



166166

BIOMETRIC IMMOBILIZER FOR AUTOMOBILES**BACKGROUND OF THE INVENTION**

G00002

(a) Technical Field

The present invention relates to biometric immobilizer, and in particular, an immobilizer employing biometrics for use in all kinds of automobiles. The biometric immobilizer integrates a generic immobilizer system to gather with personal biometric parameters for the protection and authorized access to immobilization function of automobiles.

(b) Description of the Prior Art

An immobilizer is a control unit protecting a motor vehicle against unauthorized use or allows the access of a motor vehicle by the rightful owner. US Patent No. 5,675,490 entitled " Immobilizer For Preventing Unauthorized Starting Of A Motor Vehicle And Method For Operating The Same" issued to Anton Bachhuber on 7 October 1997 discloses an immobilizer including a test unit, control devices connected through a data line to the test unit, and at least one ignition key having a transponder. When the ignition key is actuated, the test unit transmits a request signal through the data line to all of the control devices, which respond thereto by transmitting back identification codes which are compared with desired codes. The test unit prevents starting of the motor if less than a prescribed number of control devices reply with their identification code. The test unit enables all of the control devices if at least the prescribed number of control devices reply with their identification code word, in the event of interrogation.

US Patent No. 6,181,026 entitled " Vehicle Immobilizer System For Electronic Engine Control" issued to William David Treharne on 30 January 2001 discloses the monitoring engine conditions using various sensors to determine whether the immobilizer should be rearmed. The immobilizer disarms when an

authorized security code is received from a transponder during an attempt to start the engine. The controller for the engine immobilizer monitors engine receiving sensors and switches to the armed state if the engine-running sensors indicate that the engine is not running even though the ignition switch has not been detected to have been put in the position.

None of the disclosed patent relates to the application of biometrics and immobilizer. The conventional art does not disclose the use of a secure communication protocol within the system. To overcome the above drawbacks, the biometric immobilizer for automobiles make use of biometrics and immobilizer technologies together with a secure communication protocol being built within the biometric system for generation of secure communication vector key for authorized access to various function units. The present biometric immobilization also has an internal built in proprietary data protection protocol and procedure to ensure all information within the memory storage being encrypted by personal biometrics information generated key is also one of the key code technologies within the biometric fingerprint authorization unit system.

SUMMARY OF THE INVENTION

Embodiments of the present invention seek to provide a biometric immobilizer for automobiles, wherein the immobilizer is designed employing biometrics and immobilizer technologies. In embodiments of the present invention, a secure communication protocol is built within the biometric immobilizer for generation of secure communication vector key for authorized access to various function units installed in automobiles. In addition, internal built-in proprietary data protection protocol and procedure to ensure all information within the memory storage is encrypted by personal biometrics information "generated" key.

According to one aspect of the present invention, there is provided a biometric immobilizer for automobiles comprising: a bio-fingerprint authentication unit including an embedded fingerprint biometrics processing unit, a sensor capable of capturing human fingerprint biometric pattern, and a flash memory able to store biometric data and information, wherein

the bio-fingerprint authentication unit is capable of biometrics verification; an embedded immobilizer controller communicating with the bio-fingerprint authentication unit to perform biometric fingerprint enrollment, biometric fingerprint verification operation, and bio-data management, wherein the embedded immobilizer controller establishes a secure communication protocol between the embedded immobilizer controller and the bio-fingerprint authentication unit to prohibit illegal access to the bio-fingerprint authentication unit, and generates a secure communication key between the bio-fingerprint authentication unit and the embedded immobilizer controller; and a driver door unit for sensing a door opening status of a driver door of the automobile; wherein the embedded immobilizer controller changes from a driving mode into a hijacking mode in response to detection of the driver door open status during the driving mode, and instruct the bio-fingerprint authentication unit to detect for an authorized fingerprint within a detection period.

In an embodiment, the embedded immobilizer controller, in response to failure to detect the authorized fingerprint within the detection period, may activate a first warning mechanism and instruct the bio-fingerprint authentication unit to detect for an authorized fingerprint within a further detection period.

In another embodiment, the embedded immobilizer controller, in response to failure to detect the authorized fingerprint within the further detection period, may activate a second warning mechanism and instruct the bio-fingerprint authentication unit to detect for an authorized fingerprint within another detection period.

In another embodiment, the embedded immobilizer controller, in response to failure to detect the authorized fingerprint within the another detection period, may instruct cutting off the engine of the automobile.

