



(51) International Patent Classification:

G01D 3/08 (2006.01)

G06F 7/00 (2006.01)

B60R 25/10 (2013.01)

(21) International Application Number:

PCT/IN2021/050112

(22) International Filing Date:

04 February 2021 (04.02.2021)

(25) Filing Language:

English

(26) Publication Language:

English

(30) Priority Data:

202041005015

05 February 2020 (05.02.2020)

IN

(71) Applicant: **SUNDARAM, Rajarajeswari** [IN/IN]; 1 D, L Block, Rite Choice Surya Apartments, 18 Avenue, 86 Street, Ashok Nagar, Tamil Nadu, Chennai 600 083 (IN).

(72) Inventors: **SUBRAMANIAN, Sundaram**; 1 D, L Block, Rite Choice Surya Apartments, 18 Avenue, 86 Street, Ashok Nagar, Tamil Nadu, Chennai 600 083 (IN). **KRISHNASWAMY, Srikanth**; C Block, 2nd Floor, Flat No 4, Gemini PARSN Apartments, No 599, (New No 448), Anna Salai, Tamil Nadu, Chennai 600 006 (IN).

(74) Agent: **RAJA RAVINDRAN, Sudhir** et al.; Altacit Global, C2-A, Industrial Estate, Guindy, Tamil Nadu, Chennai 600 032 (IN).

(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, BN, BR, BW, BY, BZ, CA, CH, CL, CN, CO, CR, CU, CZ, DE, DJ, DK, DM, DO,

DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, GT, HN, HR, HU, ID, IL, IN, IR, IS, IT, JO, JP, KE, KG, KH, KN, KP, KR, KW, KZ, LA, LC, LK, LR, LS, LU, LY, MA, MD, ME, MG, MK, MN, MW, MX, MY, MZ, NA, NG, NI, NO, NZ, OM, PA, PE, PG, PH, PL, PT, QA, RO, RS, RU, RW, SA, SC, SD, SE, SG, SK, SL, ST, SV, SY, TH, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, WS, ZA, ZM, ZW.

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

Declarations under Rule 4.17:

— as to the identity of the inventor (Rule 4.17(i))

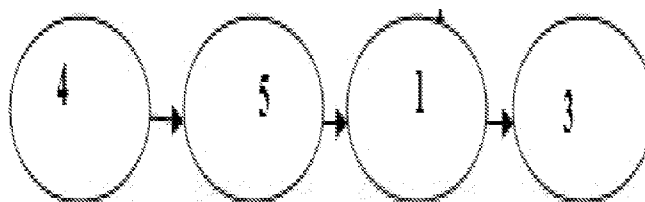
Published:

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

— in black and white; the international application as filed contained color or greyscale and is available for download from PATENTSCOPE

(54) Title: ELECTRONIC SIGNAL BASED AUTHENTICATION SYSTEM AND METHOD THEREOF

FIGURE 1:



(57) Abstract: The present invention relates to the field of authentication systems. More particularly, it relates to electronic signal-based authentication system. It relates to authentication system which integrates into devices in electro-mechanical systems without interfering with any of its internal functions and hence provides ease of maintenance and upgradability. The present invention relates to prevention of un-authorized usage of electro-mechanical systems. To demonstrate the signal-based authentication, the vehicle is chosen as a candidate system, since vehicles are part of daily life and has widespread usage all over the world. As an embodiment of electro-mechanical device, the present invention covering vehicle anti-theft authentication system, suggests electronic signal intervention/modification unit [5] comprising of one or more microprocessors with embedded computer instructions, input – output ports, networking units, communication units, display units resulting in a highly secure authentication mechanism to prevent vehicle from being burgled and driven away.



ELECTRONIC SIGNAL BASED AUTHENTICATION SYSTEM AND METHOD THEREOF

FIELD OF THE INVENTION:

5 The present invention relates to the field of authentication systems. More particularly, it relates to the electronic signal-based authentication system. It relates to an authentication system which integrates into devices in electro-mechanical systems without interfering with any of its internal functions and hence provides an ease of maintenance and upgradability. More particularly, the present invention relates to prevention of un-authorized usage of electro-mechanical systems.

