US006164403A

United States Patent [19]

Wuidart

[11] **Patent Number: 6,164,403**

[45] **Date of Patent: Dec. 26, 2000**

[54] **SECURITY SYSTEM**

[75] Inventor: **Luc Wuidart**, Pourrieres, France

[73] Assignee: **STMicroelectronics S.A.**, Gentilly, France

[21] Appl. No.: **09/220,524**

[22] Filed: **Dec. 23, 1998**

[30] **Foreign Application Priority Data**

Dec. 24, 1997 [FR] France 97 16467

[51] **Int. Cl.**[7] **B60R 25/00**

[52] **U.S. Cl.** **180/287**; 340/425.5

[58] **Field of Search** 180/287; 340/425.5, 340/426, 485.69

[56] **References Cited**

U.S. PATENT DOCUMENTS

4,151,512	4/1979	Riganati et al.	340/146.3
4,663,626	5/1987	Smith	340/825.69
4,926,332	5/1990	Komuro et al.	364/424.05
5,661,451	8/1997	Pollag	340/426
5,729,191	3/1998	Allen et al.	340/426
5,818,330	10/1998	Schweiger	340/426
5,887,466	3/1999	Yoshizawa	70/257

FOREIGN PATENT DOCUMENTS

01114193	5/1989	Japan .
08270281	10/1996	Japan .
WO95/15663	6/1995	WIPO .

Primary Examiner—Kevin Hurley
Assistant Examiner—Kevin McKinley
Attorney, Agent, or Firm—Theodore E. Galanthay; Stephen C. Bongini; Fleit, Kain, Gibbons, Gutman & Bongini P.L.

[57] **ABSTRACT**

A security system of the type having a fixed terminal and a portable unit such as a remote control. The portable unit produces an activation signal based on active intervention by a user and a measurement signal based on the measurement of a biometrical signature of the user. A control signal is generated when the activation and measurement signals are both generated within a specified temporal window and the measured biometrical signature corresponds to that of an authorized user. Thus, there is a reduced chance of both the security system being disarmed by an ill-intentioned third party and of untimely or inadvertently disarming the system.

