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

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
5 October 2006 (05.10.2006)

PCT

(10) International Publication Number
WO 2006/105552 A2

(51) International Patent Classification:
G06F 21/00 (2006.01)

(21) International Application Number:
PCT/YU2006/000006

(22) International Filing Date: 27 March 2006 (27.03.2006)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
P-2005/0259 29 March 2005 (29.03.2005) PL

(71) Applicant and
(72) Inventor: **TOMASOVIC, Milan** [YU/YU]; Bulevar AVNOJ 47, YU-11000 Beograd (YU).

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

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

Declaration under Rule 4.17:
— *of inventorship (Rule 4.17(iv))*

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

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

WO 2006/105552 A2

(54) **Title:** DEVICE FOR PROTECTING DATA IN LAPTOP COMPUTERS IN CASE OF THEIR LOSS OR THEFT

(57) **Abstract:** Patent application relates to the DEVICE FOR PROTECTING DATA IN LAPTOP COMPUTERS IN CASE OF THEIR LOSS OR THEFT. This invention has solved the problem of design of devices enabling the owner of the laptop computer to locate the position of his/her computer in case of loss or theft and after this, as required, to provide the function of locking and destruction of data in it. This has been achieved so that the device (1), according to the invention, consists of the assembly (2) of sensors for alarming loss of laptop computers, the assembly (3) for communication with the operative center (8) consisting of GSM module (4) and (A)GPS module (5), assembly (6) for providing the function of hard disk data protection (9), control module (10) and batteries for autonomous feeding (7).

DEVICE FOR PROTECTING DATA IN LAPTOP COMPUTERS IN CASE OF THEIR LOSS OR THEFT

FIELD OF THE INVENTION

Field of the invention, generally speaking is the field of electrical engineering and it specifically relates to the complex electronic system allowing the permanent locating of the position of laptop computers and implementation of the process of protection of data in them.

According to the International classification of patents (Int.cl[7]) the invention is marked with the basic classification symbol H04M 11/04 that defines telephone communication systems combined with alarm systems, as well as with the secondary classification symbol G08B 21/20 that relates to alarms reacting to the presence and absence of persons or G08B 21/24 defining warning alarms.

As the subject device, according to the invention, resolves the problem of protection of data in case of laptop computer disappearance, it can be marked with yet another secondary classification symbol A45C 13/24 defining alarms against losses.

ART PROBLEM

The art problem resolved by the invention consists of the following: How to design a device constantly giving the owner of the laptop computer the position of his computer and in case of loss or theft, as required, allows locking or destruction of data in it and such a device should be small by dimensions and should not reduce laptop computer performances, or rather the process of locating and giving commands for locking and destruction of data should be simple, quick, automatic and safe and it should function in all areas covered by GSM network and (A)GPS.

STATE OF ART

Laptop computers are increasingly becoming dominant and used allowing their owners rational time use. Despite small dimensions they now have all functions as desktop computers so that they contain various data in the fields of science, technology, finance and even defense, or data representing business, military, political and other secrets and therefore they should be adequately safeguarded.

In the past few years, according to reports by the British Ministry of Defense, around 50 laptop computers containing important data are averagely lost each year. Those computers have contained most confidential data. It is interesting that the highest

number of laptops has been lost in public transport, coffee shops and at other public places. During the past two years, according to media information, laptop computers have been lost or stolen with data relating to nuclear and other weapons for mass destruction and with information about the latest types of armament, etc.

Prevention and stopping loss of laptops and safeguard of data in them is today achieved in one of the following ways:

A) Prevention from theft or loss

- fitting special alarms with various sensors reacting to separation of the device from its owner;
- use of special protective bags;
- fitting anti-theft cards reacting to forbidden move of computers;
- use of various mechanical theft protection devices.