10

BACKGROUND OF THE INVENTION:

There are a large number of costly equipments whose functionality is critical in nature. The entry into the places where these equipments are located is controlled by a variety of access control mechanisms. However, not all these access control mechanisms prevent abuse / misuse of these systems, since someone can bypass these access control systems. There is a need to incorporate an authentication system which is built into the natural functioning of the system and is fool proof. This way, even if a person gains access to operating the system and is knowledgeable about the operation of system, cannot operate the system, if he is not authorized. By providing such an authentication, we can, not only prevent unauthorized usage, but also collect vital information regarding the usage of the equipment viz., who has used for how long, what problems has occurred during the usage by a person, attempts at unauthorized access with time stamp, system shutdown event with time stamp etc. and such data collection is authentic as these are collected at source and does not involve any manual operation and can be used for variety of purposes such as controlling the usage, costing, preventive maintenance etc.

25

An anti-theft system is any device and/or or method used to prevent or detect the unauthorized access and/or appropriation of items considered valuable. One such system is vehicle anti-theft authentication system. Nowadays, quick and easy transport has been an essential part of our daily life. As the dark side of this phenomenon, vehicle theft has become one of the costliest property crimes of modern society. From the invention of the first lock and key to the introduction of RFID tags and biometric identification, anti-theft systems have evolved to match the introduction of new inventions to society and the resulting theft of such assets by others. Despite the various technologies that have been introduced in recent years to detect car thefts and tracking of vehicles, it

30

is being continuously reported that many cars were stolen yearly in the world. There are still security breaches where these technologies don't prevent a vehicle from theft, don't assist to recover it and don't allow the users to know the status of their vehicles.

5 JP2008080968A relates to an electric power steering device and vehicle antitheft system. An electric power steering apparatus and a vehicle theft prevention system are provided that can reliably prevent theft of a vehicle without requiring a special device for theft prevention. When an IG switch for turning on / off the supply of power to a steering assist motor is off, a motor lock short circuit using a relay contact supplies power to the motor. The motor is locked by short-circuiting the power
10 supply lines. Even when the IG switch is bypassed, the communication control unit monitors the on / off state of the IG switch, and when the IG switch is off, the short circuit is set in the motor lock state via the relay drive circuit. Further, the EPS ECU including the short circuit and the motor are integrally accommodated in the housing so that illegal work such as cutting of power supply lines, communication lines, etc., bypassing and the like is impossible. However, this patent covers a
15 disruptive method of functional intervention by short circuiting power supply to motor forcefully stopping the motor.

JP2010208554A relates to a vehicle antitheft device, vehicle antitheft method, and program. A security level is improved without impairing convenience. An ID authentication unit authenticates
20 an electronic key in which a vehicle-specific ID code is stored. The biometric authentication unit authenticates whether or not the boarded driver is a registered driver registered in advance based on the driver's biometric information. The mode change input unit receives an input by a registered driver when the mode is set to the password authentication mode or the provisional permission mode, and receives the mode change information indicating either the password authentication mode
25 or the provisional permission mode as the authentication control unit. In the biometric authentication mode, the authentication control unit controls the departure of the vehicle based on the authentication results of ID authentication and biometric authentication. In the password authentication mode, the authentication control unit controls the departure of the vehicle based on the authentication results of ID authentication and password authentication. The present invention
30 can be applied to, for example, a vehicle antitheft device that prevents the vehicle from being stolen. However, the vehicle door only will be authorized and the way of immobilizing the vehicle is different, and no functional flow intervention is achieved.

US20170106904A1 relates to a control method for vehicle with electronic steering column lock. Side loads on an Electronic Steering Column Lock (ESCL) can prevent the ESCL from releasing upon command. An Electric Power-Assisted Steering (EPAS) system is used to reduce or eliminate any side load on the ESCL to mitigate this problem. The EPAS system is activated in response to driver authentication before the driver requests a transition to a ready-to-drive state. The ready-to-drive state is entered only if the ESCL is unlocked. If a predetermined time elapses between driver authentication and the request to enter ready-to-drive state, the EPAS is deactivated and the ESCL is commanded to re-lock. However, this invention only controls the ESCL component.

