

US Patent & Trademark Office

Patent Public Search | Text View

United States Patent	12389221
Kind Code	B2
Date of Patent	August 12, 2025
Inventor(s)	Hirabayashi; Masayuki et al.

Mobile terminal and control method thereof

Abstract

There is provided a mobile terminal capable of being protected against unauthorized use by a third party without using a dedicated key device. A plurality of mobile terminals are previously registered mutually. When unlocked among them, one mobile terminal communicates with another mobile terminal in a communication range of short-range wireless communications, unlocks the above another mobile terminal, and when out of the communication range, locks it again.

Inventors: Hirabayashi; Masayuki (Yokohama, JP), Nishijima; Hideo (Hitachinaka, JP)

Applicant: MAXELL, LTD. (Kyoto, JP)

Family ID: 1000008749691

Assignee: MAXELL, LTD. (Kyoto, JP)

Appl. No.: 18/424997

Filed: January 29, 2024

Prior Publication Data

Document Identifier	Publication Date
US 20240171971 A1	May. 23, 2024

Foreign Application Priority Data

JP	2012-117105	May. 23, 2012
----	-------------	---------------

Related U.S. Application Data

continuation parent-doc US 17399126 20210811 US 11924633 child-doc US 18424997
continuation parent-doc US 16115940 20180829 US 11388593 20220712 child-doc US 17399126
continuation parent-doc US 13874535 20130501 US 10212586 20190219 child-doc US 16115940

Publication Classification

Int. Cl.: H04W12/06 (20210101); H04L9/40 (20220101)

U.S. Cl.:

CPC H04W12/06 (20130101); H04L63/0492 (20130101);

Field of Classification Search

CPC: H04W (4/80); H04W (12/06)

References Cited

U.S. PATENT DOCUMENTS

Patent No.	Issued Date	Patentee Name	U.S. Cl.	CPC
6871063	12/2004	Schiffer	N/A	N/A
7941534	12/2010	De La Huerga	N/A	N/A
8149089	12/2011	Lin et al.	N/A	N/A
8810392	12/2013	Teller et al.	N/A	N/A
9339727	12/2015	Isgreen	N/A	N/A
10097353	12/2017	Carlson	N/A	H04L 67/306
2004/0046638	12/2003	Kawasaki	N/A	N/A
2004/0181678	12/2003	Lee et al.	N/A	N/A
2006/0041746	12/2005	Kirkup et al.	N/A	N/A
2006/0123242	12/2005	Merrem	N/A	N/A
2006/0128305	12/2005	Delalat	N/A	N/A
2006/0224882	12/2005	Chin	N/A	N/A
2007/0287423	12/2006	Kakiuchi et al.	N/A	N/A
2009/0158423	12/2008	Orlassino et al.	N/A	N/A
2010/0144275	12/2009	Satou	N/A	N/A
2011/0086615	12/2010	Golder	N/A	N/A
2011/0125875	12/2010	Matsui	709/219	H04L 63/08
2011/0195665	12/2010	Friedlaender	N/A	N/A
2012/0040611	12/2011	Griffin et al.	N/A	N/A
2012/0280790	12/2011	Gerhardt et al.	N/A	N/A
2013/0152185	12/2012	Singh et al.	N/A	N/A
2013/0183936	12/2012	Smtih et al.	N/A	N/A
2013/0194067	12/2012	Kimbrell	N/A	N/A

FOREIGN PATENT DOCUMENTS

Patent No.	Application Date	Country	CPC
2002-183866	12/2001	JP	N/A
2004-102682	12/2003	JP	N/A
2008-227758	12/2007	JP	N/A
2006-285965	12/2008	JP	N/A
2010-086281	12/2009	JP	N/A

OTHER PUBLICATIONS

Apple Inc.'s Invalidity Contentions which were filed in the following litigation: *Maxell, Ltd. v. Apple Inc.*, Civil Action No. 5:19-cv-00036-RWS (E.D. TX), filed Aug. 14, 2019. cited by applicant
Apple Inv. v. Maxell, Ltd., Petition for Inter Partes Review of U.S. Pat. No. 10,212,586, Inter Partes Review No. IPR2020-00202 dated Dec. 19, 2019. cited by applicant
iPhone Technical Specifications, Jul. 4, 2007, Apple Inc. cited by applicant
iPhone User's Guide, Apple Inc., 2007, pp. 1-124. cited by applicant
Elmer-Dewitt, P., "How Many iPhones Did Apple Sell Last Quarter?", *Fortune*, Jan. 14, 2016. cited by applicant
Office Action mailed on Mar. 3, 2015, which issued during the prosecution of Japanese Patent Application No. 2012-117105. cited by applicant
Office Action mailed on Feb. 28, 2017, which issued during the prosecution of Japanese Patent Application No. 2015-241178. cited by applicant
Office Action mailed Jun. 30, 2015, which issued during the prosecution of Japanese Patent Application No. 2012-117105. cited by applicant