B) Prevention of device use

- putting a password on BIOS (boot password and supervisor password);
- putting a password for Windows;
- fitting an anti-theft card for hardware protection;
- fitting biometric sensors allowing access to computer data;

C) Prevention of access to data

- fitting biometric sensors allowing access to computer data;
- using passwords for access to data;

D) Locating position of stolen or lost computers

- tracking computer positions from operative centers dealing with tracking.

In the author's opinion the above methods of laptop protection from theft and loss and disabling access to computer data are not reliable enough for the following reasons:

- password functions can be bypassed with simple BIOS resetting or by transferring hard disk to another computer;
- fitting biometric sensors that undoubtedly has more positive than negative effects, despite a significant rise in computer prices, has one essential shortage reflected in the fact that the problem of laptop theft moves from the stealing item to the owner and entails the question of his privacy and also it does not disable a possibility of a simple transfer of hard disk to another computer.
- the tracking problem is of a technical nature, first of all because the computer can be tracked only if connected to Internet and only via the IP address with a note that the tracking system operates in some countries only;

- various alarm types are effective only in cases when the device is satisfactorily near the owner so that he/she can receive a warning and take specific measures for computer and data protection.

The following have been found when perusing local and foreign patent applications and patent papers and adequate expert and scientific literature in the field of devices and electronic systems allowing the location of laptops and implementation of the process of protection of data in them:

- ANTITHEFT DEVICE FOR PC OR OTHERS (Japanese patent, JP 10225346);
- ANTITHEFT APPARATUS, ANTITHEFT METHOD AND RECORDING MEDIUM RECORDING THEREON ANTITHEFT ORIGRAM (patent US 6307470);
- COMPUTER-OR TELEPHONE CONTROLLABLE PROGRAMMABLE ANTITHEFT SYSTEM, HAVING AN IDENTIFICATION OF THE STATE OR SINGLE PROTECTION FITTINGS (EP 1 335 337 A1).

Comparison of the above patent documentation it has been established that the indicated technical solutions, except by names and identical classification symbols according to the International classification of patents, are essentially different from this invention.

FUNDAMENTAL NATURE OF THE INVENTION

Fundamental nature of the invention is reflected primarily in the fact that according to the author's idea a device has been designed allowing electronic communication between the laptop and owner for permanent control and location of the place where the device is currently placed.

Fundamental nature of the invention is reflected in the fact that the function of laptop is achieved with a double control system and with control achieved via satellite tracking of the device through AGPS or GPS control systems and GSM network of mobile telephony with standard possibilities of continuing position control and passing to the active state ensuring the alarming of the owner and protection of computer data.

One novelty of the invention is reflected in the fact that the device, according to the invention, based on commands by the laptop owner, after a simple process, performs instant locking or destruction of all data in the computer, or, as required, destroys the hard disk. According to the author's idea, the process of laptop protection that together with the subject device is this whole invention, is allowed with suitable software tracking operation of the device in its passive state (when the laptop is with the owner) and activates operation of the device warning the owner, implements location commands and as required data protection commands.

Fundamental nature of the invention is also reflected in the way of device application that for the protection of laptops and data in them is implemented through the following process:

1. A sensor assembly for alarm activation reacts based on the separation of the laptop and its owner;

2. An assembly for sending warning signals about theft or loss of laptops through GPS, AGPS and GSM sends data about this to the operative center and to the owner of the missing laptop;

3. The operative center sends a message or a call to the computer owner to his mobile phone about the current position of the missing device;

4. The owner decides whether to implement a process of data protection or thinks that the laptop is in a safe position;

5. The owner sends a command via his mobile phone, or with a simple call locks data, brings the device back in the passive state or as required destroys data in it;

6. If he/she has decided to protect data, an adequate assembly in the device gives a signal to the computer to implement locking, destruction of data or destruction of the hard disk.

Note: in case that the owner of the laptop does not respond to the call of warning in respect of the loss of the device, the operative center after the planned time directly activates the assembly for data protection after which locking of the hard disk is done or its destruction.