33 Claims, 2 Drawing Sheets

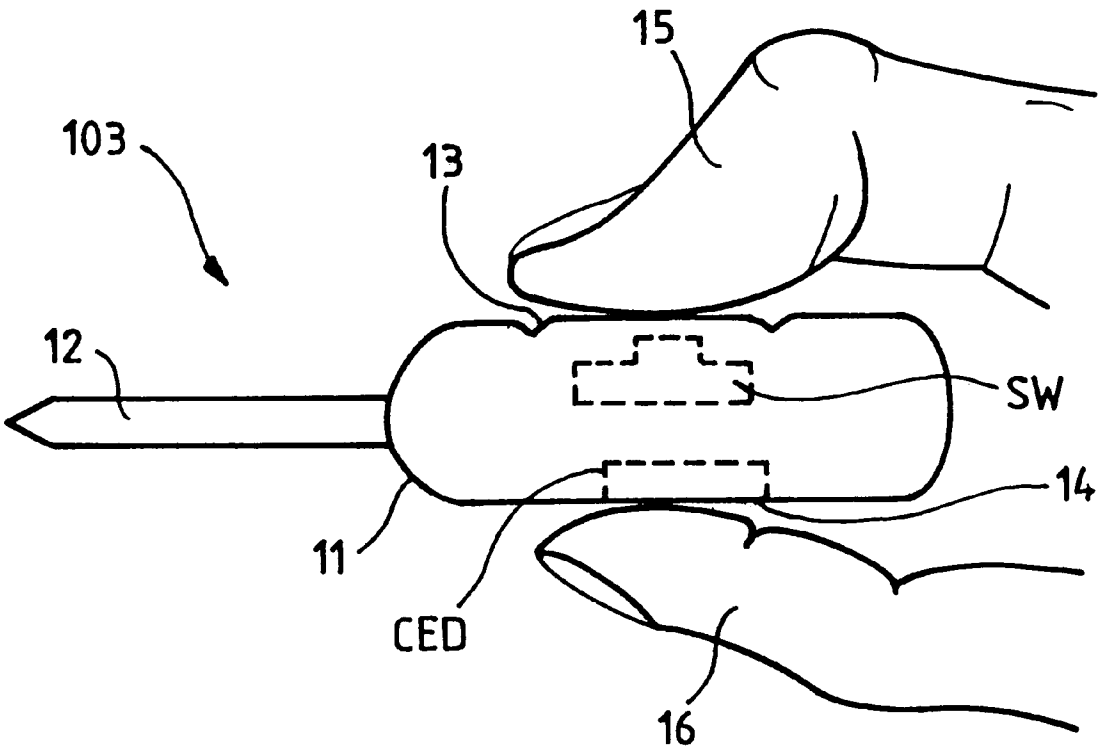


FIG_1

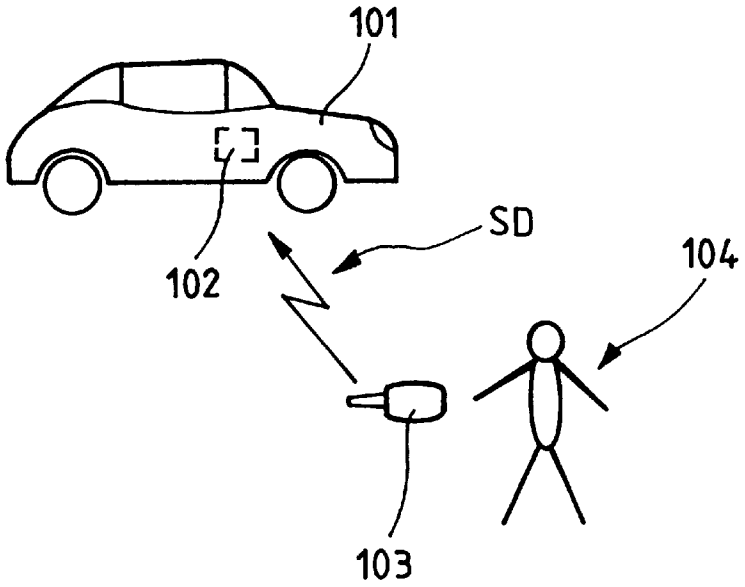


FIG_2

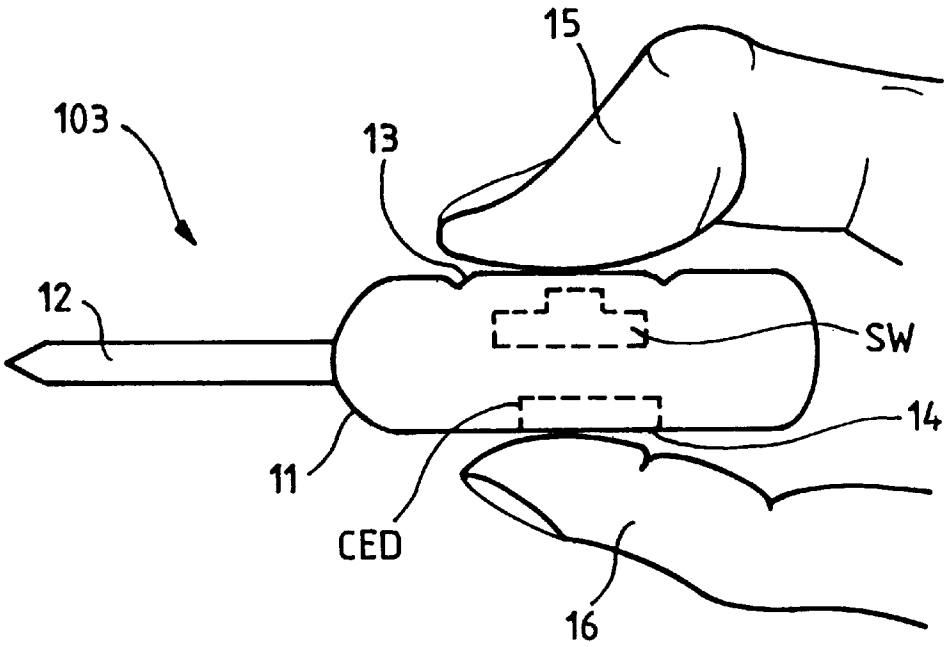
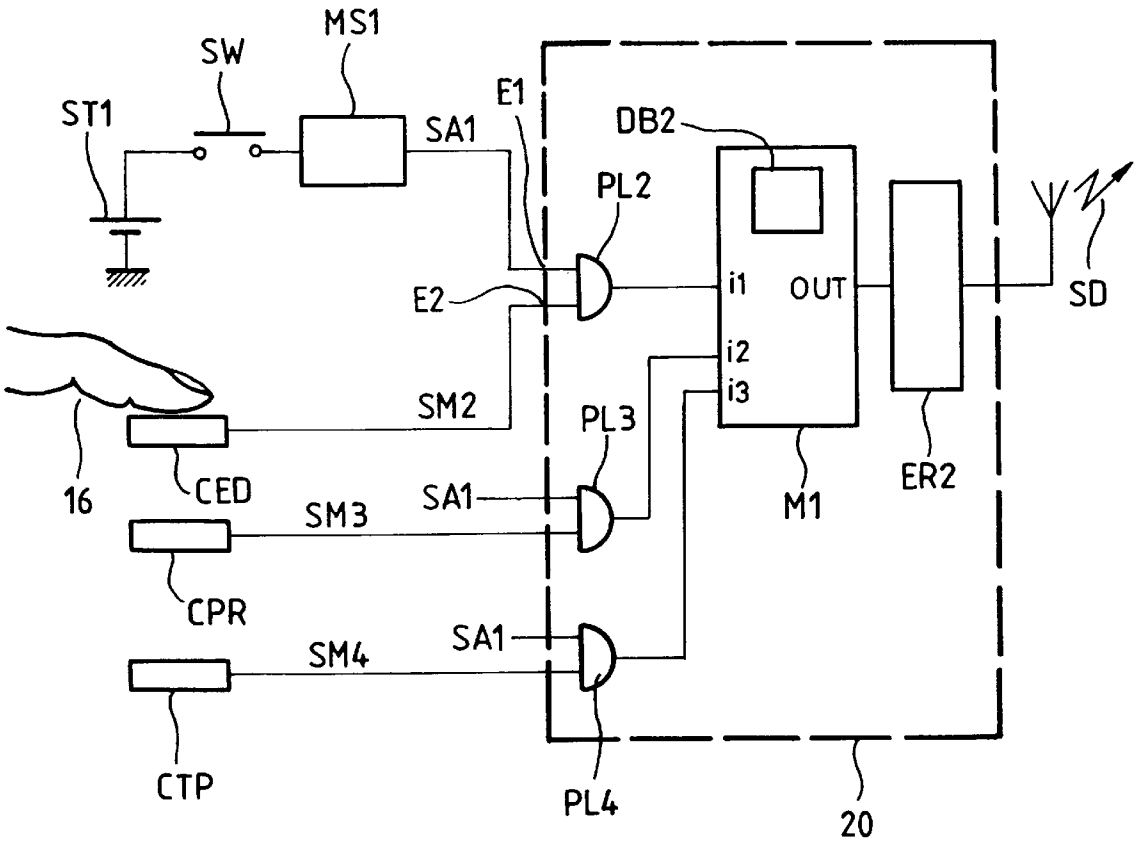


FIG_3



SECURITY SYSTEM

CROSS-REFERENCE TO RELATED APPLICATIONS

This application is based upon and claims priority from prior French Patent Application No. 97-16467, filed Dec. 24, 1997, the entire disclosure of which is herein incorporated by reference.

BACKGROUND OF THE INVENTION

1. Field of the Invention

The present invention relates to security systems, and more specifically to security systems of the type having a fixed terminal and a portable unit that delivers a signal to the fixed terminal.