Primary Examiner: Huang; Wen W

Attorney, Agent or Firm: Mattingly & Malur, PC

Background/Summary

CROSS REFERENCE TO RELATED APPLICATIONS (1) This application is a continuation of U.S. patent application Ser. No. 17/399,126, filed Aug. 11, 2021 and entitled "MOBILE TERMINAL AND CONTROL METHOD THEREOF", which is a continuation of U.S. patent application Ser. No. 16/115,940, filed Aug. 29, 2018 and entitled "MOBILE TERMINAL AND CONTROL METHOD THEREOF", now U.S. Pat. No. 11,388,593, which is a continuation of U.S. patent application Ser. No. 13/874,535 filed May 1, 2013 and entitled "MOBILE TERMINAL AND CONTROL METHOD THEREOF", now U.S. Pat. No. 10,212,586, which is related to and claims priority from Japanese Application No. JP2012-117105 filed May 23, 2012, each of which is incorporated herein by reference in its entirety and from each of which priority is claimed.

BACKGROUND OF THE INVENTION

(1) The present invention relates to a mobile terminal and a control method thereof.
(2) As a background art of this technical field, JP-A-2004-102682 is disclosed. In its publication, a problem will be described as below. "According to the conventional schemes described above, therefore, the user of the terminal device needs to make a complex action in order to prevent a third party from making unauthorized use of the terminal device. If the user has inadvertently made the password known or lost the terminal device together with the ID card, then it is impossible to reliably prevent unauthorized use of the terminal device by a third party."
(3) A method for solving this problem will be described as below. "There is provided a terminal lock system for verifying that the user of a terminal device is a person with the legitimate right to use the terminal device for thereby protecting the terminal device against unauthorized use by a third party, the terminal lock system comprising a key device and a terminal-associated device. The key device is portable and has a radio communication means for performing short-range wireless communications. The terminal-associated device requests a connection to the key device through the short-range wireless communications, and inhibits the terminal device which is combined with the terminal-associated device from being used if information of the key device which is confirmed

as being connected to the terminal-associated device does not agree with information registered in the terminal-associated device, or if the terminal-associated device is not confirmed as being connected to the key device through the short-range wireless communications.”

SUMMARY OF THE INVENTION

(4) In JP-A-2004-102682, the following advantage will be described. “With the above arrangement, when the user who is carrying the key device moves away from the terminal device combined with the terminal-associated device until the terminal-associated device and the key device are no longer capable of connecting to each other based on a short-range wireless communication technique, the terminal-associated device locks the terminal device against use. The terminal lock system thus authenticates the user without the need for asking the user to make any action, and reliably protects the terminal device against unauthorized use by a third party.”

(5) However, the user needs to always carry the dedicated key device having a communication function when using the terminal device.

(6) In view of the foregoing, it is an object of the present invention to provide a convenient mobile terminal and control method thereof capable of being protected against unauthorized use by a third party without using the dedicated key device.

(7) The object of the present invention can be attained by the following technical proposal: For example, a plurality of mobile terminals are previously registered mutually. When unlocked among them, one mobile terminal communicates with another mobile terminal in a communication range of the short-range wireless communications, unlocks the above another mobile terminal, and when out of the communication range, locks it again.

(8) According to the present invention, for example, when one mobile terminal is unlocked among a plurality of mobile terminals, another mobile terminal can be unlocked.

(9) Other objects, features and advantages of the invention will become apparent from the following description of the embodiments of the invention taken in conjunction with the accompanying drawings.

Description

BRIEF DESCRIPTION OF THE DRAWINGS

(1) FIG. 1 is a block diagram illustrating a configuration of a mobile terminal according to a first embodiment;

(2) FIG. 2 is a flowchart illustrating operations for locking and releasing a mobile terminal 1 according to a first embodiment;

(3) FIG. 3 is a flowchart illustrating operations for locking and releasing a mobile terminal 2 according to a first embodiment;

(4) FIG. 4 is a flowchart illustrating operations for locking and releasing a mobile terminal 1 according to a second embodiment;

(5) FIG. 5 is a flowchart illustrating operations for locking and releasing a mobile terminal 2 according to a second embodiment;

(6) FIG. 6 is a flowchart illustrating operations for locking and releasing a mobile terminal 1 according to a third embodiment;

(7) FIG. 7 is a display example illustrating a liquid crystal panel of a mobile terminal according to a third embodiment;

(8) FIG. 8 is a flowchart illustrating operations for locking and releasing a mobile terminal 1 according to a fourth embodiment;

(9) FIG. 9 is a flowchart illustrating operations for locking and releasing a mobile terminal 1 according to a fifth embodiment; and

(10) FIG. 10 is a flowchart illustrating a warning operation of a mobile terminal 1 according to a

sixth embodiment.