According to the invention the device, in respect of other known and applied solutions, has more advantages of which the most important are the following:

- Maximum speed of reaction in case of theft or loss laptops;
- The device is simple, reliable and has a module structure providing compatibility for building in new elements improving its hardware and software;
- It achieves full programming and logistic support for constant control of the laptop position;
- A much higher degree of safety and protection of confidential data has been achieved by accepting use of this device.

BRIEF DESCRIPTION OF FIGURES

In order to better understand the invention and to show how the invention could be realized in practice, the author, just for an example, refers to enclosed figures relating to the subject application where:

- *Figure 1* shows a simplified diagrammatic display of device functioning that disables access to laptop data in case of their loss or theft.

- *Figure 2* shows a simplified diagrammatic display of device functioning that disables access to laptop data in case of their loss or theft with the integrated control module in the hard disk.

- *Figure 3* shows a block diagram of the device according to the invention in which (A)GPS and GSM functions are integrated in the BIOS hard disk.

- *Figure 4* shows the method of connecting the control module with other device assemblies according to the subject invention.

DETAILED DESCRIPTION OF THE INVENTION

Example 1

Looking at the attached *figure 1* it can be easily seen that the device 1 for disabling access to laptop data in case of their loss pr theft consists of the following: assembly 2 of sensors alarming the forbidden separation of the laptop from the owner, assembly 3 for communication with the operative center 8 and the location of the current position of laptops made of GSM module 4 and (A)GPS mosule 5, assembly 6 providing the function of data protection on hard disk 9, control module 10 and autonomous supply battery 7.

Looking at the attached *figure 4*, in which for proving invention feasibility the device according to the invention has been shown, it can be noticed that signal entry from the alarm sensor assembly 2 is made through two direct Schmidt triggers 11 and two inverted entries with diodes 12 after which the signal, through contacts *39, 38, 37, 36* and *35*, travels to the control module 10 that is of standard make (AT89C55WD). Relay supply 19 for alarm wake activated with sensor assembly 2 and (A)GPS module 5 is carried out with the stabilization and battery filler 20. Control module 10, through contacts *15, 16 and 17*, activates DTMF 13 (the chip that allows access to voice services on the call receiver – recordist relation) through which GSM module 4 is switched on and alarm signal is passed to the operative center 8 and the owner of the mobile phone. At the same time through (A)GPS module 5, aerial 14, Eprom of chip 18 (made as temporary operating memory in which the terrain card is placed) and the satellite constantly sees the position of the laptop and relevant information is sent to operative center 8.

Functions of control module 10, which in this example of the invention is made as a microcontroller AT89C55WD, according to the author's idea, consist of the following:

a. Signal processing, SMS messages or calls

b. SMS message sending to the center

c. SMS message sending to the mobile phone.

Following the information to the effect that there has been loss or theft of the laptop its owner, by mobile phone, activates the assembly 6 for data protection and after

this locking of the hard disk 9 is performed or its destruction if necessary. Operation of the assembly 6 consisting of Tx and Rx 16 is made possible with the assembly 17 of standard design that through contacts *18 and 19* is connected to control module 10. The method of destruction of the hard disk is a business secret and it is possible to be carried out so that the hard disk is burnt with magnesium powder (capsulated in a precisely specified quantity), exposed to high voltage, strong magnetic field, etc.

Data protection in the process of communication is realized with the user name, password, telephone number and PIN code.

Feeding protection is performed with a special safeguard of the battery 7 (physical locking, etc.).

As seen in the enclosed *figure 1* components making the device disabling access to data in laptops in case of their loss or theft are not individually the subject of protection, but it is their whole assembly and therefore for easier simplification and easier understanding of the invention their detailed diagrams have not been given but are just shown in the assembly where their functional connection can be seen.

Device operation, according to the invention, is provided by a special software package compatible with the operative center software to which the device is connected and is adjustable to changes associated with technology development (A)GPS and GSM networks, mobile telephones and new laptops.