2. Description of Related Art

A conventional automobile security system is one example of a security system that has a fixed terminal and a portable unit that delivers a lock/unlock signal to the fixed terminal. In the typical automobile security system, the fixed terminal is a device for the centralized locking and unlocking of the vehicle and the portable unit is a remote control for operating the locking and unlocking device. The portable unit is designed to be carried by an authorized user (e.g., the vehicle owner), and under certain conditions delivers the lock/unlock signal to the fixed terminal in order to remotely lock or unlock the doors of the vehicle. (This description uses the term "fixed", for example in designating the locking and unlocking device on the vehicle, in a relative sense and the term should be understood with reference to the portable unit.)

The lock/unlock signal from the portable unit is generally transmitted by a carrier wave such as an electromagnetic or infrared wave, and typically includes a fixed or changing code (i.e., a code whose value depends on the number of previous transmissions). The code must be recognized as valid by the fixed terminal in order for the signal to prompt the locking or unlocking of the doors of the vehicle. While this provides some anti-theft protection, the security level of such a system against theft is still imperfect because the mere physical possession of the portable unit is generally sufficient to effect the unlocking of the vehicle. Thus, if the portable unit is lost or stolen, an ill-intentioned third party can easily use the portable unit to open the doors of the vehicle and then remove articles inside the vehicle or even steal the vehicle.

To overcome this problem, a security system can be associated with its authorized user (or users) so that only an authorized user can unlock the doors of the vehicle. For example, the system can include means for measuring a biometrical signature of an authorized user. With such a means, the security system can use a biometrical signature such as a fingerprint, the iris of the eye, or an audiometrical spectrum of the authorized user's voice to identify or authenticate a physical person. To this end, it has been proposed to use a voice recognition module in the fixed terminal of a security system to control the locking or unlocking of the vehicle upon the sound of the authorized user's voice. In such a system, the portable unit becomes superfluous and can be eliminated to produce a "hands-free" access system.

While such a system would provide some advantages over conventional security systems, there is a risk that the vehicle will be accidentally unlocked. For example, when in the vicinity of the vehicle, the authorized user could inadvertently pronounce a word or sequence of words that prompts the unlocking of the vehicle. If the user does not realize that this has happened, the user may walk away and thus inadvertently leave the vehicle unguarded with its doors unlocked.

SUMMARY OF THE INVENTION

In view of these drawbacks, it is an object of the present invention to remove the above-mentioned drawbacks and to provide a security system of the type associated with an authorized user (or users) that has a reduced chance of an inadvertent or untimely unlocking of the vehicle. The security system includes a fixed terminal and a portable unit that provides the fixed terminal with a signal for locking and unlocking a functional unit (e.g., a vehicle). The portable unit includes a detector, a measurement device, and a signal generator. The detector generates an activation signal when active intervention by a user is detected, and the measurement device measures a biometrical signature of the user. When the activation signal and a measurement signal are produced within a specified temporal window, the signal generator generates the lock/unlock signal if the measured biometrical signature corresponds to that of an authorized user. Because the measurement of a valid biometrical signal is necessary to prompt the portable unit to transmit the lock/unlock signal, an ill-intentioned third party possessing the portable unit cannot use it to unlock the vehicle. Further, because an active intervention by the user is still necessary to transmit the lock/unlock signal, the chance of untimely or inadvertently unlocking the vehicle is significantly reduced or eliminated. The present invention also preserves the function of a remote unit so that the users' current habits do not have to be significantly modified.

Other objects, features, and advantages of the present invention will become apparent from the following detailed description. It should be understood, however, that the detailed description and specific examples, while indicating preferred embodiments of the present invention, are given by way of illustration only and various modifications may naturally be performed without deviating from the present invention.

BRIEF DESCRIPTION OF THE DRAWINGS

FIG. **1** is a simplified drawing showing a security system for an automobile;

FIG. **2** is a drawing showing a portable unit according to an embodiment of the present invention; and

FIG. **3** is a block diagram of a portable unit according to an embodiment of the present invention.

DETAILED DESCRIPTION OF PREFERRED EMBODIMENTS

Preferred embodiments of the present invention will be described in detail hereinbelow with reference to the attached drawings.

