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

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
20 August 2009 (20.08.2009)

PCT

(10) International Publication Number
WO 2009/102279 A1

(51) International Patent Classification:
G06F 21/22 (2006.01) *H04L 9/32* (2006.01)

(21) International Application Number:
PCT/SG2008/000052

(22) International Filing Date:
13 February 2008 (13.02.2008)

(25) Filing Language: English

(26) Publication Language: English

(71) Applicant *(for all designated States except US)*: **TERNARY TECHNOLOGIES PTE LTD** [SG/SG]; 8 Shenton Way, #37-01 Temasek Tower, Singapore 068811 (SG).

(72) Inventor; and

(75) Inventor/Applicant *(for US only)*: **CHNG, Weng Wah** [SG/SG]; 33 Ford Avenue, Singapore 268713 (SG).

(74) Agent: **LAWRENCE Y D HO & ASSOCIATES PTE LTD**; 30 Bideford Road, #02-02, Thongsia Building, Singapore 229922 (SG).

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

(84) Designated States *(unless otherwise indicated, for every kind of regional protection available)*: ARIPO (BW, GH, GM, KE, LS, MW, MZ, NA, SD, SL, SZ, TZ, UG, ZM, ZW), Eurasian (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European (AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HR, HU, IE, IS, IT, LT, LU, LV, MC, MT, NL, NO, PL, PT, RO, SE, SI, SK, TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG).

Published:

— *with international search report (Art. 21(3))*

WO 2009/102279 A1

(54) Title: THEFT-DETERRENT SYSTEM AND METHOD

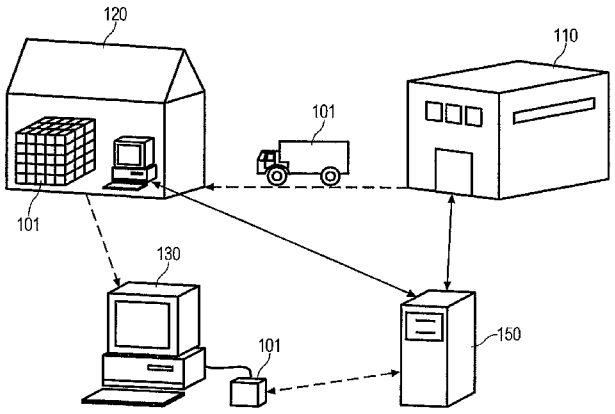

FIG. 1

(57) Abstract: The present invention provides a theft deterrent system and method that minimizes or eliminates the loss of products due to theft. The system and method is suitable for products such as electronic devices. The system and method, by default, disabling all functionalities of the products, which would render the products useless and worthless, unless it is unlocked.

THEFT-DETERRENT SYSTEM AND METHOD

Field of the Invention

[0001] The present invention relates to a theft-deterrent system and method. In particular, the invention relates to a theft-deterrent system and method suitable for electronic devices having non-volatile memory.

Background

[0002] Shoplifting and pilfering contribute significant losses for businesses. Such loss is magnified when the items for sale are high priced and miniature such as electronic devices theft of such items escape detection easily. There are many attempts at developing mechanisms and apparatuses to deter theft at retailers and department stores.

[0003] Surveillance system has been widely used for monitoring a premise for security. In a retail outlet, such system is mainly used for preventing shoplifting. For large premises, lots of CCTV cameras are required to cover as many areas as possible. Most of these surveillance systems are monitored by human operations. Such system is only effective for areas where they can be seen and monitored at all time.

[0004] One common way of deterring theft include affixing a RFID tag on the product and installing RFID scanner at all the exit of the premises. When the RFID scanner senses an active RFID (with the product) is brought out from the premises, the RFID scanner sounds an alarm. However, this method does not fully prevent theft as the RFID tag can still be detached from the product. Further, a premise with more than one exit requires more RFID scanner to be installed thereto. Such system is also not suitable for an open area, such as a product fair.

[0005] Some higher value and small size product are often kept behind a counter or packaged with a sealed packaging but viewing and browsing becomes difficult and hazardous to open. This approach is not customer-friendly, which may result in decrease in sales.

Summary

[0006] In accordance with one aspect of the present invention, there is provided a theft deterrent system for a device having a device controller for managing and controlling the function of device, the theft deterrent system comprises a software code for residing in the device controller, the software code being adapted to deny access functionalities of the device by default, the software code being executable at a first use of the device to prompt for unlocking the device; and a server for generating and managing an unlock code for unlocking the software code of the device to allow access functionalities of the device, wherein the server generates and provides the unlock code to a manufacturer of the device, the unlock code is further provided upon payment for the product at a point of sale for unlocking the device.

[0007] In accordance with one embodiment of the present invention, the unlock code may be provided in a printed form at the point of sale.

[0008] In accordance with another embodiment of the present invention, the software code may be executed to prompt for unlocking the device when the device is connected to an unlock device for a first time. It is possible that the unlock code is inputted to unlock the device via the unlock device or the unlock code can be inputted to the device directly.

[0009] In yet another embodiment, the server may be connected to the manufacturer via a communication network.

[0010] In yet another embodiment, the point of sale may acquire the unlock code from the server via a communication network.

