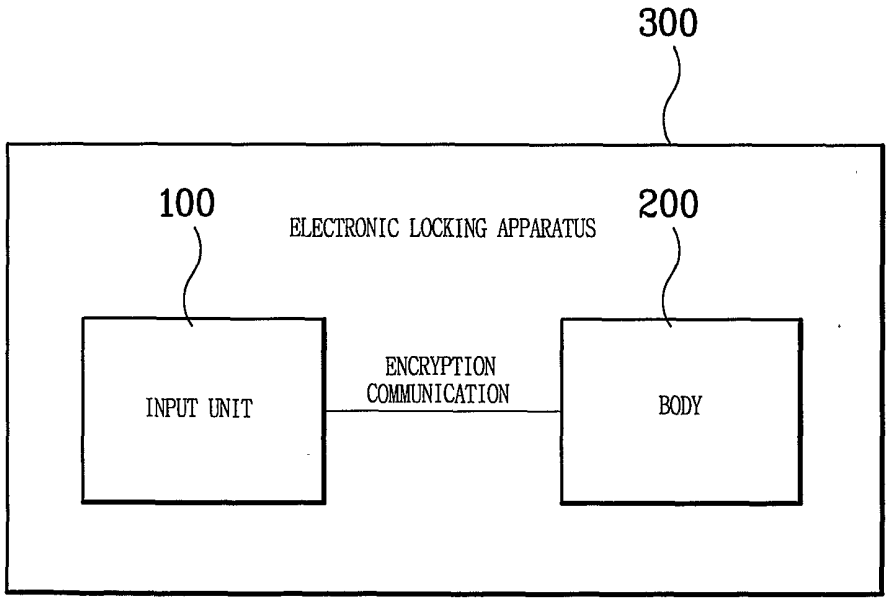

300
100
ELECTRONIC LOCKING APPARATUS
200
INPUT UNIT
ENCRYPTION
COMMUNICATION
BODY

FIG. 16

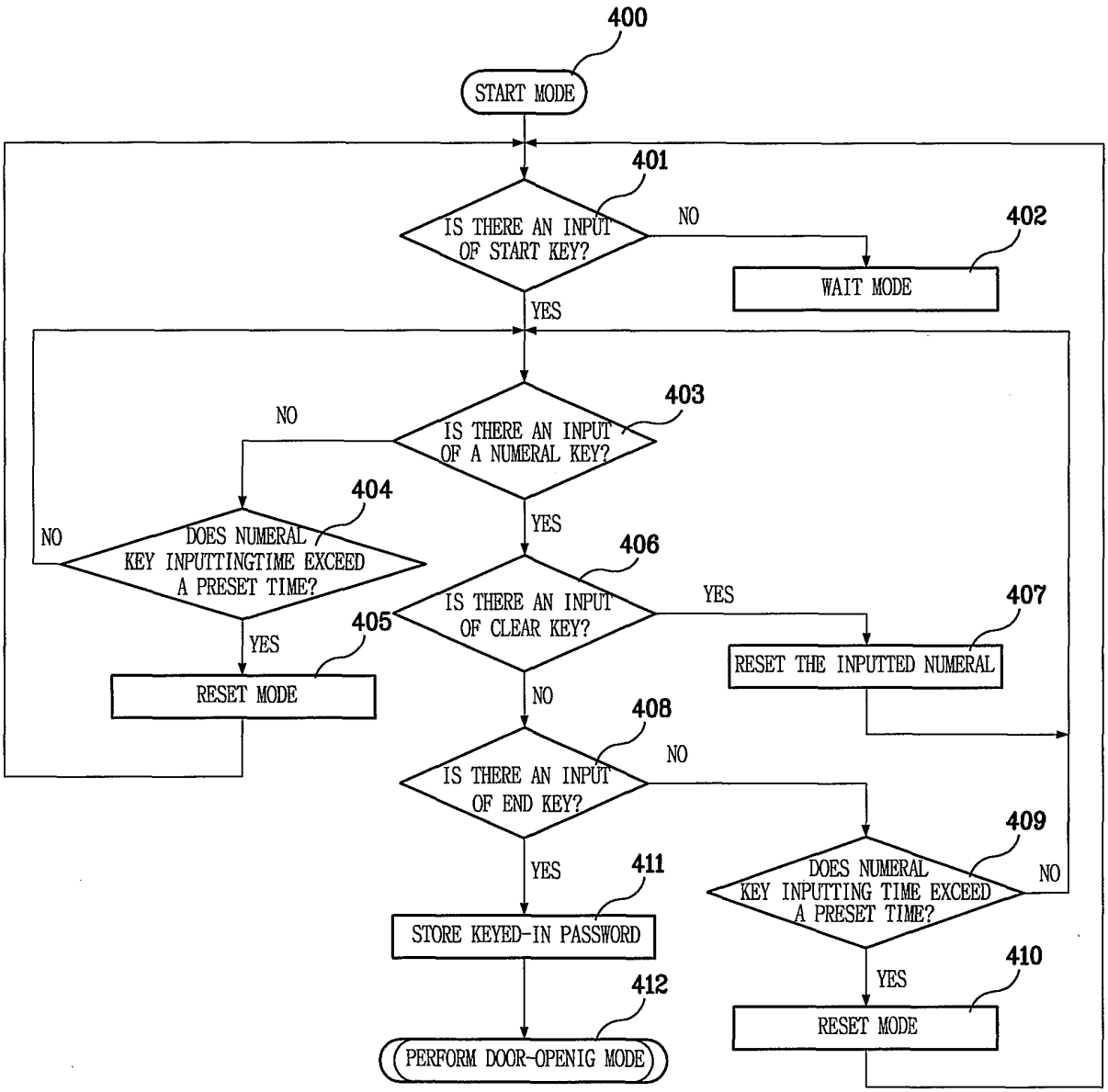

400
START MODE
401
IS THERE AN INPUT OF START KEY?
NO
402
WAIT MODE
YES
403
IS THERE AN INPUT OF A NUMERAL KEY?
NO
404
DOES NUMERAL KEY INPUTTINGTIME EXCEED A PRESET TIME?
NO
YES
405
RESET MODE
YES
406
IS THERE AN INPUT OF CLEAR KEY?
YES
407
RESET THE INPUTTED NUMERAL
NO
408
IS THERE AN INPUT OF END KEY?
NO
409
DOES NUMERAL KEY INPUTTING TIME EXCEED A PRESET TIME?
NO
YES
410
RESET MODE
YES
411
STORE KEYED-IN PASSWORD
412
PERFORM DOOR-OPENIG MODE