DESCRIPTION OF THE EMBODIMENTS

(11) Hereinafter, preferred embodiments of the present invention will be described with reference to the accompanying drawings of the embodiments.

First Embodiment

(12) FIG. 1 is a block diagram illustrating a configuration of a mobile terminal according to a first embodiment of the present invention. The mobile terminals **1** and **2** each have a radio communication function, and transmit and receive a variety of information to and from a mobile base station **3**. Further, the mobile terminals **1** and **2** each have a function of performing short-range wireless communication between mobile terminals, and can transmit and receive a variety of information between the mobile terminals **1** and **2** by using the function. Examples of the short-range wireless communication include Bluetooth (trademark), infrared rays, and Wi-Fi Direct.

(13) A controller **11** controls each unit of the mobile terminal **1**. The controller **11** is configured by a CPU (Central Processing Unit), an arbitrary control circuit, or a dedicated circuit such as an ASIC.

(14) A display unit **12** of the mobile terminal **1** is configured, for example, by a liquid crystal panel, and displays a variety of information. An operating unit **13** is configured, for example, by a push-button switch or a touch panel, and an instruction of a user is transferred to the controller **11**. A wireless communications unit **15** and a short-range wireless communication unit **16** are each configured by a communication circuit including an encoding circuit and a decoding circuit in addition to an antenna. The wireless communications unit **15** communicates with the mobile base station **3**. The short-range wireless communication unit **16** controls short-range wireless communications and communicates, for example, with the mobile terminal **2**.

(15) A storage unit **14** stores a program or various kinds of setting information for controlling a mobile terminal, and a password for unlocking a mobile terminal.

(16) A controller **21**, a display unit **22**, an operating unit **23**, a storage unit **24**, and a wireless communications unit **25** of the mobile terminal **2** are the same as the controller **11**, the display unit **12**, the operating unit **13**, the storage unit **14**, and the wireless communications unit **15** of the mobile terminal **1**, and therefore, descriptions will not be repeated here. A short-range wireless communication unit **26** controls short-range wireless communications, and communicates, for example, with the mobile terminal **1**.

(17) Next, descriptions will be made about operations which are set until the mobile terminal **2** is unlocked after the mobile terminal **1** is unlocked.

(18) In addition, the locked state of the present embodiment is a state in which functions or operations of part or the whole of a mobile terminal are limited.

(19) When the user refers to the display unit **12** of the mobile terminal **1** and operates the operating unit **13** so as to release a locked state, the mobile terminal **1** searches whether another mobile terminal is in a short-distance communication range capable of performing short-range wireless communications. The mobile terminal **1** further confirms whether it is the mobile terminal **2** being a previously registered mobile terminal. When the mobile terminal **1** confirms that information stored in the storage unit **14** is matched with that of the storage unit **24** and it is the previously registered mobile terminal, the mobile terminal **2** is unlocked.

(20) The mobile terminals **1** and **2** are supposed to transit to a locked state when not operated for a given length of time and, for example, a password is supposed to need to be entered in order to release the locked state. The given length of time is, for example, thirty seconds. Further, the mobile terminals **1** and **2** are previously registered so as to be mutually locked and unlocked through short-range wireless communications.

(21) An example where the mobile terminals **1** and **2** each have a radio communication function with the mobile base station **3** is illustrated. Further, the mobile terminal **1** and/or mobile terminal **2** may each have a wireless LAN (Local Area Network) function, and transmit and receive a variety

of information to and from a wireless LAN router.

(22) FIG. 2 is a flowchart illustrating operations of locking and unlocking the mobile terminal 1 according to the first embodiment.

(23) First, at step S201, the mobile terminal 1 confirms whether to be unlocked when the user enters a password. The mobile terminal 1 continues to wait for unlocking until the locked state is released, and when it is unlocked, the process proceeds to step S202. An example where the user enters a password is described here, and biometrics authentication may be further used.

(24) At step S202, the mobile terminal 1 searches mobile terminals in the neighborhood through short-range wireless communications. For example, the mobile terminal 1 transmits radio waves used for the short-range wireless communications and searches for a mobile terminal in which the short-range wireless communications are established by receiving the radio waves.