In another embodiment, the biometric immobilizer for automobiles may further comprises a proprietary data encryption scheme for safe keeping of biometric data and information within the memory storage for commanding the embedded immobilizer controller to operate.

In another embodiment, the biometric fingerprint authentication unit may have a biometrics enrollment-time not more than 100 msec per user, and not more than 5 users are assigned for authority access right.

In another embodiment, the sensor contained within the bio-fingerprint authentication unit may include capacitive or electric-field sensing devices, or optical sensor which are capable of capturing human fingerprint biometric pattern.

In another embodiment, the embedded immobilizer controller unit may further include a micro-controller system which communicates with the biometric fingerprint authentication unit.

In another embodiment, the biometric immobilizer of the above aspect may further comprise sub-functional units controlled by embedded authentication unit.

In another embodiment, a code may be stored within the sub-functional units with encryption for authentication.

In another embodiment, the sub-functional units may include starter motor control unit, ignition coil control.

BRIEF DESCRIPTION OF THE DRAWINGS

FIG. 1 is a block diagram showing the biometric immobilizer for automobiles in accordance with the present invention.

FIG. 2 is a schematic view showing the 12 sub-functional units which related to the biometric immobilizer in accordance with the present invention.

FIG. 3 is a flowchart showing the functional flows of biometric fingerprint authentication process and secure command set generation between the biometric fingerprint authentication unit and the embedded immobilizer controller in accordance with the present invention.

DETAILED DESCRIPTION OF THE PREFERRED EMBODIMENT

The present invention will be described with regard to the accompanying drawings which assist in illustrating various features of the invention.

In accordance with a preferred embodiment of the present invention, a biometric immobilizer 10 is provided for use in a vehicle. The biometric immobilizer 200 comprises a biometric fingerprint authentication unit (BAU) 20 and an embedded immobilizer controller (EIC) 30, as shown in FIG. 1.

The BAU 20 contains an embedded fingerprint biometrics processing unit 22 and a fingerprint sensor 24, and a bio-data storage unit 26, such as a flash memory which is a storage device capable of storing biometric data and information. The fingerprint sensor 24 can be a capacitive or electric-field sensing device or optical sensor or the like which is capable of capturing or reading human fingerprint biometric pattern. In addition, an LED indicator 28 is provided to the BAU 20 to show the confirmation of authentication.

In accordance with the present invention, built-in proprietary data encryption scheme for biometric data and information safe keeping within the memory storage is also provided to the BAU 20 and the scheme is used for commanding the EIC 30 to effectively operate in a predefined and/or described operation set by the user.

The BAU 20 is also provided with a biometrics verification and system access time (prescribed enrollment-time), preferably not exceeding 50 msec or any time suitable for the operation of the immobilizer 200. Generally, the enrollment-time

should not more than 100 msec per user, and less than 5 users are assigned for authority access right to the immobilizer 200. However, the prescribed enrollment-time and number of users are variable parameters which can be modified or adjusted in the course of manufacturing. A built-in proprietary data encryption scheme for data and information safekeeping is incorporated into the BAU 20.

In accordance with the present invention, the EIC 30 is a micro-controller system which is employed to communicate closely with the BAU 20 to command and communicate with the BAU 20 to perform biometric fingerprint enrollment, to command and communicate with the BAU 20 to perform fingerprint verification operation, and to command and communicate with the BAU 20 to perform bio-data management system.

Referring again to FIG. 1, a secure communication protocol interface 32 is provided to the EIC 30 so that the EIC 30 can establish a secure communication protocol between EIC 30 and BAU 20 to ensure no illegal access to the BAU 20 for any un-authorized access to the bio-data stored in the bio-data storage unit 26 within the BAU 20. The EIC 30 generates a secure communication key between the BAU 20 and the EIC 30, and the function of such secure communication key is for the controlling and commanding of a plurality of sub-functional operations within the access control of the EIC 30.

As mentioned earlier, the embedded secure communication protocol is a proprietary communication structure between the BAU 20 and the EIC 30. This communication structure establishes a secure data communication link between the BAU 20 and the EIC 30 so as to prevent any illegal access to the bio-data storage unit 26 of the BAU 20. Generally the data communication link is based on factory coded sequence spread with a master bio-fingerprint generated random number. The master bio-fingerprint generated random number is generated by a master bio-fingerprint enrollment.