FIG. 17a

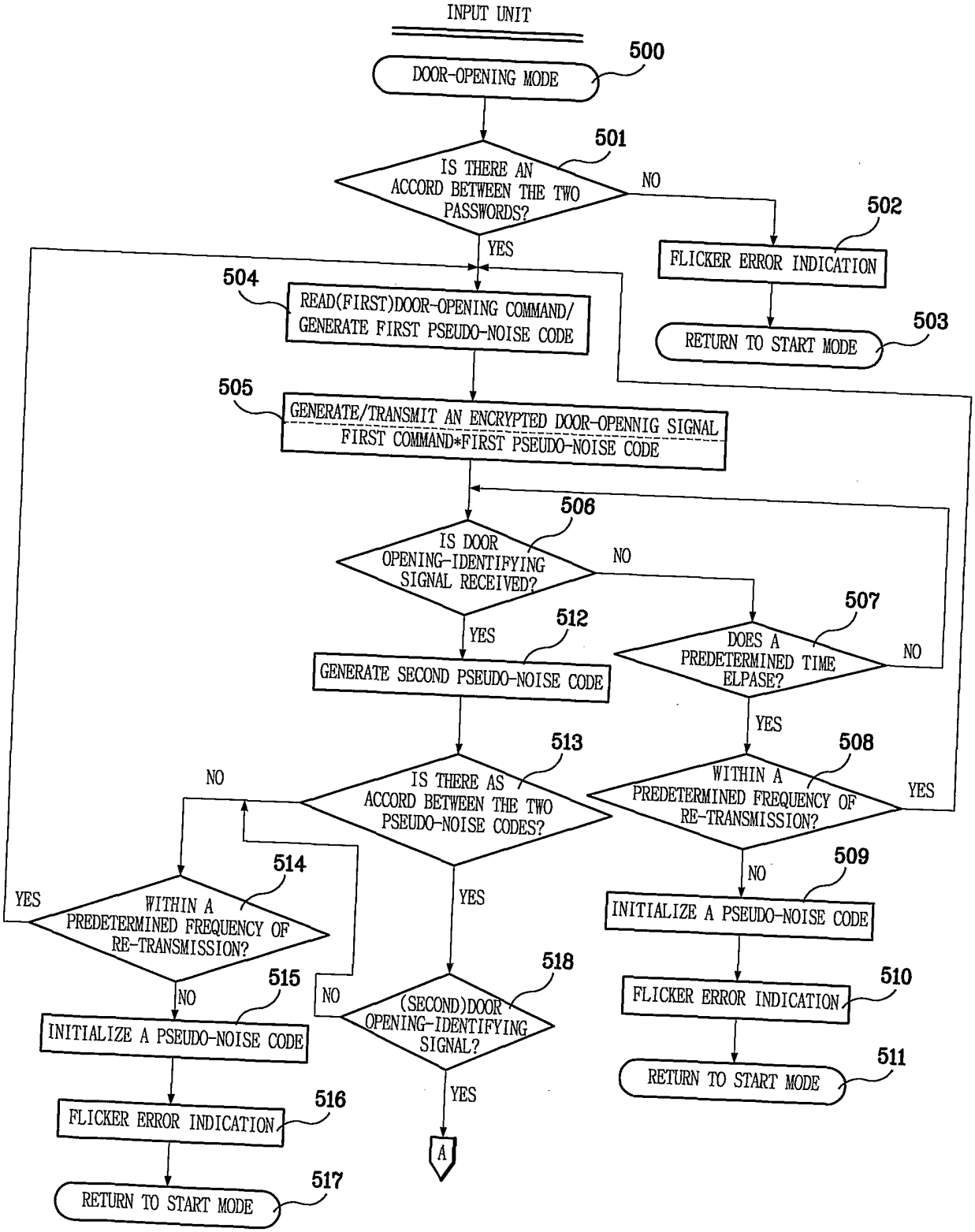

INPUT UNIT
DOOR-OPENING MODE
500
IS THERE AN ACCORD BETWEEN THE TWO PASSWORDS?
501
NO
YES
FLICKER ERROR INDICATION
502
RETURN TO START MODE
503
READ(FIRST)DOOR-OPENING COMMAND/ GENERATE FIRST PSEUDO-NOISE CODE
504
GENERATE/TRANSMIT AN ENCRYPTED DOOR-OPENNIG SIGNAL FIRST COMMAND*FIRST PSEUDO-NOISE CODE
505
IS DOOR OPENING-IDENTIFYING SIGNAL RECEIVED?
506
NO
YES
DOES A PREDETERMINED TIME ELPASE?
507
NO
YES
WITHIN A PREDETERMINED FREQUENCY OF RE-TRANSMISSION?
508
YES
NO
INITIALIZE A PSEUDO-NOISE CODE
509
FLICKER ERROR INDICATION
510
RETURN TO START MODE
511
GENERATE SECOND PSEUDO-NOISE CODE
512
IS THERE AS ACCORD BETWEEN THE TWO PSEUDO-NOISE CODES?
513
NO
YES
(SECOND)DOOR OPENING-IDENTIFYING SIGNAL?
518
NO
YES
A
WITHIN A PREDETERMINED FREQUENCY OF RE-TRANSMISSION?
514
YES
NO
INITIALIZE A PSEUDO-NOISE CODE
515
FLICKER ERROR INDICATION
516
RETURN TO START MODE
517

