US006927668B1

(12) **United States Patent**
Odle et al.

(10) **Patent No.: US 6,927,668 B1**
(45) **Date of Patent: Aug. 9, 2005**

(54) **PRINT ACCESS SECURITY SYSTEM**

(76) Inventors: **Richard Odle**, 5336 2nd Rd., Lake Worth, FL (US) 33461; **Gary Odle**, 14900 Stirrup La., West Palm Beach, FL (US) 33414; **Robert E. Henry**, 2461 Village Blvd., West Palm Beach, FL (US) 33409; **David Coriaty**, 144 Cocoplum La., Royal Palm Beach, FL (US) 33411

(*) Notice: Subject to any disclaimer, the term of this patent is extended or adjusted under 35 U.S.C. 154(b) by 218 days.

(21) Appl. No.: **09/718,530**

(22) Filed: **Nov. 21, 2000**

(51) **Int. Cl.**[7] **G05B 19/00**

(52) **U.S. Cl.** **340/5.53**; 340/5.52; 340/5.51; 340/5.64; 340/5.61; 340/5.21; 340/5.27; 340/5.2; 340/5.1; 340/426.28; 340/426.36; 382/124

(58) **Field of Search** 340/5.53, 5.52, 340/5.61, 5.72, 5.21, 5.27, 5.64

(56) **References Cited**

U.S. PATENT DOCUMENTS

5,325,442 A	*	6/1994	Knapp	382/124
5,448,659 A		9/1995	Tsutsui et al.	
5,523,746 A	*	6/1996	Gallagher	340/825.31
5,598,474 A	*	1/1997	Johnson	713/186
5,633,947 A	*	5/1997	Sibbald	382/124
5,686,765 A		11/1997	Washington	
6,100,811 A	*	8/2000	Hsu et al.	340/825.31

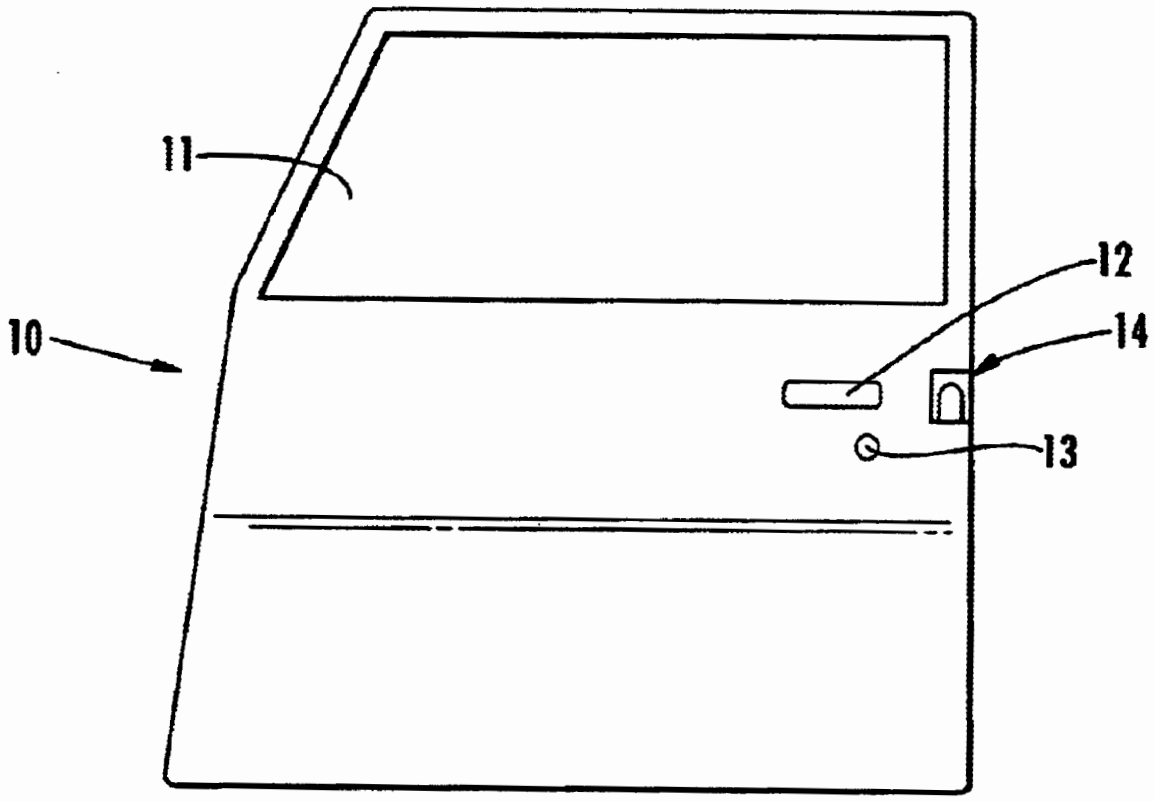
* cited by examiner

Primary Examiner—Michael Horabik
Assistant Examiner—Vernal Brown
(74) *Attorney, Agent, or Firm*—McHale & Slavin PA