[0011] In accordance with another aspect of the present invention, there is provided a device with a theft deterrent feature provided therein, said device having a controller for managing and controlling the function of device, the device comprises a software code residing in the firmware, the software code being adapted to deny access functionalities of the product by default, the software code being executed at a first use of the product to prompt for unlocking the product; wherein the software code requires an unlock code to unlock the device to allow access functionalities of the device, said unlock code is provided upon purchase.

[0012] In accordance with one embodiment, the controller may include a firmware. The software code may be executed when the device is connected to an unlock device for a first time. It is possible that the unlock device is a general personal computer, a dedicated standalone device or a remote server. Yet, the product may be connected to the unlock device via an USB interface or an I/O interface. The product may be connected to the unlock device via a reader device.

[0013] In yet another embodiment, the unlock code may be generated by a server connected to a manufacturer of the product, the unlock code may be stored on the server and provided to a retailer of the product. The unlock code for the product may be printed out upon purchase at the retailer for unlocking the product.

[0014] In yet another aspect of the present invention, there is provided a method for deterring theft for products having a device firmware for managing and controlling the product to function, said method comprises embedding a software code in the device firmware, the software code being adapted to deny access functionalities of the device by default; generating an unlock code for unlocking the software code

from a server; identifying the device at a point of sale; acquiring the unlock code from the server based on the identified device; providing the unlock code at the point of sale; and inputting the unlock code to unlock the software code to allow access functionalities of the device.

[0015] In one embodiment, the method may further comprise printing the unlock code at the point of sale.

[0016] In another embodiment, the method may further comprise executing the software code to prompt for the unlock code at the first use of the device.

[0017] In yet another embodiment, the method may further comprise connecting the device to an unlock device to activate the software code to prompt for the unlock code.

[0018] In accordance with the above embodiment, the unlock code may be inputted via the unlock device. It is also possible that the unlock code generated by the server is sent to a manufacturer for manufacturing the device.

Brief Description of the Drawings

[0019] This invention will be described by way of non-limiting embodiments of the present invention, with reference to the accompanying drawings, in which:

[0020] **FIG. 1** illustrates a block diagram of theft-deterrent system in accordance with one embodiment of the present invention;

[0021] **FIG. 2A** is a schematic diagram showing an unlocking device and a product to be unlocked in accordance with another embodiment of the present invention;

[0022] **FIG. 2B** exemplifies a clock diagram of typical camera having a theft deterrent system embedded therein in accordance with one embodiment of the present invention;

[0023] **FIG. 3** illustrates a flow diagram showing a purchase flow in accordance with one embodiment of the present invention;

[0024] **FIG. 4** illustrates a flow diagram for generating an unlock code in accordance with one embodiment of the present invention;

[0025] **FIG. 5** exemplifies a standalone unlock device in accordance with one embodiment of the present invention.

Detailed Description

[0026] In line with the above summary, the following description of a number of specific and alternative embodiments are provided to understand the inventive functions of the present invention. It shall be apparent to one skilled in the art, however that this invention may be practised without such specific details. Some of the details may not be described at length so as not to obscure the invention. For ease of reference, common reference numerals will be used throughout the figures when referring to the same or similar functions common to the figures.

[0027] **FIG. 1** illustrates a block diagram of a supply chain network having a theft-deterrent system in accordance with one embodiment of the present invention. The theft deterrent system provides a theft-deterrent function that helps to discourage stealing of products **101**. The products **101** are electronic devices. The products **101** are manufactured at a manufacturer **110**. The products **101** are distributed to distributors or retailers **120** for sale. These products **101** are generally arranged on shelves/showcases or hung on racks for displaying. These products **101** when displaying on the shelves/showcases or racks are susceptible to theft, even if they are monitored by a surveillance system. That is more so for small size products **101** that can easily be hidden in pockets without drawing attention from others. Therefore, the theft-deterrent function is embedded in all the products **101** to deter theft activities by disabling the functionalities of the products **101** by default. A one-time authentication is required to restore/enable the functionalities of the products **101** at its first used. Even when the products **101** are stolen, the theft-deterrent function renders the products **101** unusable.

[0028] Still referring to **FIG. 1,** the theft-deterrent function is in a form of software code residing in the products **101** at the time of manufacturing at the manufacturer **110**. The software code is adapted to denial access to the

functionality/usability of the products **101** by default. The soft code is self-executed at first use of the products **101** to prompt for unlocking code. Disabling the theft-deterrent function to enable/restore the functionalities of the products **101** is done by inputting a valid unlock code. The unlock code is unique to every products **101** and it is generated by a server **150**. When the products **101** are distributed to the distributors or retailers **120**, the distributors or retailers **120** are required to connect to the server **150** to obtain the unlock codes for each of the products **101**. These unlock codes can be stored securely at the distributors' or retailers' **120** computer/server, or stored on the server 150 and provided to the distributors or retailers upon request. The unlock codes are provided to the consumer who purchased the product **101** upon payment. The consumer has to unlock the product **101** to restore the functionalities of the products **101** when the product **101** is connected to a personal computer (PC) **130**. The PC **130** can be any home PC or any general purpose computer. The product **101** can be connected to the PC **130** via a cable, or through an intermediate device, such as a memory card reader. When the product **101** is first connected to the PC **130**, the theft-deterrent function is self-executed to prompt for the unlock code. The product **101** is unlocked when the valid unlock code is provided, and the consumer can then use the product **101** as usual.