FIG. **1** is a simplified illustration of a security system for an exemplary functional unit in the form of an automobile. The automobile **101** is fitted with an onboard fixed terminal such as a centralized locking and unlocking unit **102**. The security system also includes a portable unit **103** such as a "remote" control that is usually associated with a key for the vehicle. (In the following description, the portable unit is identified with the remote control or the key for the vehicle and these three expressions are used without distinction.)

The portable unit is designed to be carried and operated by an authorized user **104** (e.g., the owner of the vehicle), and

other authorized users can use the same portable unit **103** or another unit of the same kind that is assigned to them for the same function. Under certain conditions, the portable unit **103** delivers a lock/unlock signal SD to the fixed terminal **102** by means of a carrier wave such as an electromagnetic or infrared wave. In preferred embodiments, the lock/unlock signal SD is an amplitude-modulated or phase-modulated radio frequency signal that is generated by the portable unit.

FIG. **2** shows a more detailed view of a portable unit in the form of a key in accordance with an embodiment of the present invention. The key **103** has a conventional metal portion **12** that forms a key insert and an upper portion **11** that forms the head or grasping portion of the key. The upper portion **11** fulfills a remote control function of the system. For this purpose, the upper or remote control portion in the illustrated embodiment is a plastic portion containing an electronic circuit that transmits the lock/unlock signal SD. The remote control portion includes detection means for detecting the active intervention of the user in a known manner. For example, the detection means can include one or more keys of a keyboard, or more simply a switch SW (e.g., a push-button type switch) that is positioned under a first region **13** of the remote control portion **11**. The first region **13** of the remote control portion can be folded by pressure exerted by the user's thumb **15** (e.g., because of a smaller thickness or the presence of adjacent ribs) to activate the switch SW within the remote control portion **11**.

Additionally, the remote control portion **11** includes measurement means for measuring a biometrical signature of the authorized user of the vehicle. In one embodiment, the measurement means includes a microphone and a voice-recognition device that identify the user's voice. However, in preferred embodiments such as the one shown in FIG. **2**, the measurement means includes a fingerprint sensor CED that is located within the remote control portion **11** of the portable unit **103**. The active surface of the sensor CED is flush with an outer surface of the plastic portion **11** of the key.

Sensors suitable for such use are currently available in the form of monolithic integrated circuits at prices that are compatible with the market for automobile security systems. Further, these sensors are sufficiently precise, reliable, and compact for such an application. For example, one such sensor is manufactured by STMicroelectronics S.A. (Gentilly, France) under the reference STFP2015-50. This particular sensor has an active surface area of less than 2 cm^2 that includes nearly 100,000 detection cells arranged in a matrix. The entire active surface area is scanned eight times per second and serial digital data corresponding to the active surface scanning is delivered.

In the illustrated embodiment of the present invention, the fingerprint sensor CED is positioned beneath a second region **14** of the remote control portion **11** that is opposite the first region **13**. This allows the user's index finger **16** to contact the second region **14** containing the sensor while the thumb **15** contacts the first region **13** containing the switch when the plastic portion **11** of the key is clamped between these fingers. In some alternative embodiments, the sensor is positioned on the surface of the plastic portion **11** at the level of the first region **13** so that the user's thumb **15** is applied against the active surface of the sensor while also exerting pressure through the sensor to activate the push-button SW. While two mechanical layouts for the switch and sensor in the portable unit have been described, the present invention is not limited to only these specific structures. The elements of the portable unit can be laid out in any appropriate manner in accordance with design preferences by one of ordinary skill in the art, and thus specific structures are not described in detail.

FIG. **3** is a block diagram of a portable unit according to one embodiment of the present invention. As shown, the portable unit includes detection means for detecting active intervention by a user and producing an activation signal SA**1**. In one embodiment, the detection means is formed by a switch SW that has a first terminal connected to the positive terminal of a voltage source ST**1**, and a negative supply terminal of the voltage source is connected to ground. The activation signal SA**1** is delivered by the second terminal of the switch SW. Thus, the activation signal SA**1** is active (e.g., in the "1" state) when the switch SW is closed.