FIG. 17b

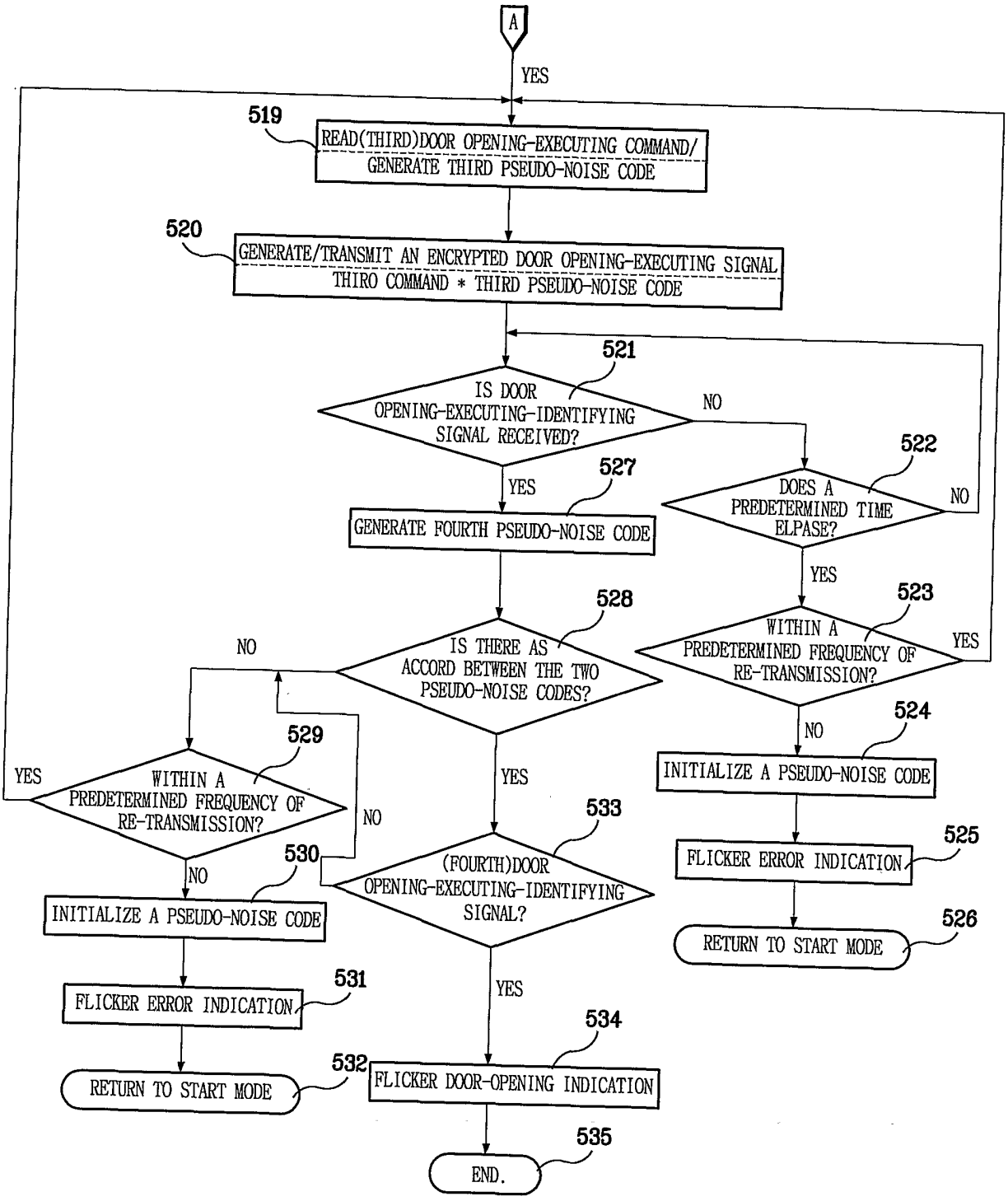

A
YES
519
READ(THIRD)DOOR OPENING-EXECUTING COMMAND/ GENERATE THIRD PSEUDO-NOISE CODE
520
GENERATE/TRANSMIT AN ENCRYPTED DOOR OPENING-EXECUTING SIGNAL THIRO COMMAND * THIRD PSEUDO-NOISE CODE
521
IS DOOR OPENING-EXECUTING-IDENTIFYING SIGNAL RECEIVED?
NO
YES
522
DOES A PREDETERMINED TIME ELPASE?
NO
YES
527
GENERATE FOURTH PSEUDO-NOISE CODE
523
WITHIN A PREDETERMINED FREQUENCY OF RE-TRANSMISSION?
YES
NO
524
INITIALIZE A PSEUDO-NOISE CODE
525
FLICKER ERROR INDICATION
526
RETURN TO START MODE
528
IS THERE AS ACCORD BETWEEN THE TWO PSEUDO-NOISE CODES?
NO
YES
529
WITHIN A PREDETERMINED FREQUENCY OF RE-TRANSMISSION?
YES
NO
530
NO
INITIALIZE A PSEUDO-NOISE CODE
531
FLICKER ERROR INDICATION
532
RETURN TO START MODE
533
(FOURTH)DOOR OPENING-EXECUTING-IDENTIFYING SIGNAL?
YES
534
FLICKER DOOR-OPENING INDICATION
535
END.

FIG. 18a

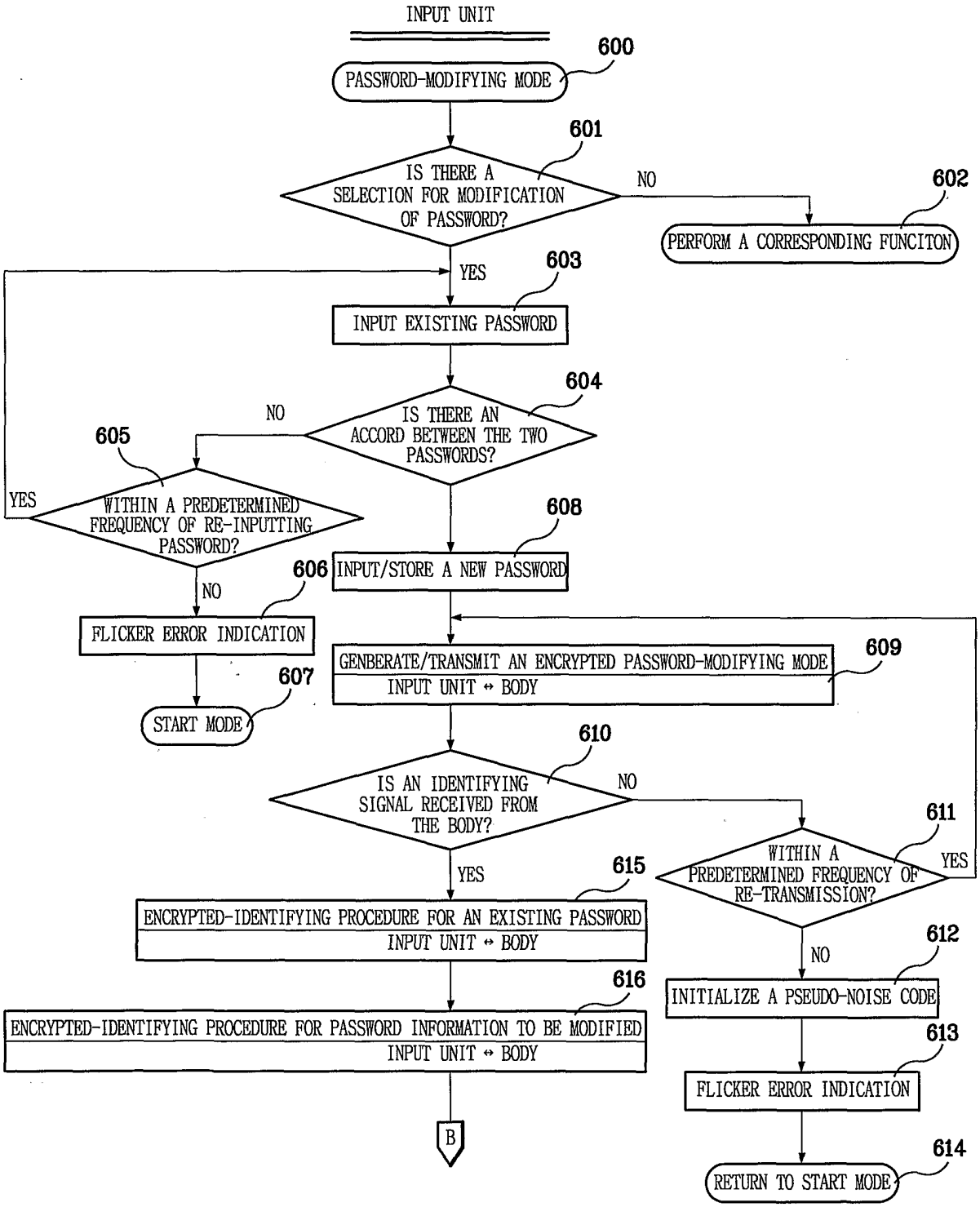

INPUT UNIT
600
PASSWORD-MODIFYING MODE
601
IS THERE A SELECTION FOR MODIFICATION OF PASSWORD?
NO
602
PERFORM A CORRESPONDING FUNCITON
YES
603
INPUT EXISTING PASSWORD
604
IS THERE AN ACCORD BETWEEN THE TWO PASSWORDS?
NO
605
WITHIN A PREDETERMINED FREQUENCY OF RE-INPUTTING PASSWORD?
YES
NO
606
FLICKER ERROR INDICATION
607
START MODE
608
INPUT/STORE A NEW PASSWORD
609
GENBERATE/TRANSMIT AN ENCRYPTED PASSWORD-MODIFYING MODE
INPUT UNIT ↔ BODY
610
IS AN IDENTIFYING SIGNAL RECEIVED FROM THE BODY?
NO
YES
611
WITHIN A PREDETERMINED FREQUENCY OF RE-TRANSMISSION?
YES
NO
612
INITIALIZE A PSEUDO-NOISE CODE
613
FLICKER ERROR INDICATION
614
RETURN TO START MODE
615
ENCRYPTED-IDENTIFYING PROCEDURE FOR AN EXISTING PASSWORD
INPUT UNIT ↔ BODY
616
ENCRYPTED-IDENTIFYING PROCEDURE FOR PASSWORD INFORMATION TO BE MODIFIED
INPUT UNIT ↔ BODY
B