[0029] Still referring to **FIG. 1,** the products **101** are being locked before shipment at the manufacturer **110**. Therefore, even when the products **101** are being stolen on the way to the distributors/retailers **120**, or any point before purchasing by consumers, the product **101** is deemed useless without a corresponding unlock code to unlock them. The unlock codes are generated by the server **150**. The server **150** is located at the manufacturer **110**. During the manufacturing of the products **101**, the unlock codes are generated and coded into the products **101**.

[0030] In accordance with an alternative embodiment, the server **150** of **FIG. 1** is provided by an unlock code provider located remotely from the manufacturers and

the retailers. The unlock code provider is a key management system where the manufacturers' and the retailers' servers are connected thereto to obtain the unlock codes. During the manufacturing process, the manufacturers acquire the unlock codes from the server **150**. The unlock codes are generated and sent to the manufacturers and a copy of unlock codes are indexed and stored at the server **150**. At the retailers' side, the unlock codes correspond to the products **101** are retrieved from the server **150** via a communication network, such as Internet. The retrieval of an unlock code from the server **150** is done at the point of sale. It can also be sent to the retailers' server when the products **101** are stocked, and retrieve from the retailers' server at the point of sale. Upon purchase of the products 101, the unlock code provider is updated to indicate that the product is legitimately purchased.

[0031] In accordance with yet another alternative embodiment, the unlock code provider may provide services that manage the unlock keys for each product registered therewith. When the unlock keys are sent to the manufacturers, in return, the manufacturers revert with a corresponding product serial number for indexing. When the key is required after a purchase, the server **150** retrieve the corresponding key and printed a copy of the key for unlocking the product. Thereby, when the purchased product **101** is connected to a PC for the first time, the unlock code required to key-in on the PC to unlock the product **101** is provided.

[0032] In accordance with yet another embodiment, the product **101** is unlocked automatically when it is connected to relevant unlock code provider via a communication network. When the product is purchased, the point of sale connecting to the communication network updates the relevant unlock code provider of the purchase. Once the relevant unlock code provider verifies that the product is purchased legitimately, the relevant unlock code provider will send the unlock code to the product automatically to unlock the product when the product is connected to the unlock code provider via the communication network. Depending on the type of product, it may be

connected to different communication networks via different communication channels. The communication networks include cellular network providers, Internet service providers, the manufacturer website, and others. For example, a mobile phone device can connect to a cellular network provider via GSM, GPRS, CDMA, EDGE, 3GSM, GPS and etc. In another example, a camera product is required to connect to the communication network via a computer connecting the Internet. When the camera is first connected to the computer, the theft-deterrent function is self-executed to connect to the unlock key provider via the Internet, and when the camera product is verified legitimate, the unlock key provider sends a corresponding unlock code to unlock the camera product.

[0033] **FIG. 2A** illustrates a schematic diagram of internal interfaces of the product **101** of **FIG. 1** in accordance with one embodiment of the present invention. The product **101** is adapted to connect to an unlocking device **230** via an I/O interfaces **250**. The product **101** comprises a firmware **220** and functional means **210**. The firmware **220** initializes the product **101** to operate the basic operations of the functional means **210**. The firmware **220** includes a theft deterrent function to disable/denial access to all the functionalities of the functional means **210** by default. When the product **101** is first connected to the unlocking device **230**, the theft deterrent function prompts to enter a unlock code. When the theft deterrent function verifies that the unlock code is valid, the functional means **210** are unlocked permanently. Depending on the type of the product, different products may have different functional means **210**. For example, the functional means of a memory card is a flash memory. In another example, the functional means of a digital camera include image capturing and storage means, image-viewing screen, image processor, etc. In yet another example, the functional means of a mobile phone device include a voice encoder and decoder, a still and/or video camera, a radio receiver, a Bluetooth module and etc, just to name a few.

[0034] **FIG. 2B** exemplifies a block diagram of typical camera **250** having a theft deterrent system embedded therein in accordance with one embodiment, of the present invention. The camera **250** include a camera firmware **251**, a processor **252**, an I/O interface **253**, a power supply **254**, a display driver **255** for controlling a LCD display, a memory controller **256**, a sensor **257** and others functional means. The theft deterrent function of the theft deterrent system is embedded in the camera firmware **251**. When the camera is first powered up, the camera firmware **251** is loaded up to initiate the camera **250** as well as the theft deterrent function. A message can be shown on the LCD display to unlock the camera by connecting the camera **250** to a computer via the I/O interface **253**. When the camera is connected to the computer, the theft deterrent function is activated to connect to an unlock server. If the camera is verified to be legitimate purchased product, the unlock server sends a unlock code to unlock the camera, thereby enabling all the functional means.

[0035] It is understood that **FIGs. 2A** and **2B** is provided by way of example merely, and not intend to limit scope of the present invention. Depending on type of the product, the theft deterrent function can also be stored in a device ROM or embedded in a controller or device driver where the device is required to execute upon first use.