(25) At step S203, the mobile terminal 1 determines whether there is a mobile terminal in the neighborhood and it is the previously registered mobile terminal, and switches the process. If so, the process advances to step S204. If not, the process proceeds to step S205.

(26) At step S204, the mobile terminal 1 unlocks the previously registered mobile terminal 2 through the short-range wireless communications. For example, the mobile terminal 1 transmits a signal for instructing the mobile terminal 2 to be unlocked thereto. Here, the mobile terminals 1 and 2 are supposed to be previously registered mutually by the same user.

(27) At step S205, the mobile terminal 1 confirms whether to be instructed to be locked by the user. If so, the process proceeds to step S207. At step S206, the mobile terminal 1 further confirms whether not to be operated for a given length of time. If not, the process proceeds to step S207. If so, the process returns to step S205.

(28) At step S207, the mobile terminal 1 locks the previously registered mobile terminal 2 through the short-range wireless communications. For example, the mobile terminal 1 transmits a signal for instructing the mobile terminal 2 to be locked thereto.

(29) At step S208, the mobile terminal 1 is locked.

(30) FIG. 3 is a flowchart illustrating operations for locking and unlocking the mobile terminal 2 according to the first embodiment.

(31) First, at step S301, the mobile terminal 2 confirms whether to be unlocked when the user enters a password. If so, the process proceeds to step S303. At step S302, the mobile terminal 2 further confirms whether to be unlocked through the short-range wireless communications. If so, the process proceeds to step S305. If not, the process returns to step S301.

(32) At step S303, the mobile terminal 2 confirms whether to be instructed to be locked by the user. If so, the process proceeds to step S307. At step S304, the mobile terminal 2 further confirms whether not to be operated for a given length of time. If not, the process proceeds to step S307. If so, the process returns to step S303.

(33) At step S305, the mobile terminal 2 confirms whether to be out of the communication range of the short-range wireless communications with the mobile terminal 1.

(34) If so, the process proceeds to step S307. At step S306, the mobile terminal 2 further confirms whether to be instructed to be locked by the mobile terminal 1 through the short-range wireless communications. If so, the process proceeds to step S307. If not, the process returns to step S305.

(35) At step S307, the mobile terminal 2 is locked.

(36) In addition, the mobile terminal 1 may detect that the short-range wireless communications established with the mobile terminal 2 is broken, and transmit a signal for instructing the mobile terminal 2 to be locked thereto immediately before the communication is broken.

(37) In the first embodiment of the present invention, a plurality of mobile terminals are previously registered mutually through the above configuration. When one mobile terminal is unlocked among them, another mobile terminal is unlocked in the communication range of the short-range wireless communications. When out of the communication range, the another mobile terminal can be locked again.

(38) In the present embodiment, an example where two mobile terminals are locked and unlocked is described; similarly, three or more mobile terminals can be further locked and unlocked.

Second Embodiment

(39) FIG. 4 is a flowchart illustrating operations for locking and unlocking the mobile terminal 1 according to a second embodiment of the present invention. The mobile terminal has the same configuration as that of the first embodiment, and therefore descriptions will not be repeated here.

(40) First, at step S401, the mobile terminal 1 confirms whether to be unlocked when the user enters a password. If so, the process proceeds to step S403. At step S402, the mobile terminal 1 further confirms whether to be unlocked through the short-range wireless communications. If so, the process proceeds to step S409.

(41) Steps S403 to S408 are the same as steps S202 to S207 of FIG. 2, and therefore descriptions will not be repeated here.

(42) At step S409, the mobile terminal 1 confirms whether to be out of the communication range of the short-range wireless communications with the mobile terminal 2.

(43) If so, the process proceeds to step S411. At step S410, the mobile terminal 1 further confirms whether to be instructed to be locked through the short-range wireless communications. If so, the process proceeds to step S411. If not, the process returns to step S409.

(44) At step S411, the mobile terminal 1 is locked.

(45) FIG. 5 is a flowchart illustrating operations for locking and unlocking the mobile terminal 2 according to the second embodiment.

(46) First, at step S501, the mobile terminal 2 confirms whether to be unlocked when the user enters a password. If so, the process proceeds to step S503. At step S502, the mobile terminal 2 further confirms whether to be unlocked through the short-range wireless communications. If so, the process proceeds to step S509.

(47) Steps S503 and S504 are the same as steps S403 and S404 of FIG. 4, and therefore descriptions will not be repeated here.

(48) At step S505, the mobile terminal 2 unlocks the previously registered mobile terminal 1 through the short-range wireless communications.

(49) At step S506, the mobile terminal 2 confirms whether to be instructed to be locked by the user. If so, the process proceeds to step S508. At step S507, the mobile terminal 2 further confirms whether not to be operated for a given length of time. If not, the process proceeds to step S508.