FIG. 18b

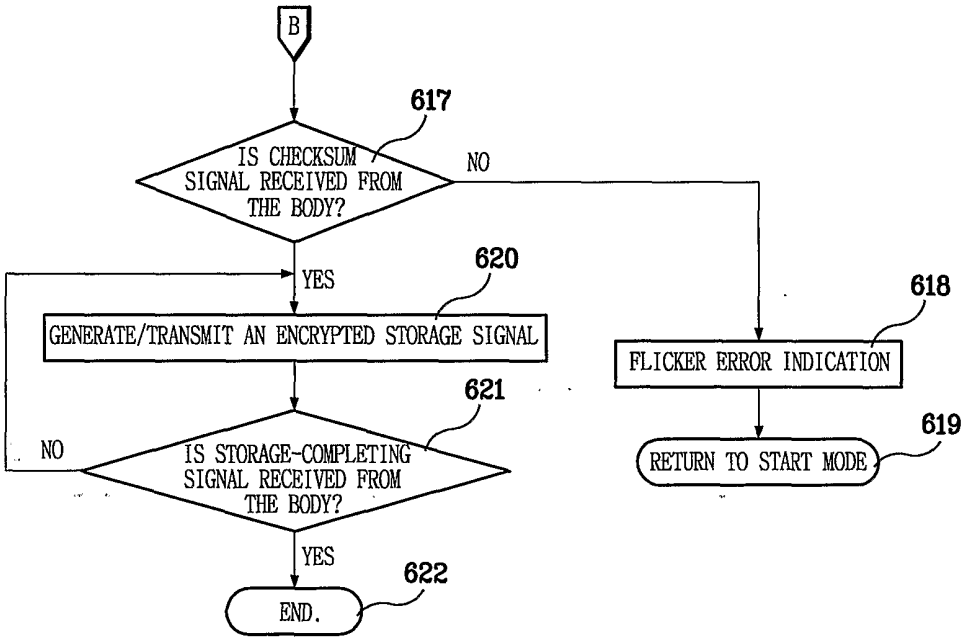

B
617
IS CHECKSUM SIGNAL RECEIVED FROM THE BODY?
NO
YES
620
GENERATE/TRANSMIT AN ENCRYPTED STORAGE SIGNAL
618
FLICKER ERROR INDICATION
621
NO
IS STORAGE-COMPLETING SIGNAL RECEIVED FROM THE BODY?
619
RETURN TO START MODE
YES
622
END.

FIG. 19

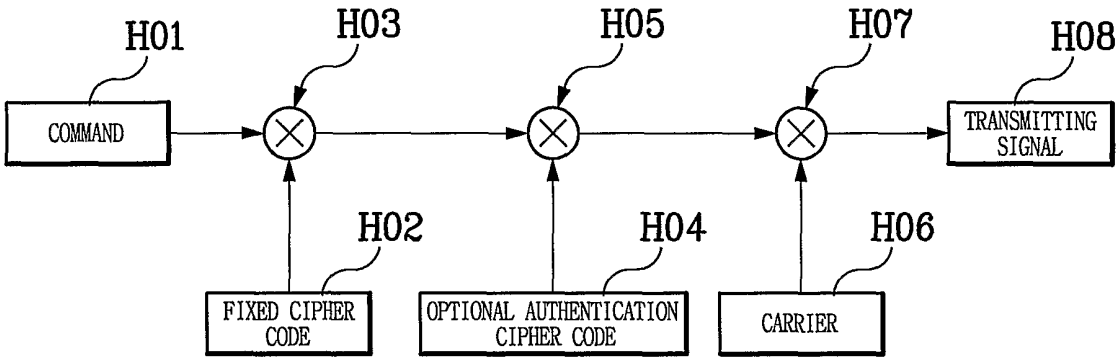

H01
H03
H05
H07
H08
COMMAND
TRANSMITTING SIGNAL
H02
H04
H06
FIXED CIPHER CODE
OPTIONAL AUTHENTICATION CIPHER CODE
CARRIER