(57) **ABSTRACT**

A fingerprint enrollment and verification module is connected to the electrical circuit of a vehicle to prevent operation of the vehicle by unauthorized users. The module has a sensor that creates a template of a fingerprint when a finger is placed on the module. The module has a flash memory to store enrolled templates and a verification step. After a fingerprint has been enrolled in the module, any operation of that vehicle is possible only after the user's fingerprint is verified to match the enrolled template.

13 Claims, 3 Drawing Sheets



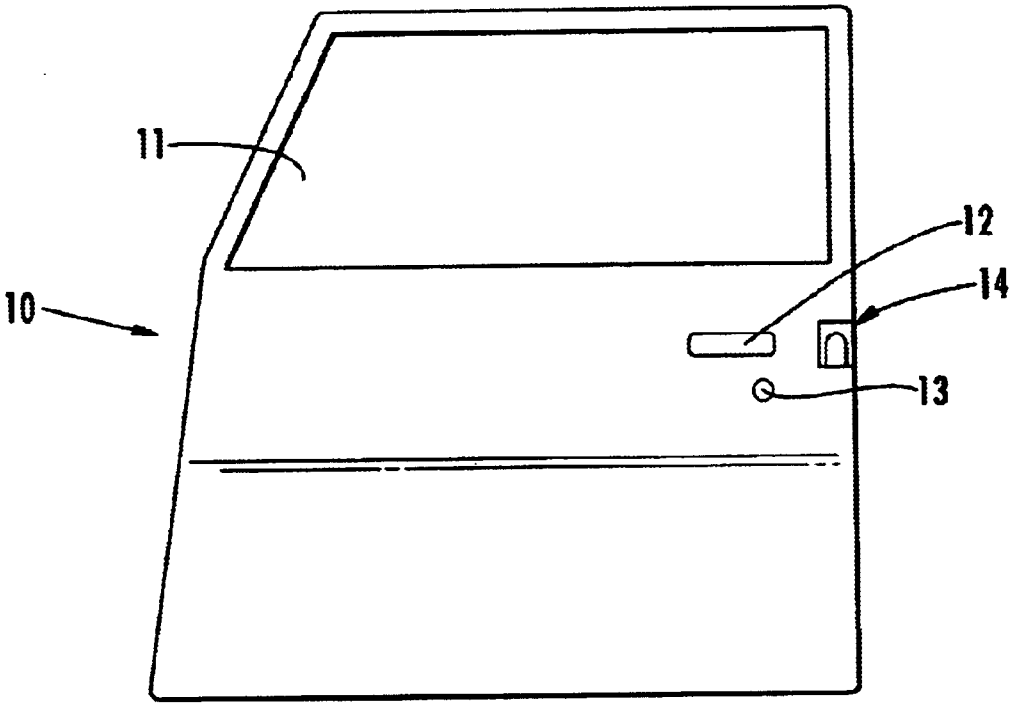


FIG. 1

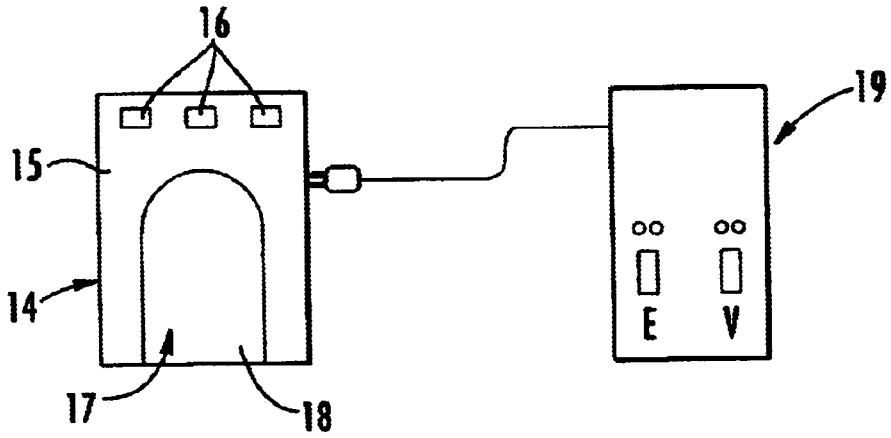


FIG. 2

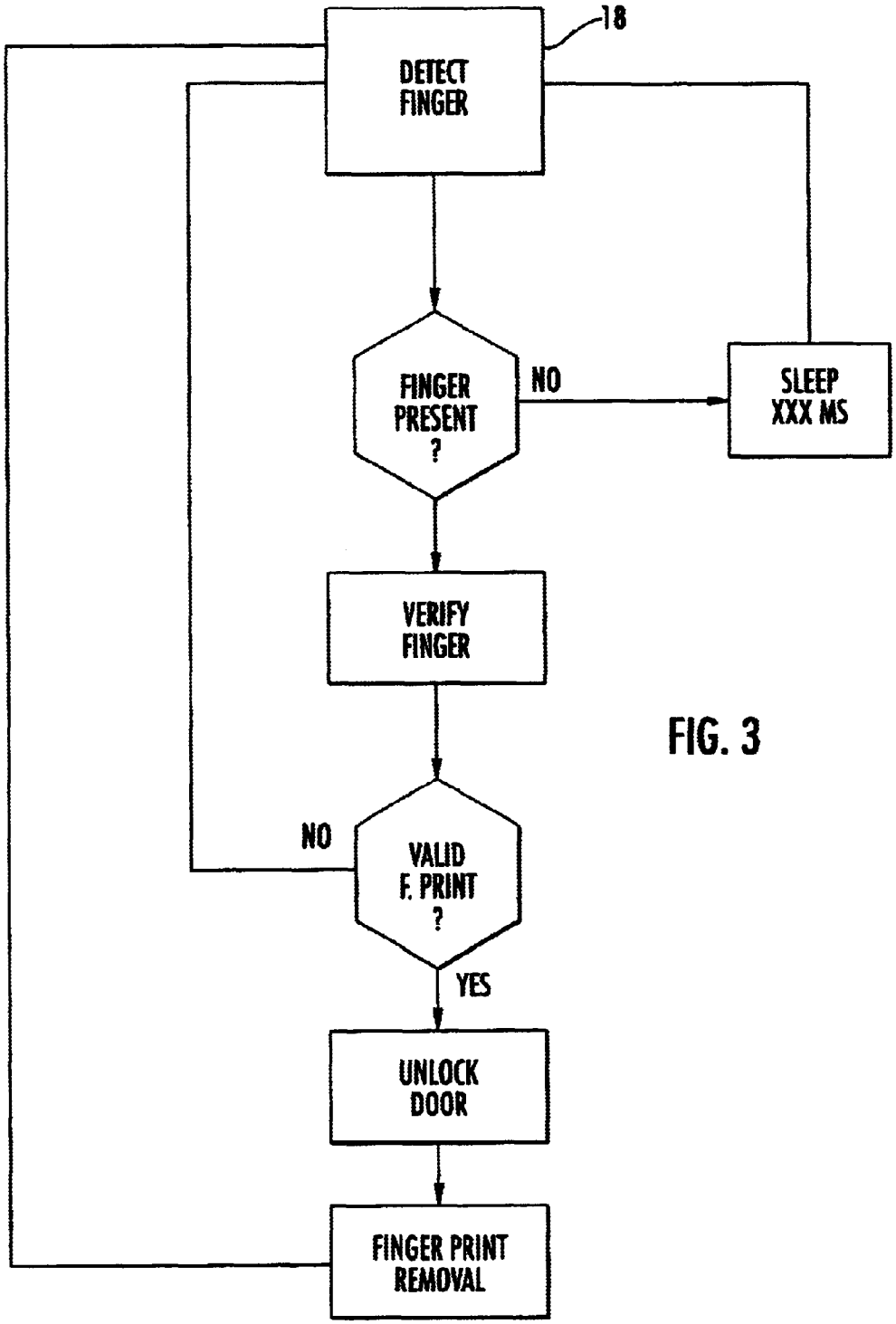


FIG. 3

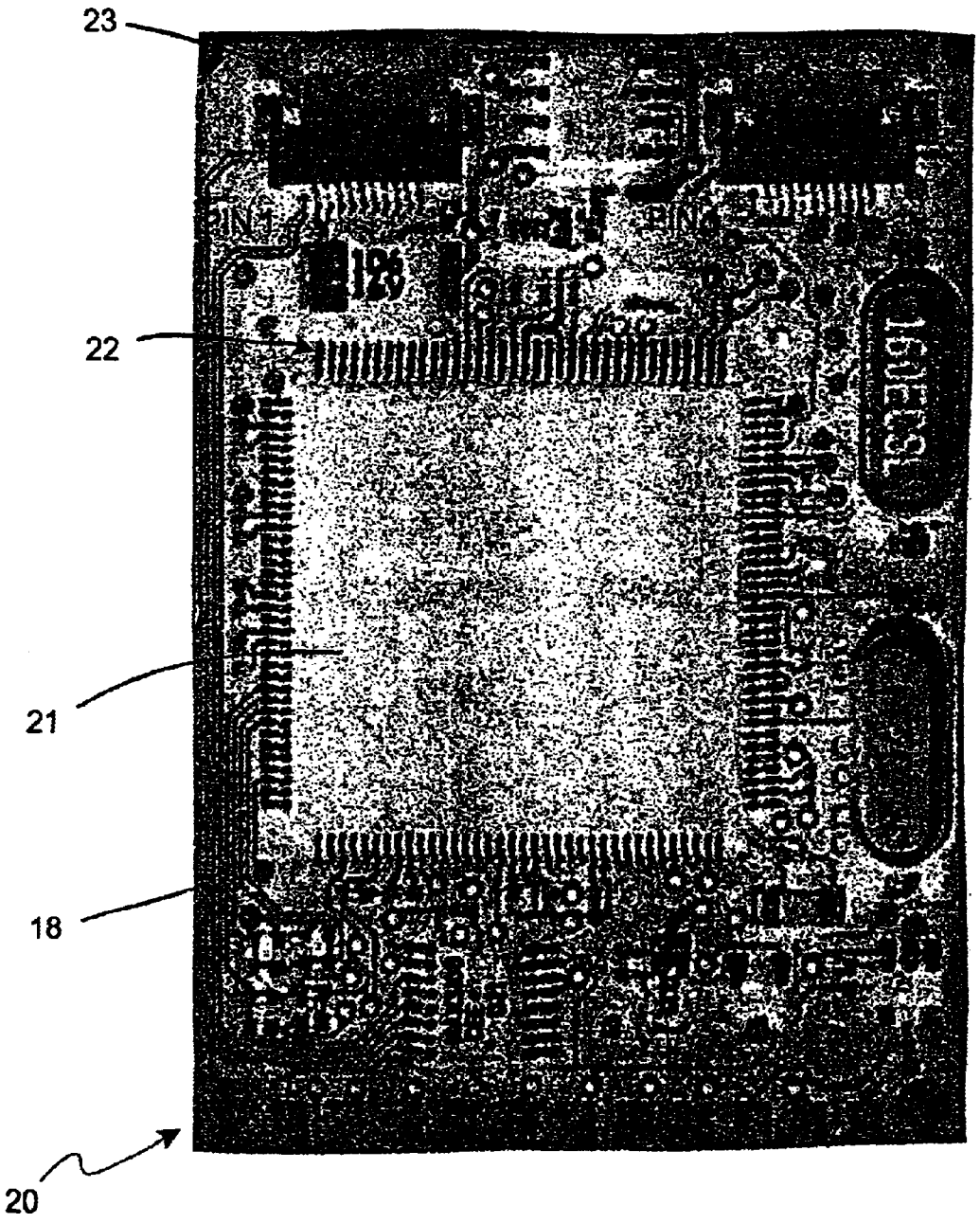


FIG. 4

PRINT ACCESS SECURITY SYSTEM

FIELD OF THE INVENTION

This invention is related to security systems and, particularly, to identity recognition through comparison of an image of a finger and a stored template. The security system may be used to gain entry and to energize the systems of a vehicle.

BACKGROUND OF THE INVENTION

It is generally accepted that vehicles are items considered highly transportable by nature. Vehicles may include cars, trucks, buses, vans, construction equipment, water craft, motorcycles, airplanes, golf carts, snowmobiles, and, generally, anything that is capable of self powered mobility. Common to such vehicles is a key or keys for security of the interior and operation of the systems. However, a key can be used by anyone and is easily duplicated, rendering the security of the vehicle vulnerable to unauthorized use.