Referring to FIGS. 1 and 2, the biometric immobilizer 200 of the present invention further comprises a plurality of sub-functional units 80, including starter motor control unit 42, brake switch unit 43, ignition key unit 44, override switch unit 45, siren unit 46, driver door and other doors unit 47, LED display & buzzer unit 48, loop antenna unit 49, power supply unit 50, cutoff valve unit 51, fuel pump unit 52, ignition coil unit 53. These sub-functions units 80 are controlled by the EIC 30, but the BAU 20 issues a "Authority Key or Access Right" to access to the sub-functional units 80, and such authority access command is a coded sequence and stored within the sub-functional units 80 with encryption for authentication.

In the present invention, the starter motor control unit 42 enables the operation of the engine and hence the automobile motor starts to run. The operation of the automobile motor is only initiated upon receiving a match command sequence from the EIC 30, which in term authorized by the BAU 20.

The ignition coil control unit 53 activates the ignition of the engine of the automobile. Such operation is only initiated upon receiving a match command sequence from the EIC 30, which in term authorized by the BAU 20.

The fuel pump control unit 52 provides fuel pump to the engine operation, and such operation is only activated upon receiving a match command sequence from EIC 30, which in term authorized by the BAU 20.

The cutoff valve unit 51 is used to disable or shut down the valve operation within the automobile. Such activity is only activated upon receiving a match command sequence from the EIC 30, which in term authorized by the BAU 20.

The power supply control unit 50 constantly provides power to the immobilizer 200 of the present invention. Such activity is only available or activated upon

receiving a match command sequence from the EIC 30, which in term authorized by the BAU 20.

The loop antenna unit 49 energizes a remote receiver (not shown) of a keyless system for door access operation. Such operation will be disabled if a non-match sequence from the EIC 30 is given, and the operation is authorized by the BAU 20.

The LED display and buzzer control unit 48 provides feedback on armed and unarmed system, and such activity will not be functioned if there is non-match command sequence from the EIC, which in term authorized by the BAU 20.

The driver door and other doors control unit 47 is used to sense the door opening status, and hence activates the subsequent action in the immobilizer 200, such as automatic armed or unarmed. Such activity will not be functioned if there is no match command sequence form EIC 30, which in term authorized by the BAU 20.

The siren control unit 46 activates the siren unit for any unauthorized access or imperfect operation of automobile. Siren activity will be activated if there is no match command sequence from the EIC 30, which in term authorized by the BAU 20.

The override switch unit 45 provides overriding function for non-biometric access. (give example of non-biometric access) Such function will only be activated upon a match command sequence from the EIC 30, which in term authorized by the BAU 20.

The ignition key unit 44 provides relevant logic control and access right to activate ignition key sensor and the sensor will only be activated only if there is a

match command sequence from the EIC 30, which in turn authorized by the BAU 20.

The brake switch unit 43 is responsible to deactivate the brake switch for any unauthorized access or imperfect operation of automobile. Such activity will be activated if there is no match command sequence from the EIC 30, which in turn authorized by the BAU 20.

FIG. 3 is a flowchart showing functional flows of bio-fingerprint authentication process and secure command set generation between the BAU 20 and the EIC 30. In order to arm the immobilizer system of the present invention from the drive state, the ignition key is turned to "OFF" position before alight the automobile. The user places his fingerprint on the fingerprint sensor 24, and awaits confirmation LED indicator 28 to appear. The LED indicator 28 indicates by a color for instance green and blinking. Before the exit delay time elapses, for instance, the delay time is set at 30 sec, and the timing is programmable or fixed during production, alighting from the automobile and close all the doors properly. The buzzer unit 48 beeps for approximately 10-15 sec before the time out, and similarly this timing is programmable or fixed. In this case, when the time out, the system is armed. The LED indicator 28 should now blink slowly with other different color such as red to indicate the system is now armed. If the doors of the automobile are not properly closed, the system will chirp for a plurality of times when the system enters the armed state. The times of chirp can be set.