FIG. 20

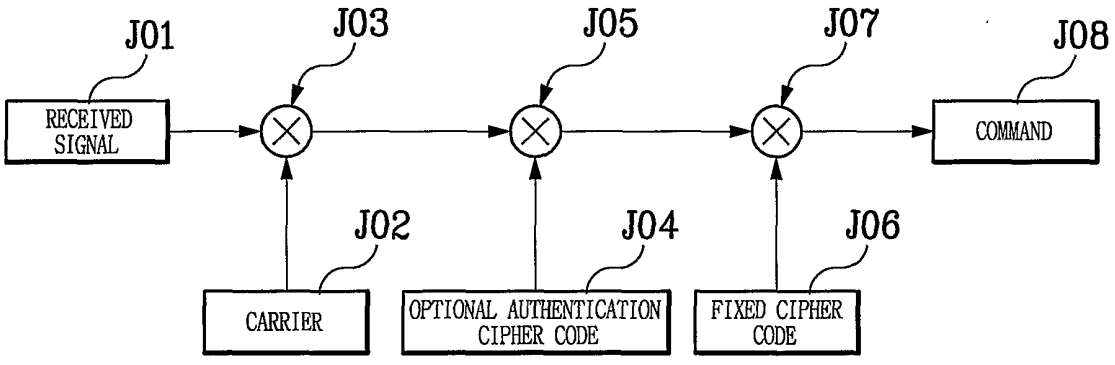

J01
J03
J05
J07
J08
RECEIVED SIGNAL
COMMAND
J02
J04
J06
CARRIER
OPTIONAL AUTHENTICATION CIPHER CODE
FIXED CIPHER CODE

FIG. 21

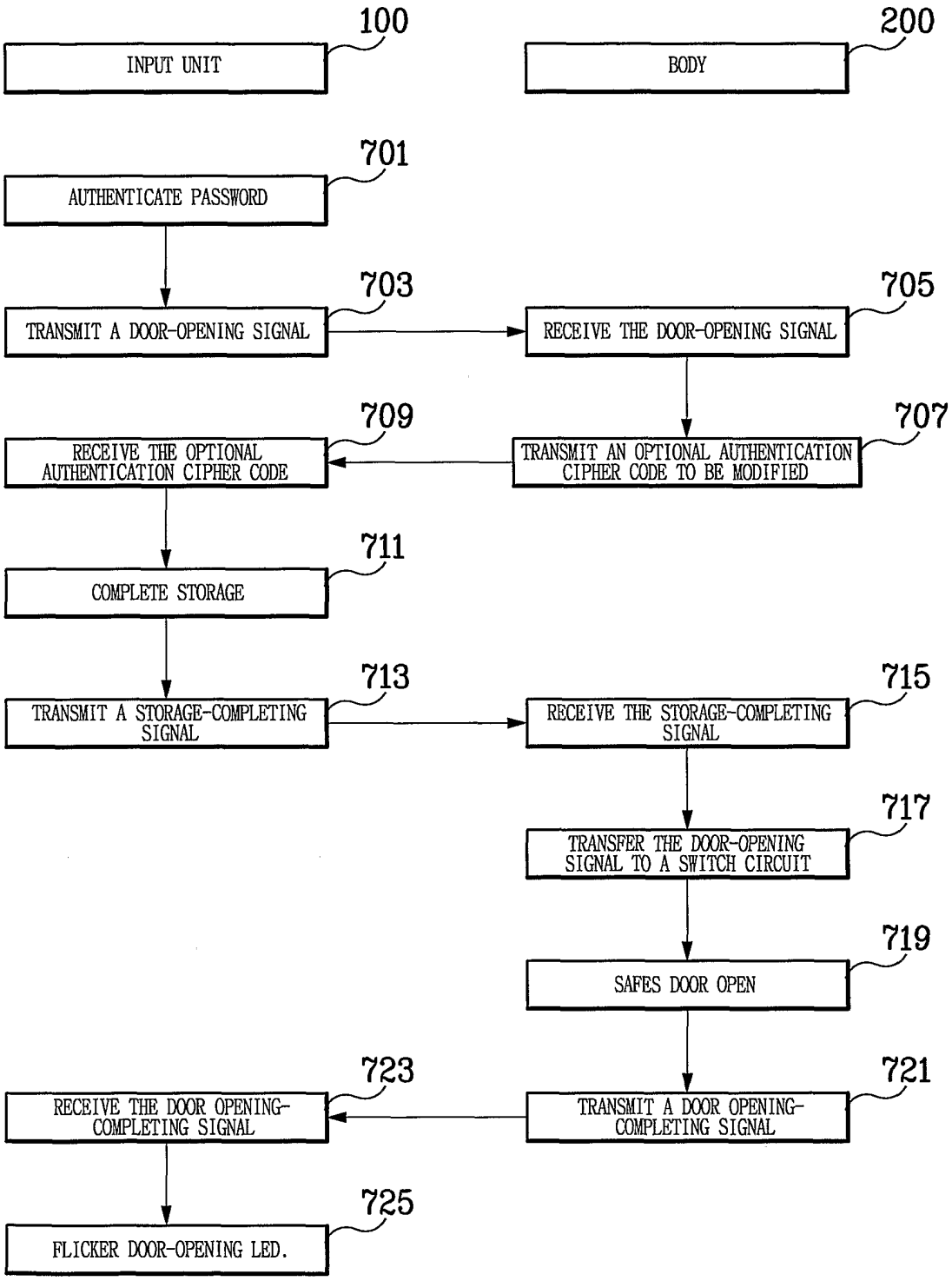

100
INPUT UNIT
200
BODY
701
AUTHENTICATE PASSWORD
703
TRANSMIT A DOOR-OPENING SIGNAL
705
RECEIVE THE DOOR-OPENING SIGNAL
709
RECEIVE THE OPTIONAL AUTHENTICATION CIPHER CODE
707
TRANSMIT AN OPTIONAL AUTHENTICATION CIPHER CODE TO BE MODIFIED
711
COMPLETE STORAGE
713
TRANSMIT A STORAGE-COMPLETING SIGNAL
715
RECEIVE THE STORAGE-COMPLETING SIGNAL
717
TRANSFER THE DOOR-OPENING SIGNAL TO A SWITCH CIRCUIT
719
SAFES DOOR OPEN
723
RECEIVE THE DOOR OPENING-COMPLETING SIGNAL
721
TRANSMIT A DOOR OPENING-COMPLETING SIGNAL
725
FLICKER DOOR-OPENING LED.