Some automobile manufacturers utilize different keys for different functions. For instance, General Motors, for many years, employed one key for unlocking the doors and trunk and a second key for starting the engine. However, anyone who had access to the keys would be able to operate the vehicle. More recently, GM has made a key system that includes a microchip. These keys are extremely difficult to duplicate however, there are specialized vendors authorized to make copies. This program also degrades the security system.

Other security systems are in use. For instance, Ford Motor Company employs a keyless entry system which allows an individual to have a numeric or alphabetic code programmed into the keyless entry and a memory circuit stores the code for activation of the door locks upon entry of a correct code sequence. The code is typically maintained by the manufacturers as well as the local dealer. Thus, access to the code can be obtained by a number of people thereby degrading the efficacy of the system.

Currently, most automobile companies and after market suppliers offer small electronic door openers which cooperate with the electrical system in the auto to unlock doors. These devices are a convenience and may be overridden by a key. As such, these devices do not add any security to the system.

In addition to controlling entry to vehicles, there are devices that will cause the engine to start and remotely operate various other electrical systems in the vehicle. However, for security purposes, these devices usually require a key for entry into the vehicle.

In both the electronic door locking devices and the electronic engine starters, there is a very real risk that the frequency used in the devices may be captured by unauthorized persons using scanners or like devices. Also, these devices and their associated circuits are over-ridden by the use of the key. Therefore, anyone with the frequency code or a key or both can operate the vehicle.

However, what is lacking in the art is a stand alone security system that is hard wired into the vehicle and cannot be duplicated by copying of codes or keys. Further, what is lacking in the prior art is a system that is programmable, only, by the owner or authorized operator of the vehicle without the possibility of unauthorized duplication.

Also what is lacking in the prior art is a mechanism for

DESCRIPTION OF THE PRIOR ART

U.S. Pat. No. 5,686,765 to Washington teaches a system for preventing unauthorized or unlicenced persons from using an automobile. In one embodiment, the system has a remote component that receives and compares physiological identification entered at the vehicle. If the data match, the ignition system of the vehicle is energized for normal operation. In another embodiment, the operator data is compared to a particular time frame for operation by that operator during specified times. And in another embodiment, the system requires subsequent data input to ensure that the authorized driver remains the current operator. There is also provision for a bar code reader of an encoded driver's licence and/or reading the signal of an electronic tether. The physiological identification data may be generated by a fingerprint reader or an eyeball scan. This requires a scan and a transmission to a remote computer.

U.S. Pat. No. 5,448,659 to Hiroshi teaches the use of a card-shaped waveguide-type image transmission device to scan, read and transmit fingerprint data. Again, the identity input is a fingerprint scan.

The fingerprint scanning technology of these prior art devices produces a representation of the grooves and ridges of the surface of a finger. Therefore, these scans are highly susceptible to errors caused by extraneous matter such as dirt, grease, paint, calluses, etc. on the fingers of the prospective users.

SUMMARY OF THE INVENTION

Accordingly, it is an objective of the instant invention to provide a system to secure any vehicle from operation by an unauthorized user.

It is a further objective of the instant invention to provide a system to identify and authenticate a potential user of a vehicle by fingerprint information. The system is referred to as Fingerprint Enrollment and Verification Module, FEVM.

It is yet another objective of the instant invention to. provide a stand alone system hard wired into the electrical system of a vehicle to authorize and/or control any vehicle function by an operator placing a finger on a sensor.

Other objects and advantages of this invention will become apparent from the following description taken in conjunction with the accompanying drawings wherein are set forth, by way of illustration and example, certain embodiments of this invention. The drawings constitute a part of this specification and include exemplary embodiments of the present invention and illustrate various objects and features thereof.

BRIEF DESCRIPTION OF THE FIGURES

FIG. **1** is a perspective of a door of an automobile;

FIG. **2** is a close up perspective of the FEVM housing shown in FIG. **1**;

FIG. **3** is a flow chart of the operative steps of the fingerprint enrollment and verification module, FEVM; and

FIG. **4** is a pictural representation of the finger print sensor.

DETAILED DESCRIPTION OF THE INVENTION

The term, "operation," refers to any initiation of any system on a vehicle, to include a range of commands from

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.