US6889792B1 relates to an electrically assisted power steering system with anti-theft capability. An electrically assisted power steering system includes an anti-theft feature. Upon detection of an event that is indicative of a vehicle theft situation, the drive circuit for the electric assist motor is selectively actuated to excite the motor windings to either prevent or oppose movement of the steering system. However, electronic drive circuit uses its switches to operate the drive assist motor by energizing its windings and rotor operation. When a vehicle theft situation is detected, power supply to drive assist motor is stopped / disrupted and this amounts to interfering with the internal functions of motor operation.

CN104590209A relates to a car anti-theft alarming device. The invention discloses a car anti-theft alarming device. The car anti-theft alarming device comprises a microprocessor, a car door lock feedback module, a car side feedback module, a car wheel rotating speed feedback module, a car door lock control module, a radio frequency reader, a radio frequency identification, a direct current stabilized power source and an alarming module; the microprocessor is connected with the car door lock feedback module, the car side feedback module, the car wheel rotating speed feedback module, the car door lock control module, the radio frequency reader and the alarming module; the radio frequency reader is used for being in communication with the radio frequency identification. The car anti-theft alarming device has the advantages that the radio frequency reader and the radio frequency identification serve as identity verification modes of car door opening; when a car door is opened and the radio frequency reader does not detect identity identification information of the radio frequency identification, it is considered that the car door is abnormally opened, the microprocessor will drive the alarming module to give out acousto-optic alarms, and therefore lawbreakers can be prevented from illegally opening the car door to steal properties in a car with the method of using a car remote signal interception device and the like. However, the radio frequency reader and the

electronic tag are used as the identify verification method for opening the car door and covers the electronics behind authentication and car door lock security (Access control only). This patent invention focuses on the electronics behind mechanisms such as door lock and not on functional flow intervention.

5

There exists a need for a method of working of the vehicle anti-theft authentication system, which does not depend on any existing solution including, steering lock, electric starter mechanism, fuel supply system etc. To demonstrate the signal-based authentication, the vehicle is chosen as a candidate system (vehicle antitheft authentication system), since vehicles are part of daily life and has widespread usage all over the world.

10

OBJECTS OF INVENTION:

It is primary object of the present invention to provide an electronic signal-based authentication system and method thereof for protecting an electromechanical device.

15

It is another object of the present invention to provide a vehicle anti-theft authentication system to completely prevent an automobile from being stolen and driven away.

It is another object of the present invention to enable a complete lockdown of a vehicle with secure authentication which can be unlocked and only driven by persons duly authenticated.

20

It is another object of the present invention to provide a secure authentication mechanism that is future proof which can be configured by Original equipment manufacturer / dealer at point of sale.

It is another object of the present invention to provide flexibility to Original Equipment Manufacturer to seamlessly add additional security features, devices and solutions to enhance vehicle/device security either through secure cloud-based interface or in-vehicle interface or leverage the existing authentication mechanism to provide full vehicle security.

25

It is another object of the present invention to provide a vehicle anti-theft system that can be integrated by the Original equipment manufacturers into a new generation vehicle and retrofitted in older vehicles with ease.

30

It is another object of the present invention to implement a system to integrate in to a vehicle's electro-mechanical systems without disrupting any of its internal functions and hence provides ease of maintenance and upgradability.

5 SUMMARY OF THE INVENTION:

One or more of the problems of the conventional prior art may be overcome by various embodiments of the present invention.