FIG. 22

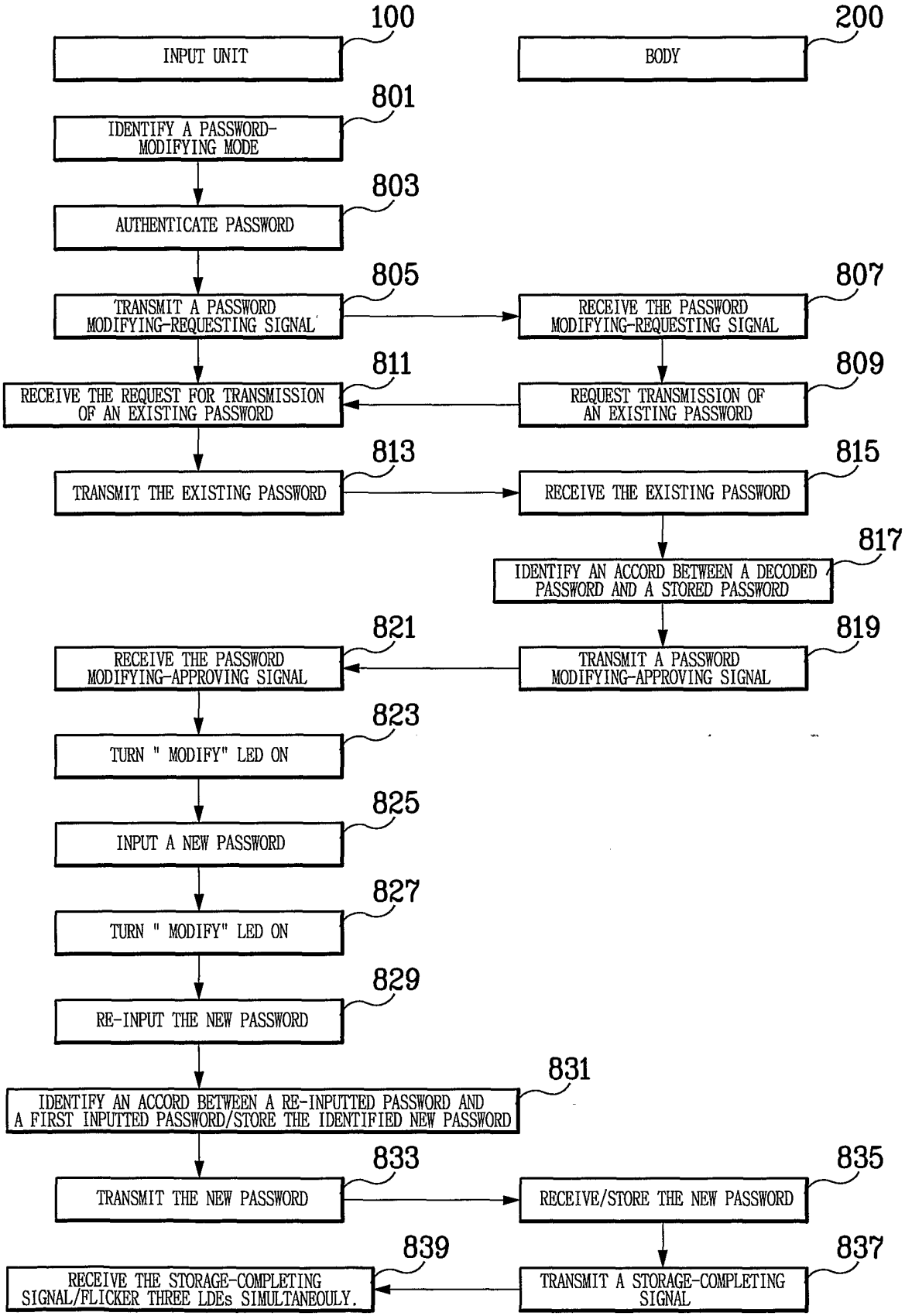

100
INPUT UNIT
200
BODY
801
IDENTIFY A PASSWORD-MODIFYING MODE
803
AUTHENTICATE PASSWORD
805
TRANSMIT A PASSWORD MODIFYING-REQUESTING SIGNAL
807
RECEIVE THE PASSWORD MODIFYING-REQUESTING SIGNAL
811
RECEIVE THE REQUEST FOR TRANSMISSION OF AN EXISTING PASSWORD
809
REQUEST TRANSMISSION OF AN EXISTING PASSWORD
813
TRANSMIT THE EXISTING PASSWORD
815
RECEIVE THE EXISTING PASSWORD
817
IDENTIFY AN ACCORD BETWEEN A DECODED PASSWORD AND A STORED PASSWORD
821
RECEIVE THE PASSWORD MODIFYING-APPROVING SIGNAL
819
TRANSMIT A PASSWORD MODIFYING-APPROVING SIGNAL
823
TURN " MODIFY" LED ON
825
INPUT A NEW PASSWORD
827
TURN " MODIFY" LED ON
829
RE-INPUT THE NEW PASSWORD
831
IDENTIFY AN ACCORD BETWEEN A RE-INPUTTED PASSWORD AND A FIRST INPUTTED PASSWORD/STORE THE IDENTIFIED NEW PASSWORD
833
TRANSMIT THE NEW PASSWORD
835
RECEIVE/STORE THE NEW PASSWORD
839
RECEIVE THE STORAGE-COMPLETING SIGNAL/FLICKER THREE LDEs SIMULTANEOULY.
837
TRANSMIT A STORAGE-COMPLETING SIGNAL