[0036] **FIG. 3** illustrates a purchase flow of the product **101** of **FIG. 1** in accordance with one embodiment of the present invention. The product **101** is provided with the theft-deterrent function described above. In the purchase flow, a consumer picks a product **101** and brings it to a checkout counter for payment in step **302**. At the point of sale, a casher of the checkout counter identifies the product **101** and retrieves a price of the product **101**. A barcode scanner can be used to identify the product **101**. When the product **101** is identified, an unlock code is provided to the consumer in step **306**. The unlock code is generally provided on a printed slip or other

similar means. The consumer unlocks the product **101** with the unlock code in step **308**.

[0037] Still referring to **FIG. 3,** in step **306**, the unlock code can be obtained from a pre-stored database, or generated by an unlock code generator. The pre-stored database can further be a local database or a remote database. In the case of a local database, all the unlock codes for each products are pre-generated on a server and provided to the retailer upon or after products delivery. In a case of the remote database, each unlock code can be obtained upon request either by the retailers or the buyers themselves from the manufacturer through a communication network, such as the Internet. For unlock codes that are generated instantaneously, it can either be generated locally or remotely. In the former case, the unlock code generator is provided locally and the code is generated based on a pre-defined algorithm. In the latter case, the unlock code generator is provided remotely, such as at the server **150** of **FIG. 1,** and is retrieved upon request either by the retailers or the consumers themselves from the server **150** through a communication network, such as the Internet.

[0038] In step **308** of **FIG. 3,** depending on the type of products, there may be various ways to unlock the products. In one embodiment, the unlock code can be keyed into the product by means of keypads. This embodiment is suitable for products that comprise keypads and a display, such as mobile phones, game consoles, personal data assistant, and the like. The keypads can be physical keypads or soft keypads, and the display can be a normal display or a touch screen type display. In another embodiment, the unlock code can be keyed through product registration through a communication network, such as the Internet while the products are connected to a PC. In this embodiment, the server **150** may require to be updated upon the purchase of the product **101**. Accordingly, if the product is verified to be not a legitimate purchased product, the server **150** will not provide an unlock key to unlock the product **101**. The products include SIM cards, software products, or PC hardware. In yet another

embodiment, for products that has a wireless receiver, such as global positioning system (GPS) receiver, the unlocking codes can be downloaded to the device wirelessly and automatically at the initial power up once the product serial number is identified to be valid. The methods of unlocking the products in said embodiments are provided herewith by way of example only, and intend to not limit the scope of the present invention. It is understood that other unlock methods may be desired depending on the nature and design of the products.

[0039] **FIG. 4** is a flow chart illustrating a process of generating an unlock code in accordance with one embodiment of the present invention. In step **410**, the product **101** serial number is inputted into an automated system. The product **101** serial number can be inputted by way of scanning the product **101** bar code or inputting manually. Based on the product serial number, the automated system connects to a server via a communication network, such as the Internet, in step **430**. The server may be located at the corresponding manufacturer's site, or it can be a server of an unlock code provider. In step **430**, the server checks if the product serial number is valid. When an invalid serial number is detected, a warning message shall be displayed, in step **435**. The invalid serial number shall signify that the product is a reported lost product, or a rejected product, therefore no unlock code is provided. All the functions of the product shall cease to function without the unlock code. Back to step **430**, when the product serial number is identified to be valid, the server provides an unlock code in step **440**. The unlock code may be pre-generated for matching with the product serial number, or it can be generated by a unlock code generator of the server. The automated system received the unlock code from the server in step **450**, and the code is printed for the consumer in step **460**.

[0040] **FIG. 5** illustrates a dedicated standalone unlock device **500** in accordance with one embodiment of the present invention. The unlock device **500** is adapted to connect with a product **501** to unlock the same. It is mainly required when a

consumer purchases the product **501** required to unlock the product **501** immediately after the purchase without a PC. The unlock device **500** comprises a display **510**, a input **520** and a plurality of I/O interfaces **530**. The display **510** is an alphanumeric display for displaying input and output information such s a liquid crystal display. The input **520** is a keypad for inputting the unlock code. The I/O interfaces **530** include a multi-card format reader/writer, an USB connector, a FireWire connector and the like. The I/O interfaces allow any product **501** to be connected to the unlock device **500** to unlock the product. When the product **501** is unpacked and connected to the unlock device **500**, the theft-deterrent function embedded in the product **501** triggers the unlock device **500** to prompt for an unlock code on the display **510**. The consumer inputs the unlock code that is provided upon purchase into the unlock device **500** via the input **520**. The unlock device **500** unlocks the product **501** when the unlock code is correctly inputted.

[0041] In an alternative embodiment, a kiosk may be provided at the retailers in placed of the stand alone device. The kiosk may provide a computer for connecting to the communication network. When a product is purchased, the consumer may bring the product to the kiosk and connect it thereto to unlock the product.