(50) At step S508, the mobile terminal 2 locks the previously registered mobile terminal 1 through the short-range wireless communications.

(51) At step S509, the mobile terminal 2 confirms whether to be out of the communication range of the short-range wireless communications with the mobile terminal 1. If so, the process proceeds to step S511. At step S510, the mobile terminal 2 further confirms whether to be instructed to be locked through the short-range wireless communications. If so, the process proceeds to step S511. If not, the process returns to step S509.

(52) At step S511, the mobile terminal 2 is locked.

(53) In the second embodiment of the present invention, a plurality of mobile terminals are previously registered mutually through the above configuration. When one mobile terminal is unlocked among them, another mobile terminal is unlocked in the communication range of the short-range wireless communications. When out of the communication range, the another mobile terminal can be locked again.

(54) First, any mobile terminal may be unlocked. Even if any mobile terminal is unlocked, another mobile terminal can be unlocked, and therefore the mobile terminal of the second embodiment is more convenient than that of the first embodiment.

(55) In the present embodiment, an example where two mobile terminals are locked and unlocked is described; similarly, three or more mobile terminals can be further locked and unlocked.

Third Embodiment

(56) FIG. 6 is a flowchart illustrating operations for locking and unlocking the mobile terminal 1 according to a third embodiment of the present invention. The mobile terminal has the same configuration as that of the first embodiment, and therefore descriptions will not be repeated here. (57) Steps S601 to S604 are the same as steps S401 to S404 of FIG. 4, and therefore descriptions will not be repeated here.

(58) At step S605, the mobile terminal 1 displays a confirmation screen in which the mobile terminal 2 is unlocked. A display example will be described later.

(59) At step S606, the mobile terminal 1 confirms whether the user instructs the mobile terminal 2 to be unlocked. If so, the process advances to step S607. If not, the process proceeds to step S608.

(60) Steps S608 to S613 are the same as steps S406 to S411 of FIG. 4, and therefore descriptions will not be repeated here.

(61) FIG. 7 is a display example illustrating a liquid crystal panel of the mobile terminal 1 at the time of detecting the mobile terminal 2 through the short-range wireless communications at step S605 of FIG. 6. A detection report of the mobile terminal 2, a selection button, and non-selection button of the unlocking are displayed on the liquid crystal panel. When detecting the mobile terminal 2 through the short-range wireless communications, the mobile terminal 1 transits to an unlocking selection mode. On the liquid crystal panel 73, an unlocking selection button 74 and an unlocking non-selection button 76 are displayed. When the user pushes a push-button switch 75 corresponding to the unlocking selection button 74, the mobile terminal 2 is unlocked. When the user pushes a push-button switch 77 corresponding to the unlocking non-selection button 76, the mobile terminal 1 releases the unlocking selection mode and returns to a normal mode.

(62) In the third embodiment of the present invention, a plurality of mobile terminals are previously registered mutually through the above configuration. When one mobile terminal is unlocked among them, another mobile terminal is unlocked in the communication range of the short-range wireless communications. When out of the communication range, the another mobile terminal can be locked again.

(63) Further, upon detection of another mobile terminal, the user can select whether to unlock it.

Fourth Embodiment

(64) FIG. 8 is a flowchart illustrating operations for locking and unlocking the mobile terminal 1 according to a fourth embodiment of the present invention. The mobile terminal has the same configuration as that of the first embodiment, and therefore descriptions will not be repeated here.

(65) First, at step S801, the mobile terminal 1 searches mobile terminals in the neighborhood through the short-range wireless communications.

(66) At step S802, the mobile terminal 1 determines whether there is a mobile terminal in the neighborhood and it is the previously registered mobile terminal, and switches the process. If so, the process advances to step S803. If not, the process proceeds to step S805.

(67) At step S803, the mobile terminal 1 requests the user to enter a simple password, and continues to wait until it is correctly entered at step S804. When the simple password is entered, the process proceeds to step S807.

(68) At step S805, the mobile terminal 1 requests the user to enter a complicated password, and continues to wait until it is correctly entered at step S806. When the complicated password is entered, the process proceeds to step S807.

(69) The simple password is, for example, a three-character number, and the complicated password is, for example, a ten-character number. That is, strengths of both passwords are different from each other.

(70) At step S807, the mobile terminal 1 is unlocked. Here, the mobile terminals 1 and 2 are supposed to be previously registered mutually by the same user.

(71) At step S808, the mobile terminal 1 confirms whether to be instructed to be locked by the user. If so, the process proceeds to step S810. At step S809, the mobile terminal 1 further confirms whether not to be operated for a given length of time. If not, the process proceeds to step S810.