FIG. 23a

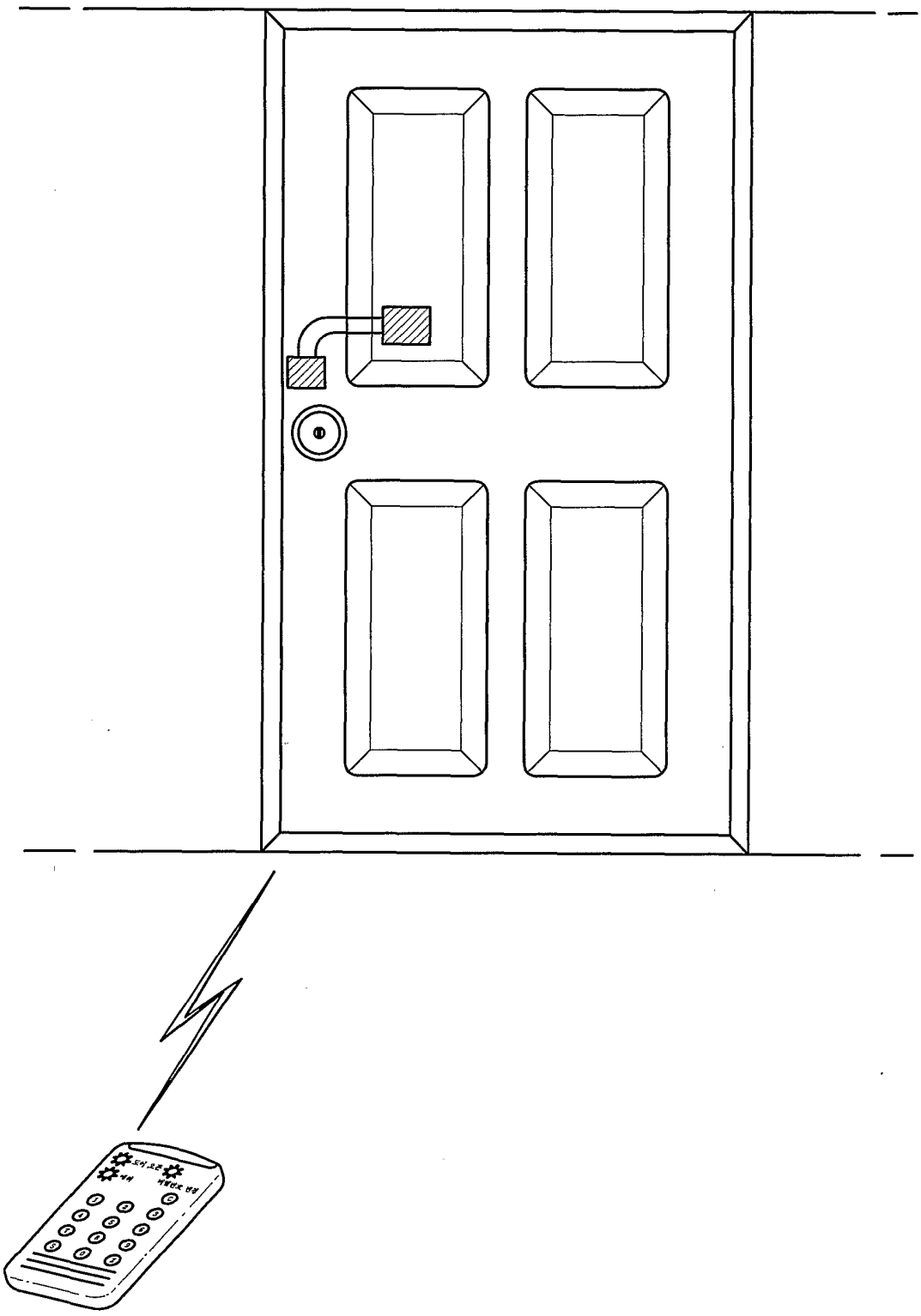


FIG. 23b

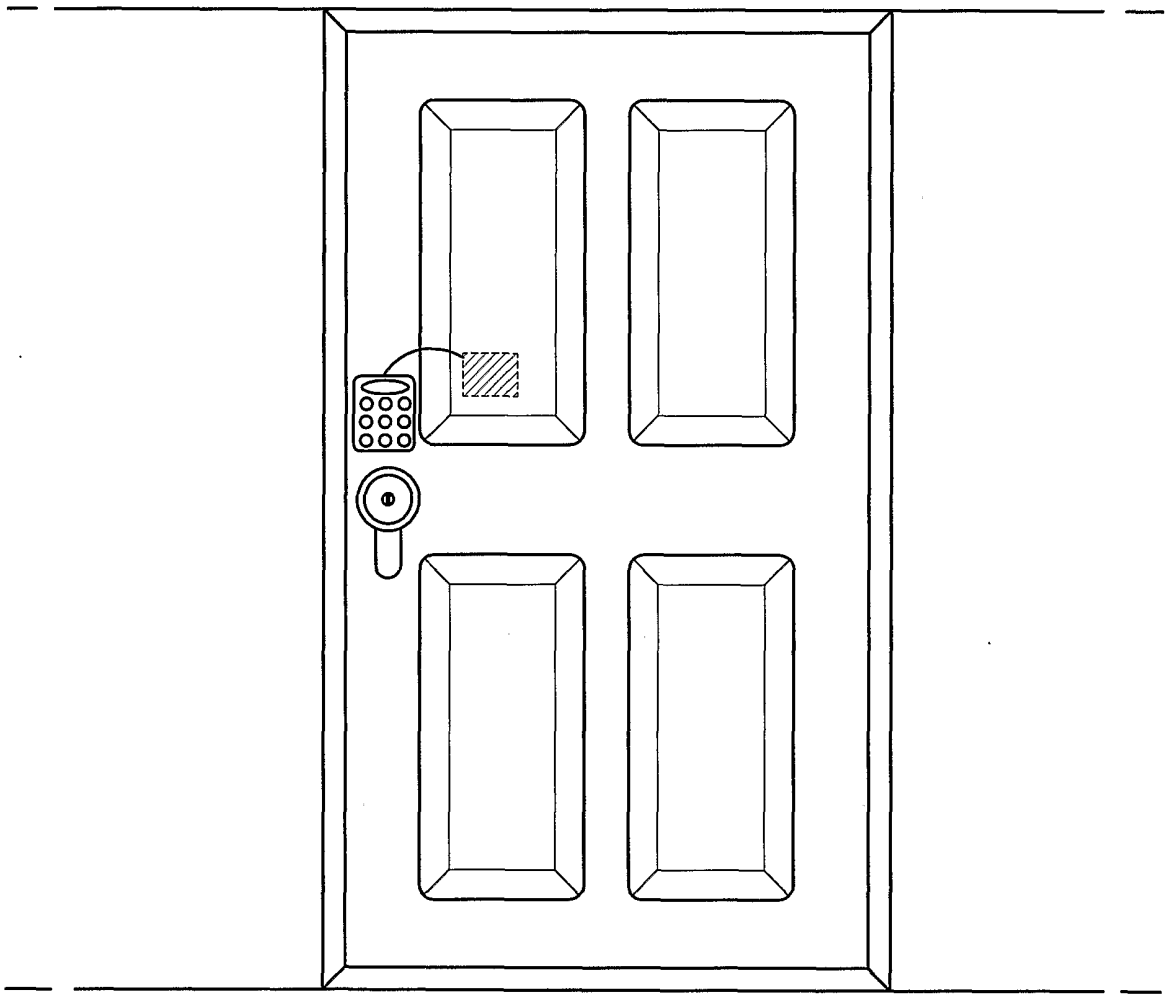


FIG. 24a

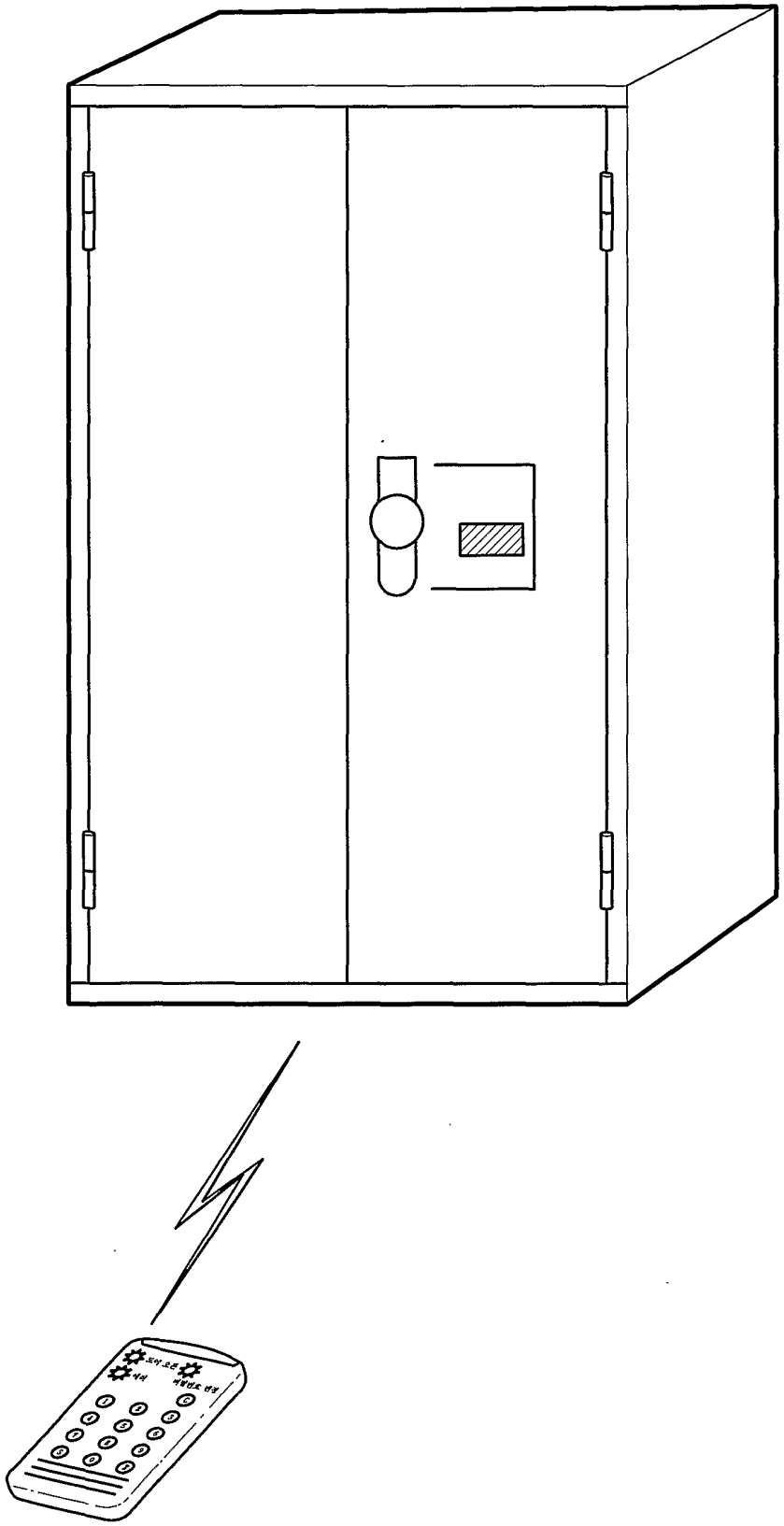