[0042] Still referring to **FIG. 5,** the unlock device **500** can further connect to a dedicated server **503** via the Internet to unlock the product **501**. When the product is connected to the unlock device **500** and the unlock code is inputted to the unlock device **500** via the input **520**, the product information, such as the product serial number, and the unlock code are sent to the dedicated server **503** to validate the unlock code. If validation is successful, the product **501** is unlocked.

[0043] Unlocking of the product is required at the first time when the product is used. Once the unlock code is accepted and the product is unlocked, subsequently, the product shall perform its regular function without the need to input the unlock code.

[0044] In yet another embodiment, the unlock code is kept with the manufacturer **110**. The consumers purchase the products **101** are required to contact the manufacturer **110** to obtain the unlock code. The contact can be through a phone call or via internet. In order to obtain the unlock code, the serial number of the products **101** is required for identification. When the serial number are identified as stolen products, the unlock code will not be provided.

[0045] With the present invention, theft activities are deterred as the product cannot be used unless they are unlocked. The present invention also provides a centralized server for generating and managing unlock codes.

[0046] While specific embodiments have been described and illustrated, it is understood that many changes, modifications, variations and combinations thereof could be made to the present invention without departing from the scope of the invention.

Claims

1. A theft deterrent system for a device having a device firmware for managing and controlling the function of device, the theft deterrent system comprising:

a software code for residing in the device firmware, the software code being adapted to deny access functionalities of the device by default, the software code being executable at a first use of the device to prompt for unlocking the device; and

a server for generating and managing an unlock code for unlocking the software code of the device to allow access functionalities of the device,

wherein the server generates and provides the unlock code to a manufacturer of the device, the unlock code is further provided upon payment for the product at a point of sale for unlocking the device.

2. The theft deterrent system according to claim 1, wherein the unlock code is provided in a printed form at the point of sale.

3. The theft deterrent system according to claim 1, wherein the software code is executed to prompt for unlocking the device when the device is connected to an unlock device for a first time.

4. The theft deterrent system according to claim 3, wherein the unlock code is inputted to unlock the device via the unlock device.

5. The theft deterrent system according to claim 1, wherein the unlock code is inputted to the device directly.

6. The theft deterrent system according to claim 1, wherein the server is connected to the manufacturer via a communication network.

7. The theft deterrent system according to claim 1, wherein the point of sale acquires the unlock code from the server via a communication network.

8. A device with a theft deterrent feature provided therein, said device having a firmware for managing and controlling the function of device, the device comprising:

a software code residing in the firmware, the software code being adapted to deny access functionalities of the product by default, the software code being executed at a first use of the product to prompt for unlocking the product;

wherein the software code requires an unlock code to unlock the device to allow access functionalities of the device, said unlock code is provided upon purchase.

9. The device according to claim 8, wherein the software code is executed when the device is connected to an unlock device for a first time.

10. The device according to claim 9, wherein the unlock device is a general personal computer.

11. The device according to claim 9, wherein the unlock device is a dedicated standalone device.

12. The device according to claim 9, wherein the product is connected to the unlock device via an USB interface.

13. The device according to claim 9, wherein the product is connected to the unlock device via an I/O interface.

14. The device according to claim 10, wherein the product is connected to the unlock device via a reader device.

15. The device according to claim 1, wherein the unlock code is generated by a server connected to a manufacturer of the product, the unlock code is stored on the server and provided to a retailer of the product.

16. The device according to claim 14, wherein the unlock code for the product is printed out upon purchase at the retailer.

17. The device according to claim 9, wherein the unlock device is a remote server.

18. A method for deterring theft for products having a device firmware for managing and controlling the product to function, said method comprising:

embedding a software code in the device firmware, the software code being adapted to deny access functionalities of the device by default;

generating an unlock code for unlocking the software code from a server;

identifying the device at a point of sale;

acquiring the unlock code from the server based on the identified device;

providing the unlock code at the point of sale; and

inputting the unlock code to unlock the software code to allow access functionalities of the device.

19. The method according to claim 18, further comprising printing the unlock code at the point of sale.

20. The method according to claim 18, further comprising executing the software code to prompt for the unlock code at the first use of the device.

21. The method according to claim 20, further comprising connecting the device to an unlock device to activate the software code to prompt for the unlock code.

22. The method according to claim 20, wherein the unlock code is inputted via the unlock device.

23. The method according to claim 18, wherein the unlock code generated by the server is sent to a manufacturer for manufacturing the device.