As shown in FIG. 3, in order to disarm the system with the biometric fingerprint unit, in the armed state, once any of the doors is opened, the system will start fingerprint identification 310 sequence for about 40-60 second. During this time frame, the automobile can be started but cannot be driven as the brake control unit 43 is now deactivated. At 320, the bio-data of the user is verified. Only when authentication process is successful, and valid command set has been issue to various sub-functional units 80 via EIC 30, the automobile will operate

normally. However, if the authentication process is failed at 330, and hence invalid command set has been sent, and the automobile ignition will go off and the automobile will not functioning. In this case, there is a warning period of approximately 15-20 seconds before the siren unit 46 is activated. The user has sufficient reaction time to put a correct fingerprint for correct authentication. When the warning period of 15-20 seconds is out, the siren unit 46 will be activated and the system goes to "trip stage". In this trip stage, the engine of the automobile will be cut off, the buzzer beeps rapidly and the LED blinks rapidly, and the siren will be whirling. In this case, if the system is to reset, the user must remove the key sensor unit, and place the correct fingerprint onto the fingerprint sensor and press the brake pedal of the automobile. At this instance, the system will get back to the identification stages and restart the cycle again. When the authentication process is successful at 330, encryption pointers 340 have to be generated. In accordance with the preferred embodiment, the pointers has an "indirect address method to store an encryption key, and the pointers are closely related to the fingerprint authentication. Hence the encryption key is not a fixed key for all and the encryption key is a key related to a fingerprint per se, and only the same fingerprint can read the particulars store in a flash memory. With the encryption pointers 340, the system in accordance with the present invention is able to retrieve the encryption key from a biometric memory, and hence the encryption key is not stored into the data flash memory. Hence even if the flash memory is removed for hard machine reading, there is nothing to read by any unauthorized parties.

In accordance with the present invention, the factory code 360 is another set of key for the manufacturer to control the production, and the factory key is the only protection key to the system when the key is first produced from the factory, and the user will need to register with the system when the key is first used in the device and is added in the user biometric key.

The security key generation (pronominal appending) 370 is a proprietary method for embedding both the biometric key and the factory key to form a final key code for the encryption of data stored and retrieve from the system. Data encryption/decryption process 380 is the encryption process for the data, and a combination key (polynomial generated master key) is used for the encryption algorithm. The flash memory read/write is the procedure for reading and writing data onto the flash memory.

When the automobile need servicing or maintenance, the system can be set into "Service Mode" where in this mode, the biometric fingerprint authentication process is bypassed. To enter the "Service Mode", from the armed mode, the system is disarmed, and following by turn on the ignition key N time (N is preferably 3) in succession within 15 seconds. The status LED will turn to a solid indicative color, such as solid orange color, and now the system is at "Service Mode". In accordance with the present invention, the biometric immobilizer will be stay in the "Service Mode" even when the battery of the immobilizer is removed and all the bio-information is secured and protected within the biometric immobilizer system.

When the system is at the Service Mode, the user must place the correct fingerprint onto the fingerprint reader 24, and turn on the ignition, press the brake pedal within 10-15 second. The LED status should now turn to some indicative "Blinking Color" such as blinking orange for 10 seconds and then stop, indicating that the system in now exit from the Service Mode, and this is further confirmed by a long beep sound from the buzzer.

If the user is enrolled from Factory Code, the user places the fingerprint on the fingerprint sensor 24 and turns on the ignition key for a prescribed time (for instance 5 time). The status LED turns to solid indicative color, for instance green color, and the BAU 20 will now process the fingerprint data and create the relevant database for future authentication. A successful enrollment will be

indicated by a blinking LED color, e.g., blinking green and following by a long beep from the buzzer. A failed enrollment will be indicated by a solid LED color, e.g., red and a short beep buzzer. On failure enrolment, and to proceed for further enrolment, the user must re-start the entire enrollment cycle.

From disarmed mode, the user is able to enroll additional users to get access to the automobile. In this case, the master user needs to place the fingerprint on the fingerprint sensor and turns on the ignition key for a prescribed time (for instance 5 time), and at the same time, press on the brake pedal within 10 to 15 seconds. Now status LED gives indicative solid color, for instance, solid green, and indicating that now new user is ready to place the finger on the fingerprint sensor.

Upon successful processing and database generation, status LED will indicate a blinking LED color, e.g., blinking green and following by a long beep from the buzzer. A failed enrollment will be indicated by a solid LED color, for instance, red and a short beep buzzer. On failure enrolment, if the user is to proceed for further enrollment, the user must re-start the entire enrollment cycle.

In accordance with the present invention, for every new user enrollment, the master user fingerprint authentication is required. The total number of authorized users for the biometric immobilizer system is limited to 8 users. However, this limitation is programmable and is set in production.