FIG. 24b

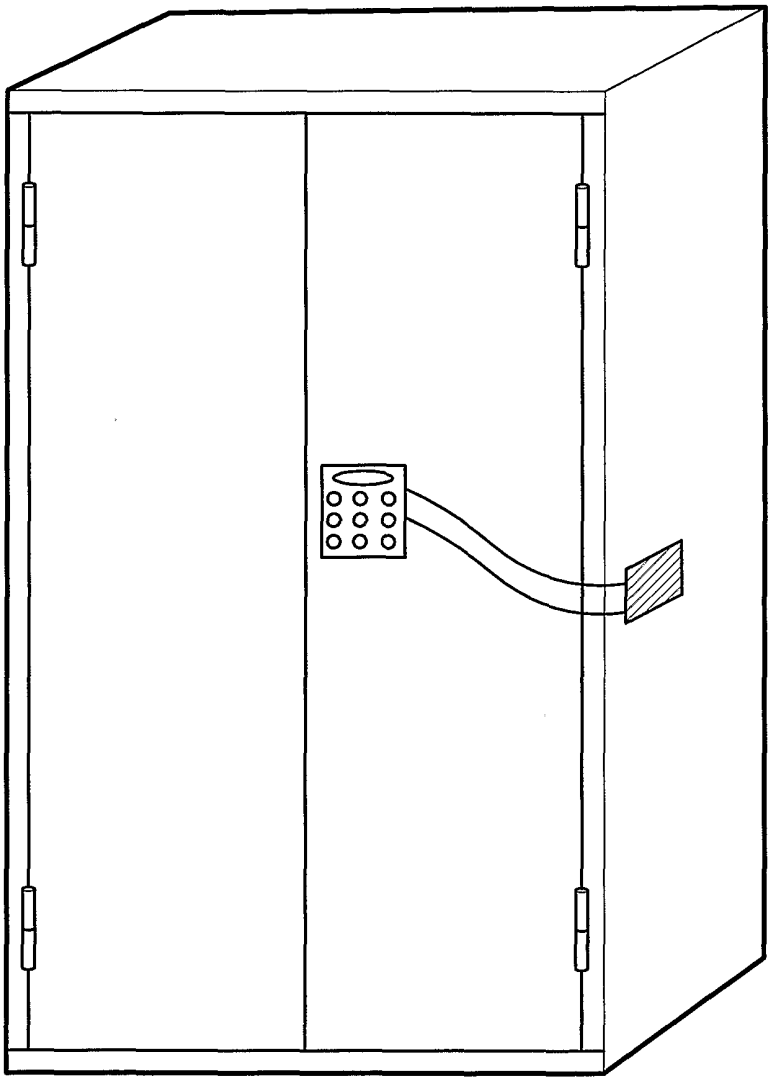


FIG. 25a

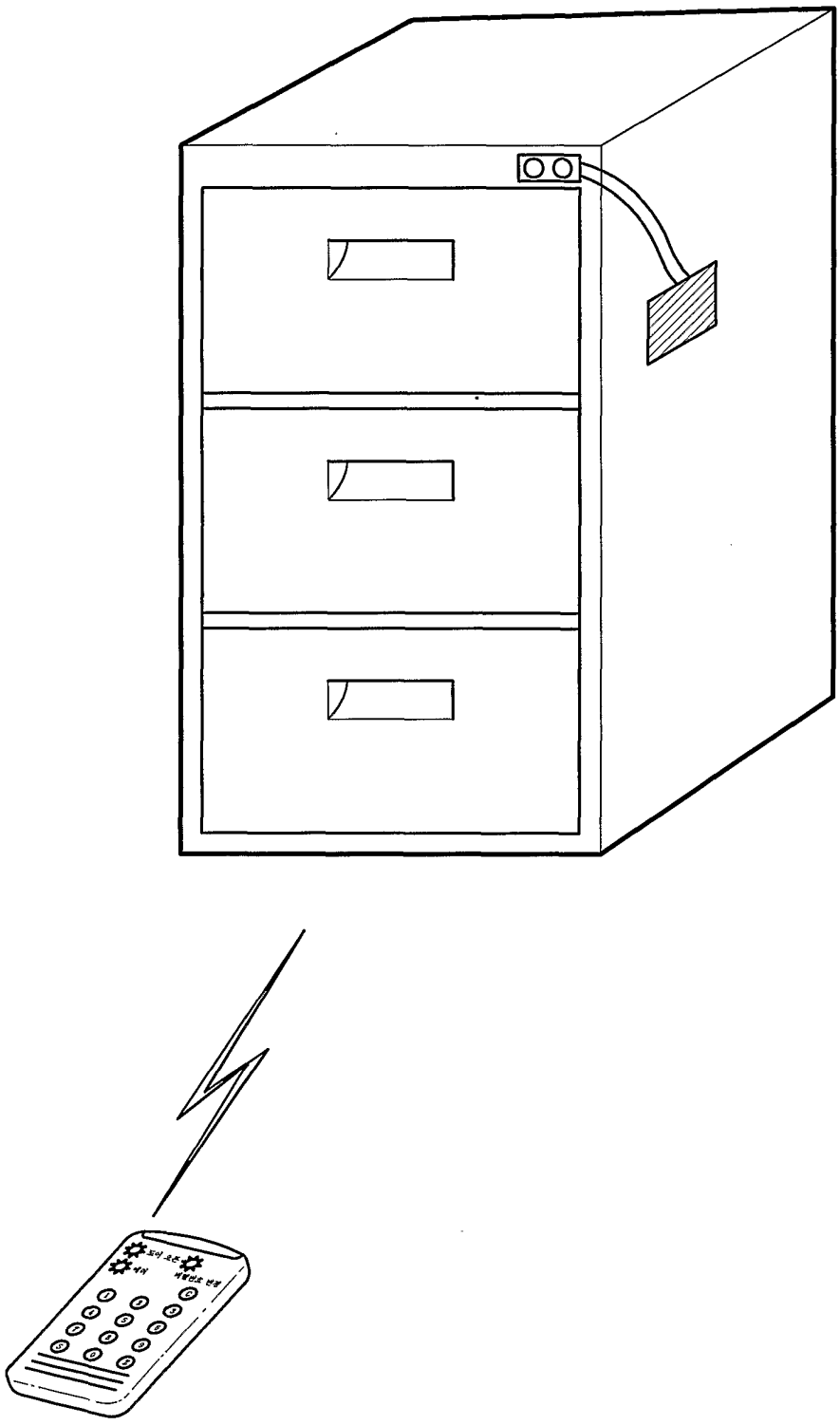
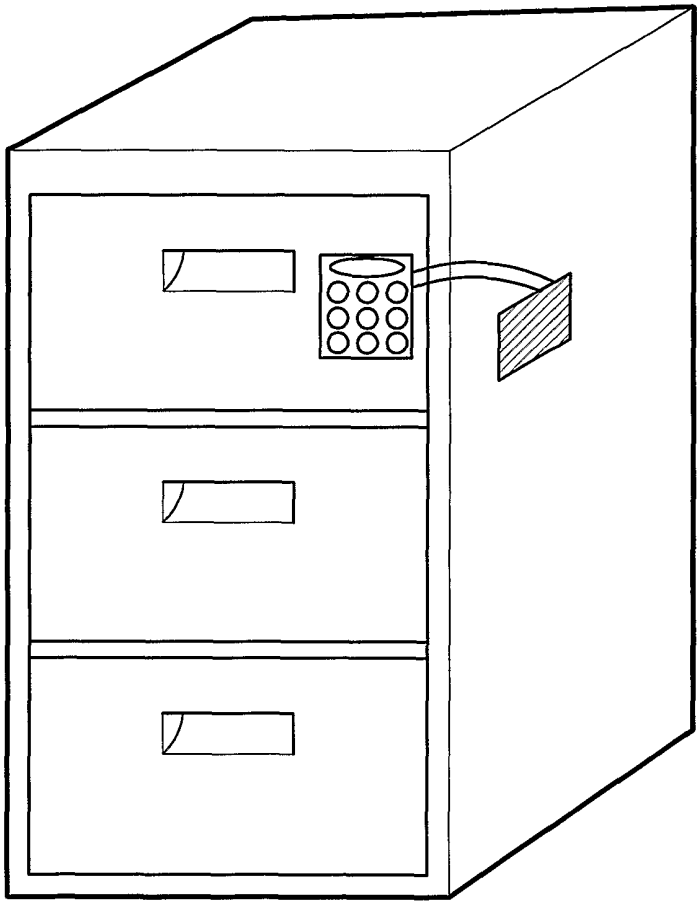



FIG. 25b