(72) At step **S810**, the mobile terminal **1** is locked.

(73) Operations for locking and unlocking the mobile terminal **2** are the same as those of the mobile terminal **1**.

(74) In the fourth embodiment of the present invention, a plurality of mobile terminals are previously registered mutually through the above configuration. When both mobile terminals are in the communication range of the short-range wireless communications, an authentication level for unlocking the mobile terminal is simplified. When both the mobile terminals are out of the communication range of the short-range wireless communications, an authentication level for unlocking the mobile terminal is detailed. Therefore, as compared to a case of simply fixing the authentication level, safety is high. On the other hand, as compared to a case of fixing the authentication level in detail, usability is preferable.

(75) In the present embodiment, an example where the number of characters of the password is changed is described as switching of the authentication level. Further, there may be changed a principal matching rate of biometrics authentication such as face and finger authentication types, or a character matching rate of character authentication.

(76) In the present embodiment, an example where two mobile terminals are locked and unlocked is described; similarly, three or more mobile terminals can be further locked and unlocked.

Fifth Embodiment

(77) FIG. **9** is a flowchart illustrating operations for locking and unlocking the mobile terminal **1** according to a fifth embodiment of the present invention. The mobile terminal has the same configuration as that of the first embodiment, and therefore descriptions will not be repeated here.

(78) First, at step **S901**, the mobile terminal **1** searches mobile terminals in the neighborhood through the short-range wireless communications.

(79) At step **S902**, the mobile terminal **1** determines whether there is a mobile terminal in the neighborhood and it is the previously registered mobile terminal, and switches the process. If so, the process proceeds to step **S903**. If not, the process returns to step **S901**.

(80) At step **S903**, the mobile terminal **1** is unlocked. Here, the mobile terminals **1** and **2** are supposed to be previously registered mutually by the same user.

(81) At step **S904**, the mobile terminal **1** confirms whether to be out of the communication range of the short-range wireless communications with the mobile terminal **2**. The mobile terminal **1** continues to wait until out of the communication range. When the mobile terminal **1** is out of the communication range, the process proceeds to step **S905**.

(82) At step **S905**, the mobile terminal **1** is locked.

(83) Operations for locking and unlocking the mobile terminal **2** are the same as those of the mobile terminal **1**.

(84) In the fifth embodiment of the present invention, a plurality of mobile terminals are previously registered mutually through the above configuration. When in the communication range of the short-range wireless communications, they are mutually unlocked. When out of the communication range, they are locked again. Therefore, the mobile terminal of the present embodiment is more convenient than those of the first and second embodiments.

(85) In the present embodiment, an example where two mobile terminals are locked and unlocked is described; similarly, three or more mobile terminals can be further locked and unlocked.

Sixth Embodiment

(86) FIG. **10** is a flowchart illustrating a warning operation of the mobile terminal **1** according to a sixth embodiment of the present invention. The mobile terminal has the same configuration as that of the first embodiment, and therefore descriptions will not be repeated here.

(87) First, at step **S1001**, the mobile terminal **1** searches mobile terminals in the neighborhood through the short-range wireless communications.

(88) At step **S1002**, the mobile terminal **1** determines whether there is a mobile terminal in the neighborhood and it is the previously registered mobile terminal, and switches the process. If so,

the process proceeds to step S1003. If not, the process returns to step S1001.

(89) At step S1003, the mobile terminal 1 confirms whether to be out of the communication range of the short-range wireless communications with the mobile terminal 2.

(90) If so, the process proceeds to step S1004. If not, the process returns to step S1003.

(91) At step S1004, the mobile terminal 1 gives warning to the user through sounds or vibrations. Alternatively, the mobile terminal 1 sends a mail to another mobile terminal. At this time, when having a GPS (Global Position System) function, the mobile terminal I may transmit positional information to the another mobile terminal.

(92) The warning operation of the mobile terminal 2 is the same as that of the mobile terminal 1.

(93) In the sixth embodiment of the present invention, a plurality of mobile terminals are previously registered mutually through the above configuration. In the case where they are once in the communication range of the short-range wireless communications, upon being out of the communication range next, the mobile terminal I notifies the user of that effect, thereby preventing the mobile terminals from being lost.

(94) Suppose, for example, that the present embodiment is combined with the first embodiment. In this case, the mobile terminal 2 can notify the user that the mobile terminal 2 is locked because of moving to the outside of the communication range of the short-range wireless communications with the mobile terminal 1.

(95) In the present embodiment, an example where two mobile terminals perform a warning operation is described; similarly, three or more mobile terminals can further perform a warning operation.