24. The method according to claim 23, wherein the server is located at the manufacturer.

25. The method according to claim 23, wherein the server is located at a service provider.

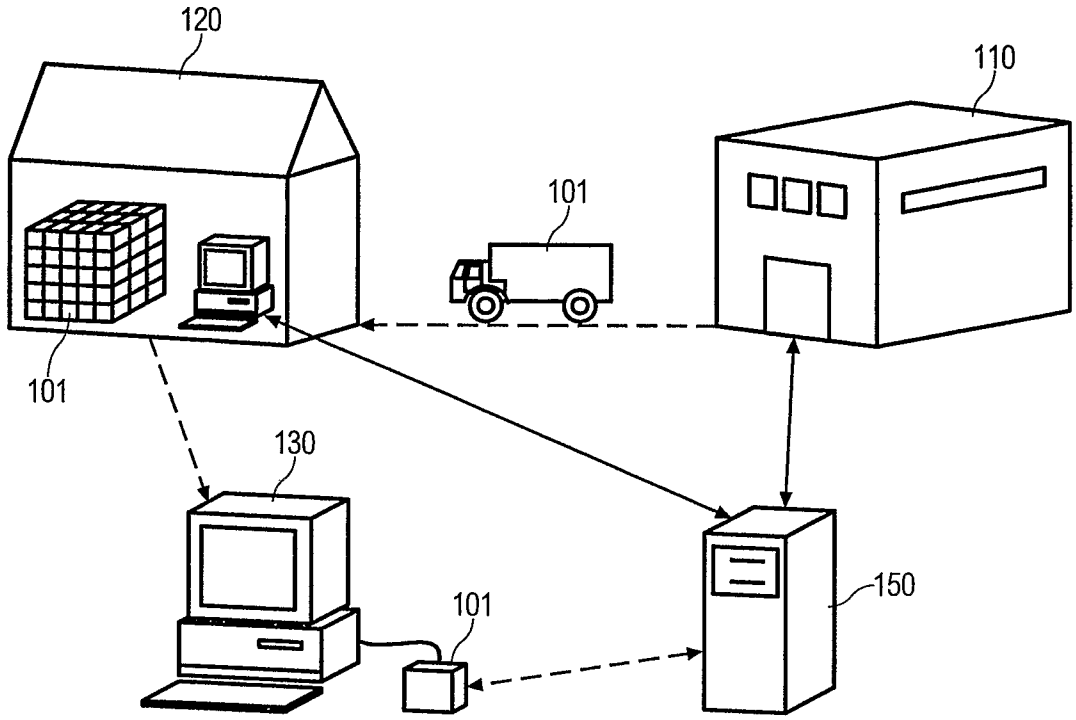
120
110
101
101
130
101
150

FIG. 1

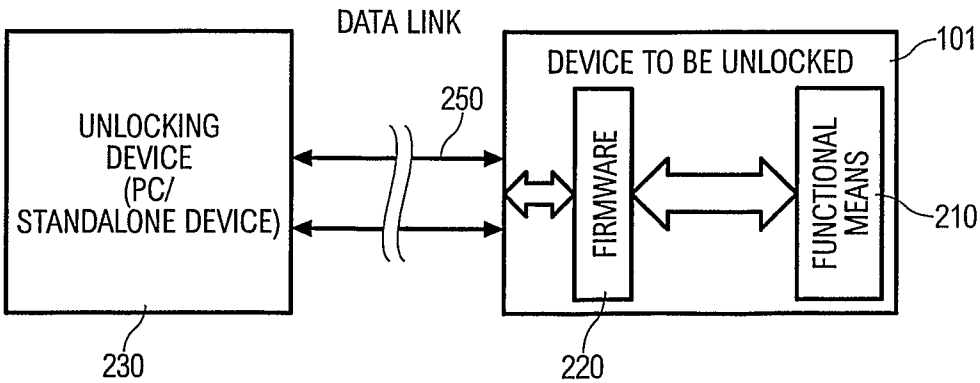
DATA LINK
UNLOCKING DEVICE (PC/ STANDALONE DEVICE)
250
DEVICE TO BE UNLOCKED
101
FIRMWARE
FUNCTIONAL MEANS
210
230
220

FIG. 2A

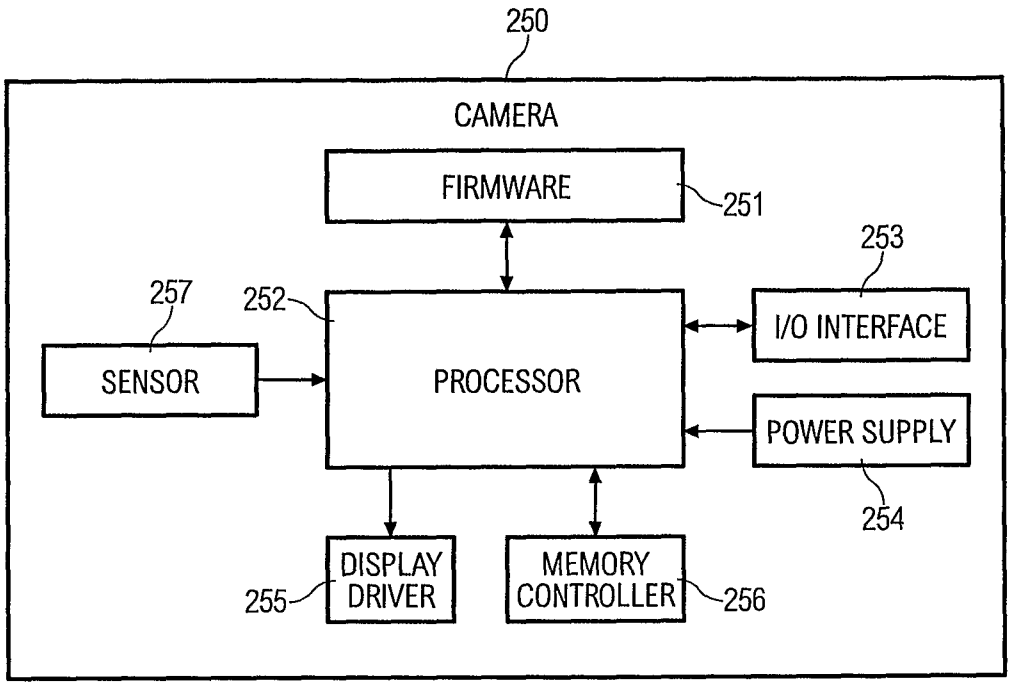
250
CAMERA
FIRMWARE
251
253
257
252
I/O INTERFACE
SENSOR
PROCESSOR
POWER SUPPLY
254
DISPLAY DRIVER
255
MEMORY CONTROLLER
256