It is necessary to mention that the author, in the example of the invention make, has opted for a double security of communication links and location of laptop positions with the help of GSM mobile telephony network and (A)GPS systems because of the need to provide maximum safety and reliability subject to the importance laptop data protection.

It is necessary to emphasize that for the protection of data of a high level of confidentiality it is recommended to introduce special operative centers or divisions in the existing operative centers that within the framework of receipt of data and information will have a segment relating to the position tracking of laptops that are under a special system of supervision with a possibility of undertaking measures for data protection in accordance with the established procedure beforehand.

Example 2

Device 1 for laptop data protection, in case of their loss or theft, as seen in *figure 3*, is possible to be made so that it consists of the assembly 2 of sensors for alarming forbidden separation of laptop computers from their owners, the assembly 3 for communication with the operative center 8 and the location of the current position of laptop computers consisting of GSM module 4 and (A)GPS module 5, the assembly 6 for providing the function of data protection on the hard disk 9, control module 10 and the battery for autonomous supply 7 when functions allowing communication through (A)GPS and GSM networks are integrated in the laptop hard disk BIOS (9).

Process of laptop data protection according to example 2 is carried out based on the same procedure as in example 1.

METHOD OF INDUSTRIAL OR OTHER APPLICATION OF THE INVENTION

Industrial make of the invention is absolutely possible in factories for making electronic devices and even in well equipped specialized electronic workshops according to workshop documentation that experts in this field can make by using descriptions and figures in this application.

Its application is recommended to users keeping data in laptop computers) scientific, military, technological, financial, etc.) of a high level of confidentiality.

CLAIMS

1. Device for protecting data in laptop computers in case of their loss or theft IS CHARACTERIZED BY THAT the device (1), according to the invention, consists of the assembly (2) of sensors for alarming disappearance of laptop computers, the assembly (3) for communication with the operative center (8) consisting of GSM module (4) and (A)GPS module (5), assembly (6) for providing the function of hard disk data protection (9), control module (10) and batteries for autonomous feeding (7).

2. Device for protecting data in laptop computers in case of their loss or theft IS CHARACTERIZED BY THAT the device (1), according to the invention, consists of the assembly (2) of sensors for alarming disappearance of laptop computers, the assembly (3) for communication with the operative center (8) consisting of GSM module (4) and (A)GPS module (5), the assembly (6) for providing the function of hard disk data protection, control module (10) and batteries for autonomous feeding (7) where the control module (10) is directly integrated in the laptop hard disk (9).

3. Device for protecting data in laptop computers in case of their loss or theft IS CHARACTERIZED BY THAT the device (1), according to the invention, consists of the assembly (2) of sensors for alarming disappearance of laptop computers, the assembly (3) for communication with the operative center (8) consisting of GSM module (4) and 9A)GPS module (5), the assembly (6) for providing the function of protection of hard disk data (7) where functions enabling communication through (A)GPS and GSM networks are integrated in hard disk BIOS (9) of laptop computers.

4. Process for data protection in laptop computers in case of their loss or theft, according to claims 1, 2 and 3 IS CHARACTERIZED BY THAT it is carried out through the following procedure:

1. Sensor assembly for activating the alarm reacts based on separation of laptop computers and owners.

2. Assembly for sending warning signals about theft or loss of laptops via GPS, AGPS and GSM send related data to the operative center and to the owner of the missing laptop computer.

3. The operative center sends a message or call to the computer owner to his mobile phone about the current position of the missing device.

4. The owner decides whether to carry out the process of data protection or thinks that the laptop is in the safe position.

5. The owner sends a command via his mobile phone, or with a simple call locks data up, bring the device back in the passive state or if required destroys data in it.

6. If the owner has decided to protect data, the relevant assembly in the device gives a signal to the computer to perform locking, destruction of data or destruction of hard disk.