(96) In addition, the above-described embodiments are described in detail in order to clearly describe the present invention, and are not necessarily limited to the mobile terminal having all the described constructions. Further, a part of configurations according to one embodiment can be replaced by those according to other embodiments, and the configurations according to other embodiments can be added to that according to one embodiment. Further, an addition, deletion, or replacement of the configurations according to other embodiments can be performed by using a part of the configurations according to each embodiment.

(97) A part or all of the respective structures, functions, processing units, and processing approaches may be realized by hardware by designing through the integrated circuit, for example. Those structures, functions and the like may be realized by software by interpreting and executing the program for realizing the respective functions through a processor. Information with respect to the program, table, and file for realizing the respective functions may be stored in the recording unit such as the memory, hard disk, and SSD (Solid State Drive), or the recording medium such as the IC card and SD card.

(98) The examples show the control line and information line considered as necessary for the explanation, which does not necessarily show all the control lines and information lines of the product. Actually, almost all the components may be considered to be connected with one another.

(99) It should be further understood by those skilled in the art that although the foregoing description has been made on embodiments of the invention, the invention is not limited thereto and various changes and modifications may be made without departing from the spirit of the invention and the scope of the appended claims.

Claims

1. A mobile terminal configured to switch between a locked state and an unlocked state in which unauthorized access of the mobile terminal is prevented, comprising: a wireless LAN communication circuit transmitting and receiving information to and from a wireless router; a wireless communication circuit transmitting and receiving information to and from a base station; a memory for storing a password corresponding to the mobile terminal and information about

another mobile terminal; a Bluetooth transceiver which performs short-range wireless communications; a processor controlling the Bluetooth transceiver to search for the another mobile terminal and determine whether the another mobile terminal is within range to conduct short-range wireless communications with the Bluetooth transceiver, wherein the Bluetooth transceiver performs short-range wireless communications with the another mobile terminal when the another mobile terminal is determined to be within range and when information about the another mobile terminal is stored in memory; and a display displaying: first information to indicate that the another mobile terminal is within range based on the determination; second information corresponding to an unlock operation when the mobile terminal is in the locked state; and a GPS for determining a location of the mobile terminal, wherein the processor is configured to: switch the mobile terminal from the unlocked state to the locked state when the mobile terminal is not used for a predetermined period of time; switch the mobile terminal from the lock state to the unlocked state when it receives input of a password by a user and the inputted password matches the stored password; perform biometric authentication to authenticate the user based on a face match operation and switch the mobile terminal from the lock state to the unlocked state when the biometric authentication is performed; and perform a warning operation such that a warning message and the position information of the mobile terminal is transmitted to second another mobile terminal during the warning operation, and wherein the wireless LAN communication circuit is further configured to transmit and receive information to and from the another mobile terminal in Wi-Fi Direct communication mode.

2. The mobile terminal according to claim 1, wherein the mobile terminal and the another mobile terminal are mutually registered to the same user.

3. The mobile terminal according to claim 1, wherein the wireless LAN communication circuit communicates the location of the mobile terminal to another mobile terminal.

4. The mobile terminal according to claim 1, further comprising an infrared ray component.

5. The mobile terminal according to claim 1, wherein the wireless LAN communication circuit performs Wi-Fi Direct communication with the another mobile terminal.

6. The mobile terminal according to claim 1, wherein the mobile terminal and the another mobile terminal are mutually locked.

7. The mobile terminal according to claim 1, wherein the mobile terminal and the another mobile terminal are mutually unlocked.

8. The mobile terminal according to claim 1, wherein the wireless communication circuit communicates the location of the mobile terminal to another mobile terminal.

9. A system of mobile terminals in communication with each other, comprising: a first mobile terminal having: a first wireless LAN communication circuit transmitting and receiving information to and from a wireless router; a first wireless communication circuit transmitting and receiving information to and from a base station; a first memory for storing a first password corresponding to the first mobile terminal and information about a second mobile terminal; a first Bluetooth transceiver which performs short-range wireless communications; a GPS for determining a location of the first mobile terminal; a first display displaying information corresponding to an unlock operation when the first mobile terminal is in a locked state; and a first processor; and a second mobile terminal having: a second wireless LAN communication circuit transmitting and receiving information to and from a wireless router; a second wireless communication circuit transmitting and receiving information to and from a base station; a second memory for storing a second password corresponding to the second mobile terminal and information about the first mobile terminal; a second Bluetooth transceiver which performs short-range wireless communications; a second display displaying information corresponding to an unlock operation when the second mobile terminal is in a locked state; and a second processor, wherein the first processor controls the first Bluetooth transceiver to search for the second mobile terminal and determine whether the second mobile terminal is within range to conduct short-range wireless