FIG. 2B

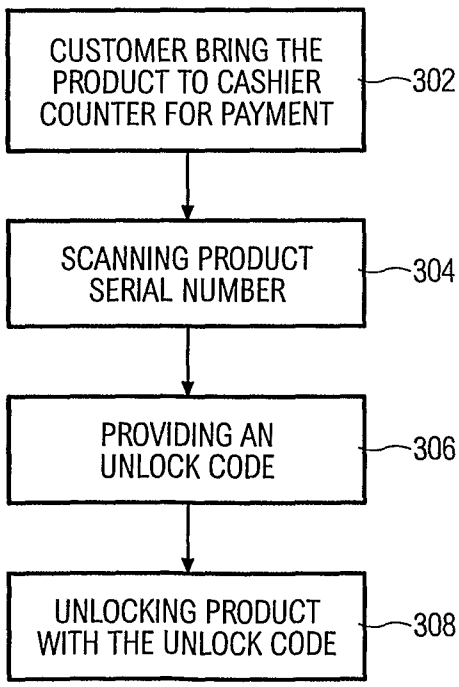
CUSTOMER BRING THE PRODUCT TO CASHIER COUNTER FOR PAYMENT
302
SCANNING PRODUCT SERIAL NUMBER
304
PROVIDING AN UNLOCK CODE
306
UNLOCKING PRODUCT WITH THE UNLOCK CODE
308

FIG. 3

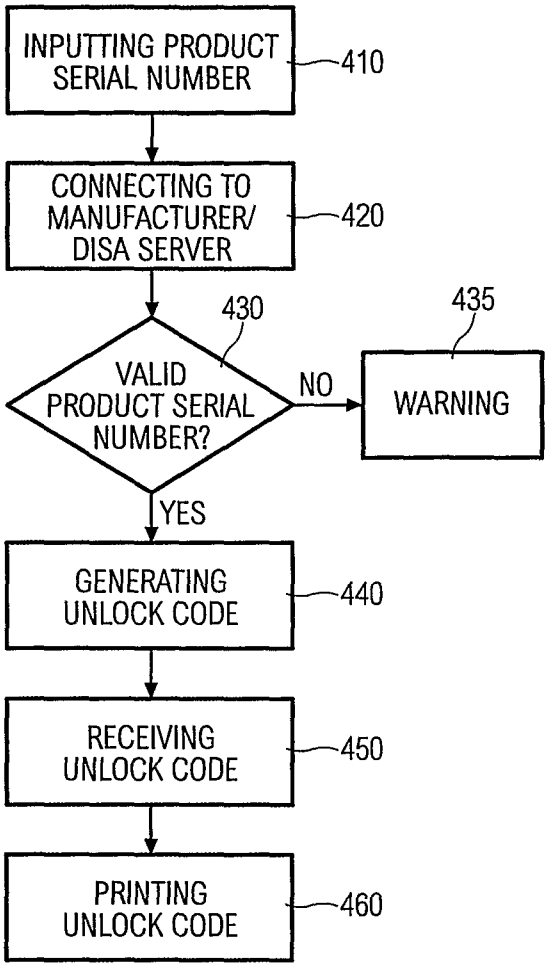
INPUTTING PRODUCT SERIAL NUMBER
410
CONNECTING TO MANUFACTURER/ DISA SERVER
420
430
VALID PRODUCT SERIAL NUMBER?
NO
435
WARNING
YES
GENERATING UNLOCK CODE
440
RECEIVING UNLOCK CODE
450
PRINTING UNLOCK CODE
460