10 It is the primary aspect of the present invention to provide a signal-based authentication system for electromechanical devices, comprising of:

one or more power on/starter units;

an integrated circuit controller;

one or more signal converters;

one or more user devices;

15 one or more authentication input and alert signal receiver units

one or more workflow sensors/functional components;

a server;

a memory;

a power supply unit;

20 characterized in that, a signal intervention/modification box/unit comprising one or more microprocessors with embedded computer instructions, input – output ports, one or more networking units, one or more communication units, one or more display units;

one or more authentication modules;

one or more actuators; and

25 one or more alert signal units,

wherein the converters comprise of analog to digital converter, digital to analog converter and the like,

30 wherein the signal intervention/modification box/unit is installed between the workflow sensor/functional component and the integrated circuit controller of the device, the microprocessor in the signal intervention / modification box/unit is configured to load the security program instructions into the memory and to receive user authentication data from the user device and is programmed to fetch and compare the user authentication data against authentication data/code/image from the

server/from the internal memory of microprocessor, the programmed microprocessor enables a cloud based / in-device authentication from the server and is configured to detect events indicating an unauthorized entry into/operation of the device and notifying a control function to the alert signal unit,

5 wherein the signal intervention unit is configured to execute instructions at the microprocessor, to provide the response to the event, based on authentication status by the authentication module, and

wherein the response comprises of allowing/altering the signal from the workflow sensor/functional component to the integrated circuit controller of the device.

10 It is another aspect of the present invention to provide a signal-based authentication system for electromechanical devices, wherein the analog to digital converter (ADC) is configured to read the analog signals from the sensor/component and to convert the analog signal values into digital values to the microprocessor.

15 It is another aspect of the present invention to provide a signal-based authentication system for electromechanical devices, wherein the microprocessor is configured to send the converted digital signal received from the sensor/component to the integrated circuit controller and allows normal function of the device, if the authentication status is valid/authentic.

20 It is another aspect of the present invention to provide a signal-based authentication system for electromechanical devices, wherein the alteration of signal comprises of sending of digitally altered pre-configured signal to the integrated circuit controller for functioning the device in an abnormal manner that is pre-defined, if the authentication status is invalid/failed.

25 It is another aspect of the present invention to provide a signal-based authentication system for electromechanical devices, wherein the signal from the workflow sensor/component comprises of voltage signal, current signal, sensor signal, optical signal, wireless signal, magnetic signal and the like.

30 It is another aspect of the present invention to provide a signal-based authentication system for electromechanical devices, wherein the events comprise of successful authentication, failed authentication, hacking of programs, locking of programs, recording the credentials of user,

timestamp, location of equipment, system shutdown forcing only authorized user to unlock / restart the system and the like.

5 It is another aspect of the present invention to provide a signal-based authentication system for electromechanical devices, wherein the events are stored in the memory real-time and offline/asynchronous.

10 It is another aspect of the present invention to provide a signal-based authentication system for electromechanical devices, wherein the electromechanical devices comprise of steering lock device, electric starter mechanism, fuel supply system, automatic teller machine, secret locker device, authenticated medical devices for measuring/recording critical illness, vehicle anti-theft authentication system and the like.

15 It is another aspect of the present invention to provide a signal-based vehicle anti-theft authentication system, comprising of:

one or more ignition switches;
one or more converters;
one or more user devices;
one or more torque sensors;
20 a server;
a memory;
a power supply unit;
an electronic control unit;
a steering wheel;
25 a gear box;
a rack;
a steering column shaft;
a steering motor;
a global positioning system (GPS);
30 characterized in that, a signal intervention/modification box/unit comprising one or more microprocessors with embedded computer instructions, input – output ports, one or more networking units, one or more communication units, one or more display units;
one or more authentication modules; and

one or more alert signal units,

wherein the converters comprise of analog to digital converter, digital to analog converter and the like,

wherein the signal intervention/modification box/unit is installed between the torque sensor and the electronic control unit of the steering motor to turn the wheels, the microprocessor is configured to load the instructions into the memory and to receive user authentication data from the user device and is programmed to fetch and compare the user authentication data and authentication data/code/image from the server or from the internal storage of microprocessor, the programmed microprocessor enables a cloud based / in-device authentication from the server and is configured to detect events indicating an unauthorized entry into the vehicle and notifying a control function to the alert signal unit,

wherein the signal intervention unit is configured to execute instructions at the microprocessor with computer instructions enabled functional flow intervention module, to provide the response to the event, based on authentication status by the authentication module, and

wherein the response comprises of allowing/altering the signal from the torque sensor to the electronic control unit of the vehicle.