communications between the first Bluetooth transceiver and the second Bluetooth transceiver, wherein the first display displays information to indicate that the second mobile terminal is within range based on the determination, wherein the Bluetooth transceiver performs short-range wireless communications with the second mobile terminal when the second mobile terminal is determined to be within range and when information about the second mobile terminal is stored in the first memory, wherein the first processor is configured to: switch the first mobile terminal from the unlocked state to the locked state when the first mobile terminal is not used for a predetermined period of time; switch the first mobile terminal from the locked state to the unlocked state when it receives input of a password by a user and the inputted password matches the first password; and perform biometric authentication to authenticate the user based on a face match operation and switch the first mobile terminal from the lock state to the unlocked state when the biometric authentication is performed, wherein the second processor controls the second Bluetooth transceiver to search for the first mobile terminal and determine whether the first mobile terminal is within range to conduct short-range wireless communications between the second Bluetooth transceiver and the first Bluetooth transceiver, wherein the second display displays information to indicate that the first mobile terminal is within range based on the determination, and wherein the second Bluetooth transceiver performs short-range wireless communications with the first mobile terminal when the first mobile terminal is determined to be within range and when information about the first mobile terminal is stored in the second memory, and wherein the second processor is configured to: switch the second mobile terminal from the unlocked state to the locked state when the second mobile terminal is not used for a predetermined period of time; switch the second mobile terminal from the locked state to the unlocked state when it receives input of a password by a user and the inputted password matches the second password; perform biometric authentication to authenticate the user based on a face match operation and switch the second mobile terminal from the lock state to the unlocked state when the biometric authentication is performed; perform a warning operation such that a warning message and the position information of the mobile terminal is transmitted to second another mobile terminal during the warning operation, and wherein the wireless LAN communication circuit is further configured to transmit and receive information to and from the first another mobile terminal in Wi-Fi Direct communication mode.

10. The system according to claim 9, wherein the first mobile terminal and the second mobile terminal are mutually registered to the same user.

11. The system according to claim 9, wherein the first wireless LAN communication circuit communicates the location of the first mobile terminal to the second mobile terminal.

12. The system according to claim 9, wherein the first mobile terminal further comprises an infrared ray component.

13. The system according to claim 9, wherein the first wireless LAN communication circuit performs Wi-Fi Direct communication with the second wireless LAN communication circuit.

14. The system according to claim 9, wherein the first mobile terminal and the second mobile terminal are mutually locked.

15. The system according to claim 9, wherein the first mobile terminal and the second mobile terminal are mutually unlocked.

16. The system according to claim 9, wherein the first wireless communication circuit communicates the location of the first mobile terminal to the second mobile terminal.

17. The system according to claim 9, wherein the first mobile terminal includes a push-button switch such that the first mobile terminal switches mode of operation when a user presses the push-button switch.

18. The system according to claim 9, wherein the second mobile terminal includes a push-button switch such that the second mobile terminal switches mode of operation when a user presses the push-button switch.

19. The system according to claim 9, wherein the first display displays a warning when the second

mobile terminal is determined to be out of range.

20. A method to switch a mobile terminal between a locked state and an unlocked state in which unauthorized access of the mobile terminal is prevented, comprising: transmitting and receiving information to and from a wireless router by performing wireless LAN communications; transmitting and receiving information to and from a base station by performing wireless communications; storing a password corresponding to the mobile terminal and information about another mobile terminal; performing Bluetooth short-range wireless communications; controlling the Bluetooth transceiver to search for the another mobile terminal and determine whether the another mobile terminal is within range to conduct Bluetooth short-range wireless communications, wherein the Bluetooth short-range wireless communications are performed with the another mobile terminal when the another mobile terminal is determined to be within range and when information about the another mobile terminal is stored in the memory; displaying, based on the determination, first information to indicate that the another mobile terminal is within range; displaying second information corresponding to an unlock operation when the mobile terminal is in the locked state; determining a location of the mobile terminal via GPS; switching the mobile terminal from the unlocked state to the locked state when the mobile terminal is not used for a predetermined period of time; switching the mobile terminal from the locked state to the unlocked state when it receives input of a password by a user and the inputted password matches the stored password; performing biometric authentication to authenticate the user based on a face match operation; switching the mobile terminal from the lock state to the unlocked state when the biometric authentication is performed; and performing a warning operation such that a warning message and the position information of the mobile terminal is transmitted to second another mobile terminal during the warning operation, and wherein the wireless LAN communication circuit performs transmitting and receiving information to and from the another mobile terminal in Wi-Fi Direct communication mode.