However, in the illustrated embodiment, the detection means includes the switch SW and a timer MS**1**. The first terminal of the switch SW is similarly connected to the voltage source ST**1**, but the timer MS**1** is connected to the second terminal of the switch and outputs the activation signal SA**1**. In this embodiment, the timer is a monostable circuit with a time constant T. The timer has the effect of holding the activation signal SA**1** in the active state for a specified time, which corresponds to the time constant T, after the closing of the switch SW. Thus, even if the pressure exerted on the switch by the user's thumb is stealthy, the activation signal is kept active for the specified time. This is especially advantageous when the switch is of a stealthy type such as a push-button.

Additionally, the portable unit includes measurement means CED, preferably in the form of a fingerprint sensor, for measuring a biometrical signature of the user and delivering a measurement signal SM**2**. The portable unit also includes generation means for generating the unlock signal SD when the activation signal SA**1** and the measurement signal SM**2** are produced within a specified temporal window and the measured biometrical signature corresponds to an authorized user. The generation means is in the form of a control circuit **20** having a first input E**1** that receives the activation signal SA**1** and a second input E**2** that receives the measurement signal SM**2** from the sensor CED.

The control circuit **20** also includes a microcontroller M**1** that has a memory DB**2** in which biometrical signatures of one or more authorized users are stored (e.g., the fingerprint of the thumb, index finger, or any other finger). Preferably, each biometrical signature is stored as a matrix of binary data and the biometrical signatures of each authorized user are stored in distinct areas of the memory DB**2** that are referenced by a user number. For example, five distinct areas could be reserved for storing the biometrical signatures of five different authorized users (e.g., the members of a family), with each user being fictitiously associated with a user number (e.g., 1, 2, 3, 4 or 5). It is also preferable to have the fingerprint sensor CED deliver the measurement signal SM**2** as a digital signal so that the data supplied to the second input E**2** of the control unit **20** can be directly exploited by the microcontroller M**1**. Otherwise, it is necessary to provide an analog-to-digital converter for the measurement signal.

The microcontroller M**1** is driven by a control program. When the data elements of the measurement signal SM**2** correspond to the data elements stored in one of the areas of the memory DB**2**, the microcontroller M**1** delivers an output signal OUT. The output signal OUT is then supplied to a transmission circuit ER**2** to prompt the transmission of the unlock signal SD, for example through an antenna, infrared diode, or electrical connection. In order to provide a clear illustration of the logical combination of the activation signal SA**1** and the measurement signal SM**2** within the control unit **20**, FIG. **3** shows an AND gate PL**2** that receives the activation signal SA**1** at one input and the measurement signal SM**2** at another input. The output of the AND gate PL**2** is supplied to an input i**1** of the microcontroller M**1**.

DOCKET ALARM

Explore Litigation Insights

Docket Alarm provides insights to develop a more informed litigation strategy and the peace of mind of knowing you're on top of things.

Real-Time Litigation Alerts

Keep your litigation team up-to-date with **real-time alerts** and advanced team management tools built for the enterprise, all while greatly reducing PACER spend.

Our comprehensive service means we can handle Federal, State, and Administrative courts across the country.

Advanced Docket Research

With over 230 million records, Docket Alarm's cloud-native docket research platform finds what other services can't. Coverage includes Federal, State, plus PTAB, TTAB, ITC and NLRB decisions, all in one place.

Identify arguments that have been successful in the past with full text, pinpoint searching. Link to case law cited within any court document via Fastcase.

Analytics At Your Fingertips

Learn what happened the last time a particular judge, opposing counsel or company faced cases similar to yours.

Advanced out-of-the-box PTAB and TTAB analytics are always at your fingertips.

API

Docket Alarm offers a powerful API (application programming interface) to developers that want to integrate case filings into their apps.

LAW FIRMS
Build custom dashboards for your attorneys and clients with live data direct from the court.

Automate many repetitive legal tasks like conflict checks, document management, and marketing.

FINANCIAL INSTITUTIONS
Litigation and bankruptcy checks for companies and debtors.

E-DISCOVERY AND LEGAL VENDORS
Sync your system to PACER to automate legal marketing.