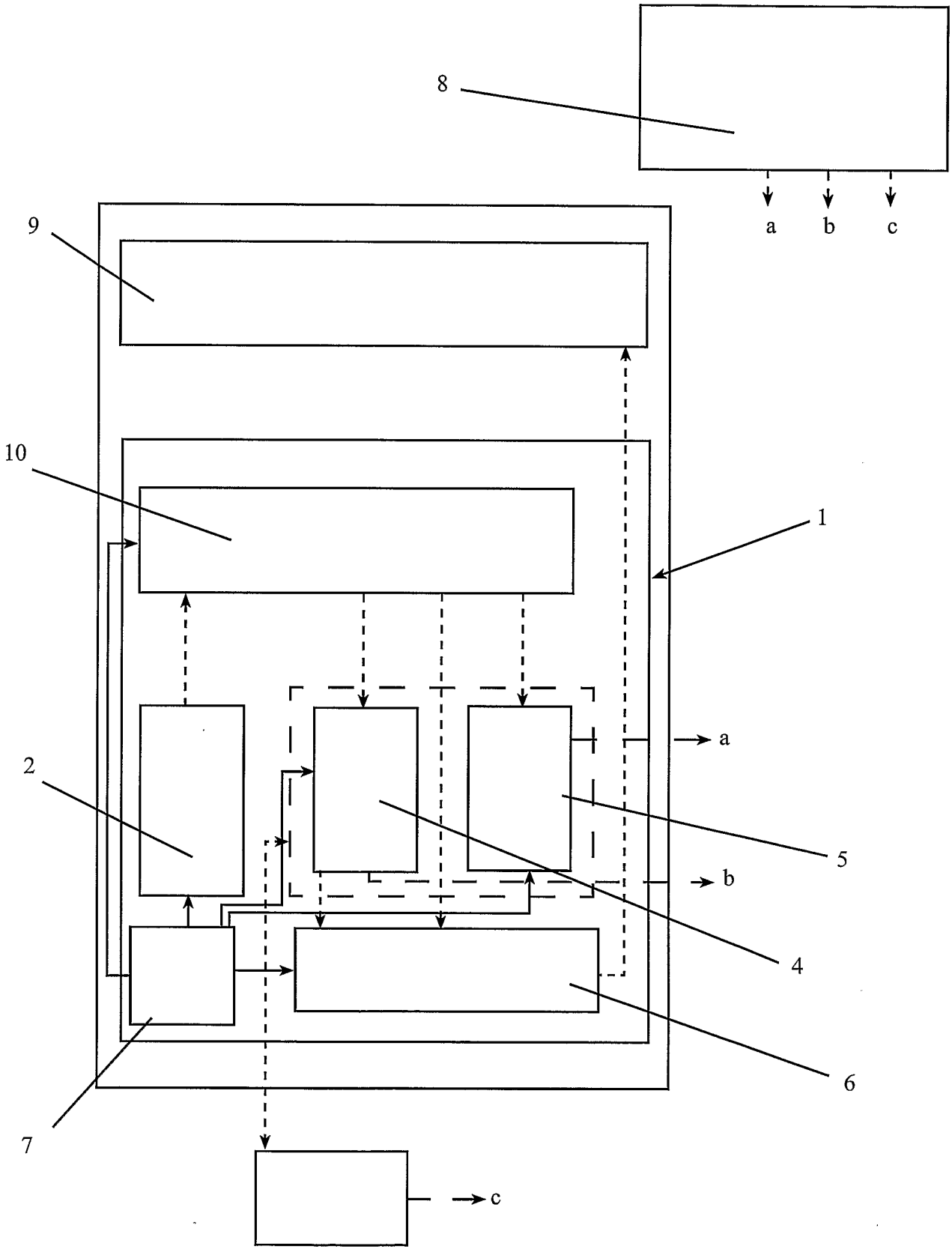

FIG. 1

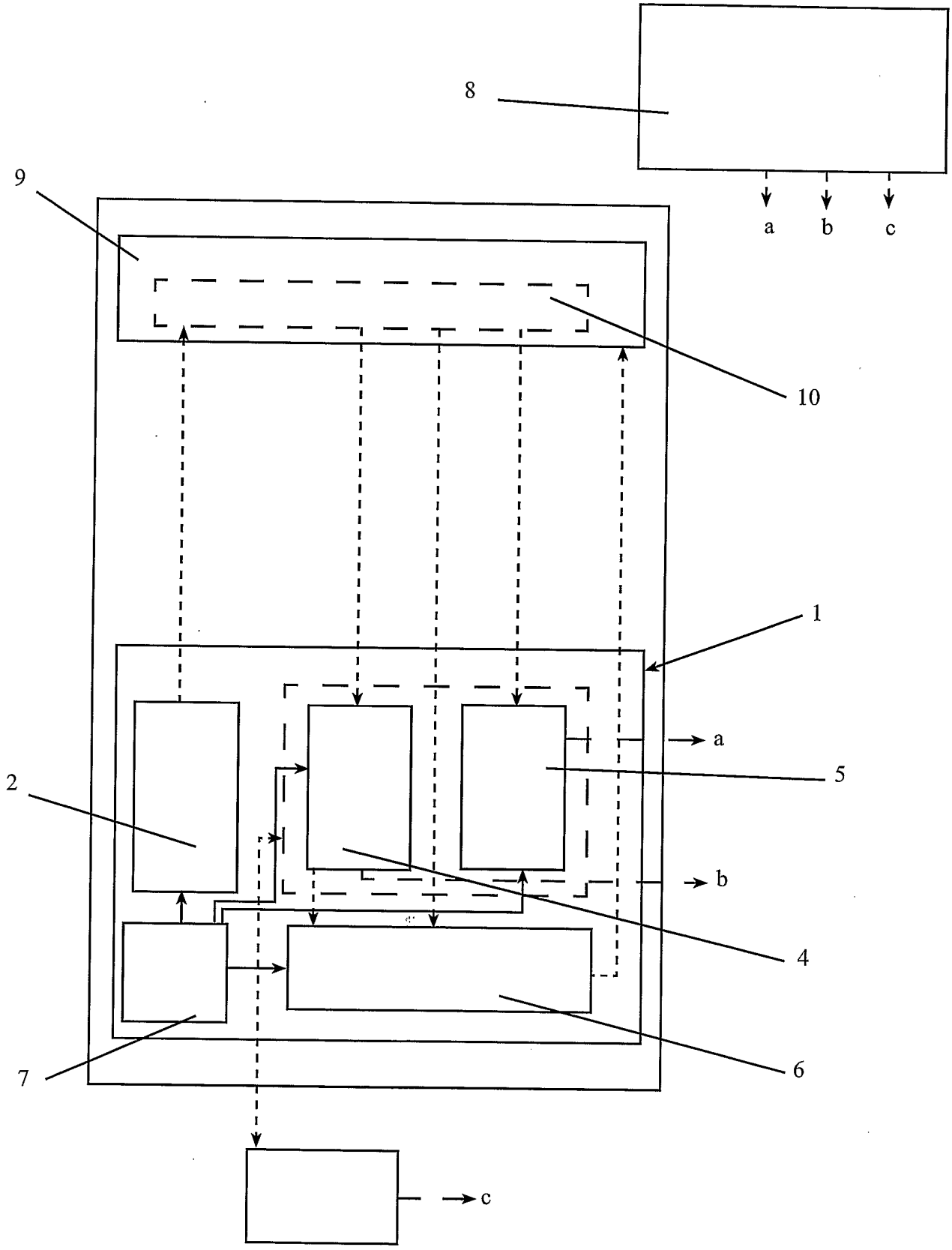