FIG. 4

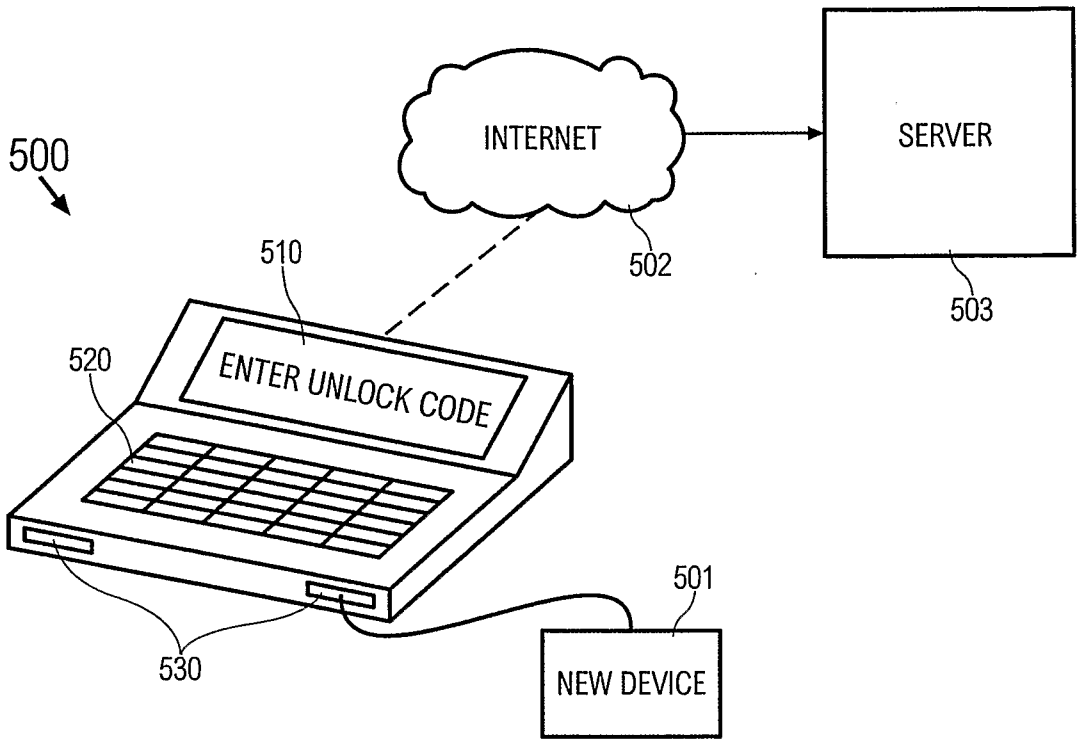
500
INTERNET
SERVER
502
503
510
520
ENTER UNLOCK CODE
501
530
NEW DEVICE

FIG. 5

INTERNATIONAL SEARCH REPORT

International application No.
PCT/SG2008/000052

A. CLASSIFICATION OF SUBJECT MATTER

Int. Cl.

G06F 21/22 (2006.01) *H04L 9/32* (2006.01)

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)
USPTO, DWPI & keywords: anti, deterrent, theft, activation, lock, unlock, code, password, identification, authentication and similar terms

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	US 7275686 B2 (ESTAKHRI ET AL.) 2 October 2007 Entire document (see particularly figures 1-16; column 5, lines 14-34; column 7, lines 57-61; column 7, lines 49-52; column 10, lines 7-12; column 11, lines 23-30)	1-25
X	US 2007/0257768 A1 (BOWERS ET AL.) 8 November 2007 Entire document (see particularly figures 1-4; paragraphs 0017, 0022, 0024)	1-5, 7-11, 13, 14, 16-22
Y	Entire document	12
X	US 2007/0109103 A1 (JEDREY ET AL.) 17 May 2007 Entire document (see particularly figures 1, 2, 4, 8; paragraphs 0006, 0007, 0052, 0104, 0105, 0108, 0109, 0110, 0123)	1-11, 13-25
Y	Entire document	12
X	US 2005/0240498 A1 (THALER) 27 October 2005 Entire document (see particularly figures 1-3; paragraphs 0007, 0008, 0010, 0037, 0039, 0041, 0043)	1-5, 7-11, 13, 14, 16, 18-22
Y	Entire document	12

[X] Further documents are listed in the continuation of Box C [X] See patent family annex

* Special categories of cited documents:

"A" document defining the general state of the art which is not considered to be of particular relevance

"E" earlier application or patent but published on or after the international filing date

"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)

"O" document referring to an oral disclosure, use, exhibition or other means

"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art

"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
16 April 2008	30 APR 2008
Name and mailing address of the ISA/AU AUSTRALIAN PATENT OFFICE PO BOX 200, WODEN ACT 2606, AUSTRALIA E-mail address: pct@ipaustralia.gov.au Facsimile No. +61 2 6283 7999	Authorized officer **Benjamin Lam** AUSTRALIAN PATENT OFFICE (ISO 9001 Quality Certified Service) Telephone No : +61 2 6225 6121

INTERNATIONAL SEARCH REPORT

International application No.
PCT/SG2008/000052

C (Continuation). DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
Y	US 2007/0268111 A1 (CHNG ET AL.) 22 November 2007 Entire document (see particularly figures 4, 5; paragraphs 007, 0026)	12

INTERNATIONAL SEARCH REPORT

Information on patent family members

International application No.
PCT/SG2008/000052

This Annex lists the known "A" publication level patent family members relating to the patent documents cited in the above-mentioned international search report. The Australian Patent Office is in no way liable for these particulars which are merely given for the purpose of information.

Patent Document Cited in Search Report		Patent Family Member					
US	7275686	CN	1809833	EP	1695304	US	2005133593
		WO	2005059854				
US	2007257768	NONE					
US	2007109103	NONE					
US	2005240498	NONE					
US	2007268111	EP	1891573	SG	137706	WO	2007133162

Due to data integration issues this family listing may not include 10 digit Australian applications filed since May 2001.

END OF ANNEX