In another preferred embodiment, during the driving mode, when the driver is forced to leave the automobile, for instance, the vehicle is hijacked, the system of the present invention is activated. If the driver door is opened in the driving state, the system will be initialized and awaiting an authorized fingerprint to be detected within 30 seconds. In other words, in this preferred embodiment, if the driver is forced to leave the vehicle, and the engine is still running, and if the system does not detect an authorized fingerprint, the system will be activated and starts the

procedure of anti-hijacking. After the first 30 seconds failure to identify the authorized fingerprint, the system will start warning short beeps and hazard lights flashing to provide warning to driver to process authorized fingerprint on the fingerprint sensor 24. For the next 30 seconds, if an authorized fingerprint is still not identified the LED indicator 28 flashes and then following by a long beep buzzer. In the next 30 seconds, if an authorized fingerprint is still not identified, siren starts to whirl, and in the next 30 seconds, the engine will cut off.

During the anti-hijacking procedure, as long as an authorized fingerprint is identified, the anti-hijacking procedure will be restored and return to the normal driving mode. However, when the engine is cut off as a result of the completing of the anti-hijacking procedure, authorized driver can reset the vehicle to normal driving mode by first off the ignition key and then turn on the ignition key again and press the brake pedal and provide an authorized fingerprint on the fingerprint sensor 24 and the BAU 20 simultaneously. This will reset the system to a normal state.

It will be appreciated by persons skilled in the art that numerous variations and/or modifications may be made to the invention as shown in the specific embodiments without departing from the spirit or scope of the invention as broadly described. The present embodiments are, therefore, to be considered in all respects as illustrative and not restrictive

CLAIMS

1. A biometric immobilizer for an automobile, comprising:
 - a bio-fingerprint authentication unit including an embedded fingerprint biometrics processing unit, a sensor capable of capturing human fingerprint biometric pattern, and a flash memory able to store biometric data and information, wherein the bio-fingerprint authentication unit is capable of biometrics verification;
 - an embedded immobilizer controller communicating with the bio-fingerprint authentication unit to perform biometric fingerprint enrollment, biometric fingerprint verification operations, and bio-data management, wherein the embedded immobilizer controller establishes a secure communication protocol between the embedded immobilizer controller and the bio-fingerprint authentication unit to prohibit illegal access to the bio-fingerprint authentication unit, and generates a secure communication key between the bio-fingerprint authentication unit and the embedded immobilizer controller; and
 - a driver door unit for sensing a door opening status of a driver door of the automobile;
 - wherein the embedded immobilizer controller changes from a driving mode into a hijacking mode in response to detection of the driver door open status during the driving mode, and instructs the bio-fingerprint authentication unit to detect for an authorized fingerprint within a detection period.
2. The biometric immobilizer as claimed in Claim 1, wherein the embedded immobilizer controller, in response to failure to detect the authorized fingerprint within the detection period, activates a first warning

mechanism and instructs the bio-fingerprint authentication unit to detect for an authorized fingerprint within a further detection period.

3. The biometric immobilizer as claimed in Claim 2, wherein the embedded immobilizer controller, in response to failure to detect the authorized fingerprint within the further detection period, activates a second warning mechanism and instructs the bio-fingerprint authentication unit to detect for an authorized fingerprint within another detection period.

4. The biometric immobilizer as claimed in Claim 3, wherein the embedded immobilizer controller, in response to failure to detect the authorized fingerprint within the another detection period, instructs cutting off the engine of the automobile.

5. The biometric immobilizer as claimed in any one of the preceding claims, further comprising a proprietary data encryption scheme for safe keeping of biometric data and information within the memory storage for commanding the embedded immobilizer controller to operate.

6. The biometric immobilizer as claimed in any one of the preceding claims, wherein the biometric fingerprint authentication unit has a biometrics enrollment-time and is not more than 100 msec per user, and not more than 5 users are assigned for authority access right.

7. The biometric immobilizer as claimed in any one of the preceding claims, wherein the embedded immobilizer controller unit further includes a micro-controller system which communicates with the biometric fingerprint authentication unit.

8. The biometric immobilizer as claimed in any one of the preceding claims, wherein the sensor contained within the bio-fingerprint authentication unit includes capacitive or electric-field sensing devices, or optical sensor which are capable to capture human fingerprint biometric pattern.
9. The biometric immobilizer as claimed in any one of the preceding claims, further comprising sub-functional units controlled by embedded authentication unit.
10. The biometric immobilizer as claimed in claim 9, where a coded sequence is stored within the sub-functional units with encryption for authentication.
11. The biometric immobilizer as claimed in claims 9 or 10, wherein the sub-functional units include starter motor control unit, ignition coil control