FIG. 2

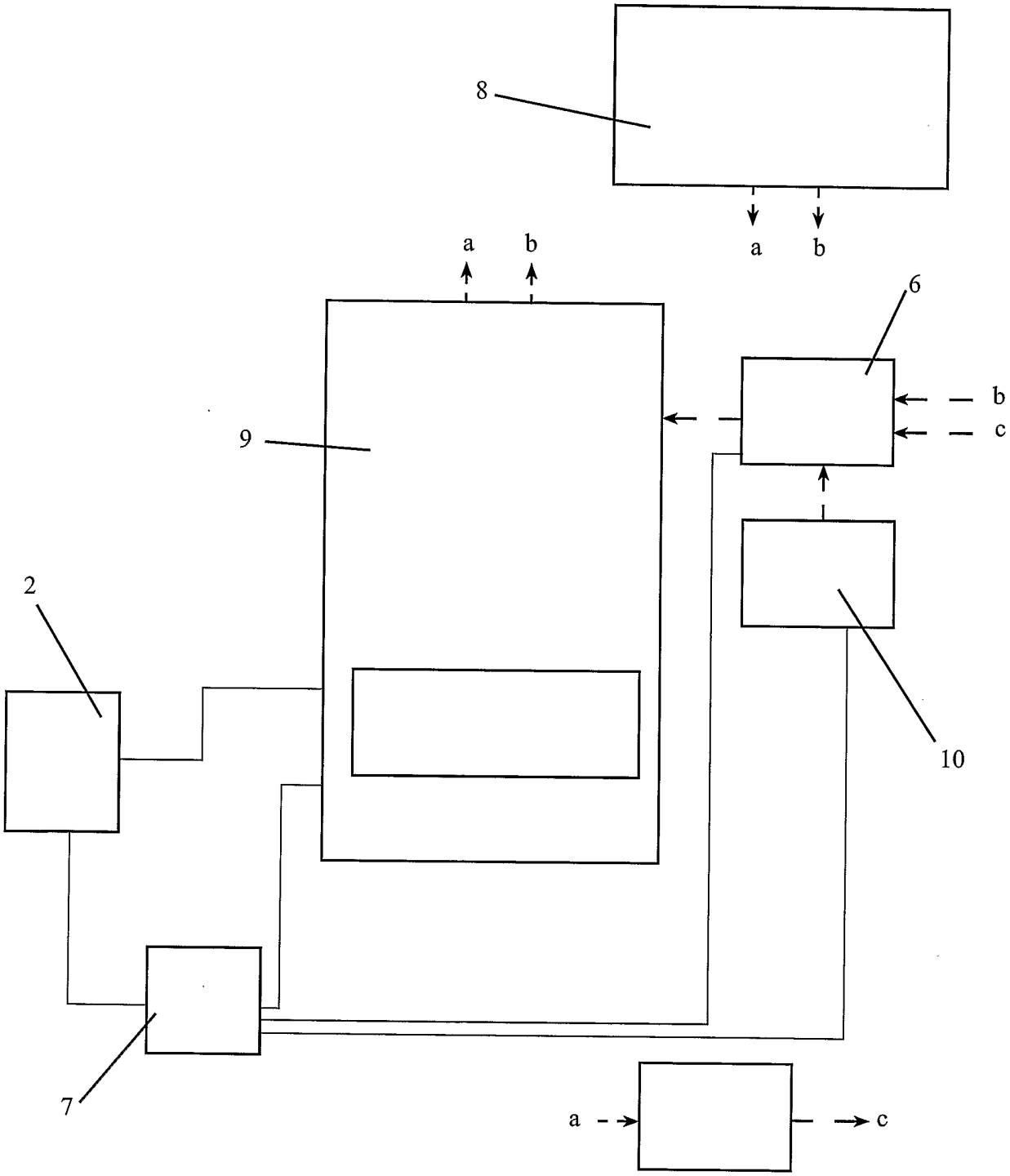

FIG. 3

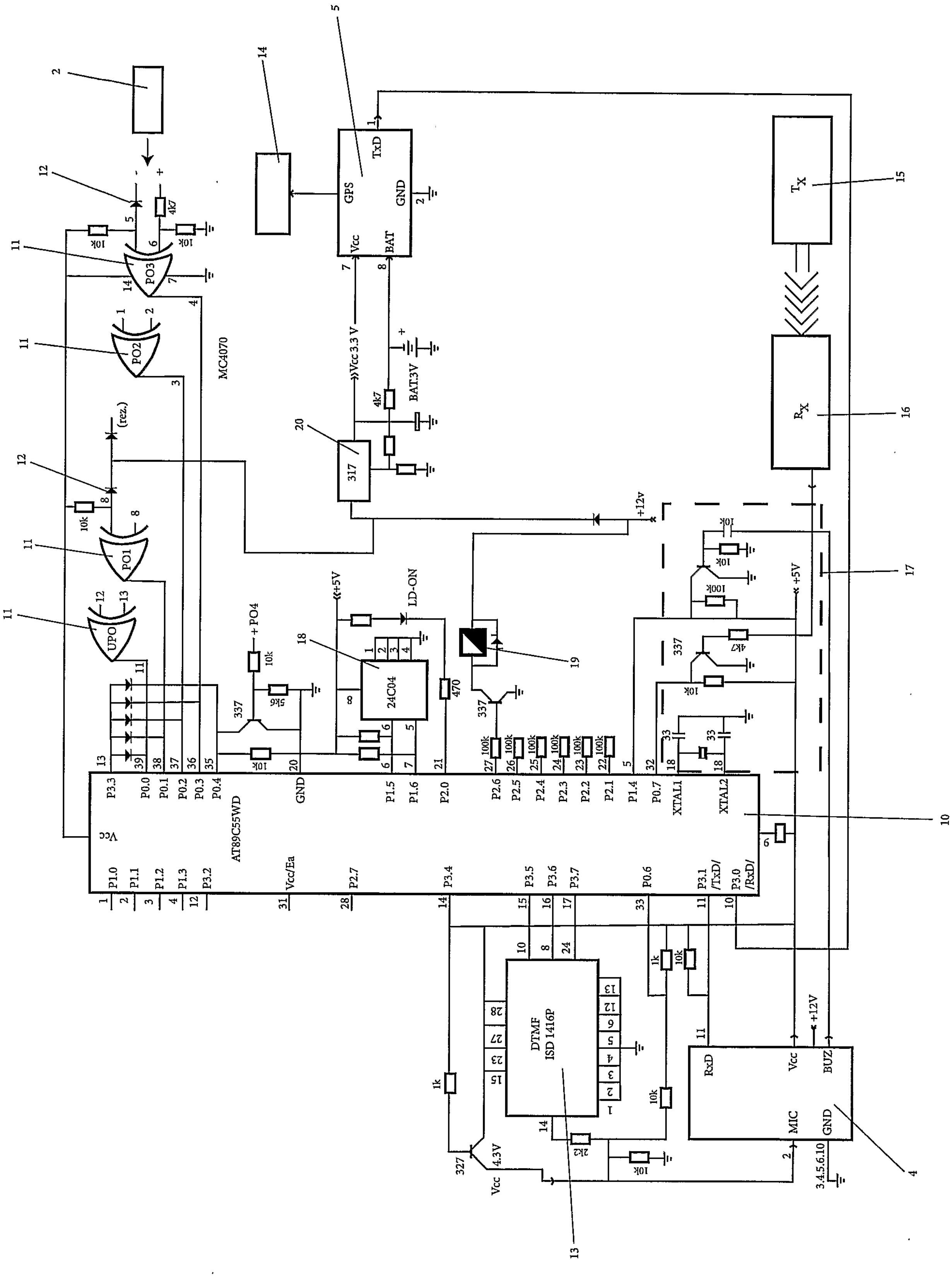
AT89C55WD
MC4070
DTMF
ISD 1416P
24C04
317
GPS
TxD
GND
Vcc
BAT
Vcc 3.3 V
BAT3V
LD-ON
+12v
+5V
RxD
BUZ
MIC
Tx
Rx
(rez.)
UPO
PO1
PO2
PO3
XTAL1
XTAL2

FIG. 4