It is another aspect of the present invention to provide a signal-based vehicle anti-theft authentication system, wherein the analog to digital converter (ADC) is configured to read the analog signals from the sensor and to convert the analog signal values into digital values to the microprocessor.

It is another aspect of the present invention to provide a signal-based vehicle anti-theft authentication system, wherein the microprocessor sends the converted digital signal received from the sensor to the electronic control unit and allows normal movement of the vehicle, if the authentication status is valid/authentic.

It is another aspect of the present invention to provide a signal-based vehicle anti-theft authentication system, wherein the alteration of signal comprises of sending of digitally altered pre-configured signal to the electronic control unit for driving the steering motor in only one direction

either clockwise or anti-clockwise direction that is pre-defined in the microprocessor, if the authentication status is invalid/failed.

5 It is another aspect of the present invention to provide a signal-based vehicle anti-theft authentication system, wherein the signal from the sensor comprises of voltage signal, current signal, sensor signal, optical signal, wireless signal, magnetic signal and the like.

10 It is another aspect of the present invention to provide a signal-based vehicle anti-theft authentication system, wherein the events comprise of successful authentication, failed authentication, hacking of programs, locking of programs, recording of credentials of user, timestamp, location of vehicle, shutting down the microprocessor, unlocking a locked program, restarting the microprocessor which is shutdown and the like.

15 It is another aspect of the present invention to provide a signal-based vehicle anti-theft authentication system, wherein the events are stored in the memory real-time and offline/asynchronous.

20 It is another aspect of the present invention to provide a signal-based vehicle anti-theft authentication system, wherein the electronic control unit is configured to receive the analog signals and send signal to the steering motor to steer the wheels.

25 It is another aspect of the present invention to provide a signal-based vehicle anti-theft authentication system, wherein the signal-based vehicle anti-theft authentication system is configured for extraneous conditions to allow the driver/user to enter special authentication code and to send SOS alert to the owner/main user device/law enforcement device with location of the vehicle using the GPS.

30 It is another aspect of the present invention to provide a signal-based vehicle anti-theft authentication system, wherein the extraneous conditions comprise of vehicle hijack, accidents, breakdowns and the like.

It is another aspect of the present invention to provide a signal-based vehicle anti-theft authentication system, wherein the complete lockdown of the vehicle is performed with secure

authentication (when the number of attempts of authentication exceeds the configured number of retry), which is unlocked and driven by users/drivers duly authenticated.

- 5 It is another aspect of the present invention to provide a signal-based vehicle anti-theft authentication system, wherein the signal intervention/modification box/unit is configured to be installed by the original equipment manufacturer/dealer at point of sale into new generation devices/vehicles and the signal intervention/modification box/unit is retrofitted in the circuit of the existing devices/vehicles.
- 10 It is another aspect of the present invention to provide a signal-based vehicle anti-theft authentication system, wherein the embedded microprocessor sends an audio/visual alert by the alert signal unit to the owner device of the vehicle /law enforcement user device on the security network configured in the device upon receiving failed authentication code by the user/driver.
- 15 It is another aspect of the present invention to provide a signal-based vehicle anti-theft authentication system, wherein the user is authenticated by checking the personal identification details comprises of name, mobile number, credentials like driving license and the like for operating the signal-based device.
- 20 It is another aspect of the present invention to provide a signal-based vehicle anti-theft authentication system, wherein the authentication modules comprise of smart device, bio-metric unit, Bluetooth unit, near field communication unit, face recognition sensor, finger print sensor, identification unit, and the like.
- 25 It is another aspect of the present invention to provide a signal-based vehicle anti-theft authentication system, wherein the authentication data comprises of password, bio-metric, voice command, video command, one-time password, driving license, National Unique ID (e.g., Aadhar in India), face recognition, finger print and the like.
- 30 It is another aspect of the present invention to provide a method of working of the signal-based authentication system for electromechanical devices, comprising of the steps:
installation of the signal intervention/modification box/unit between the workflow sensor/
functional component and the integrated circuit controller of a device;

switching on of the start-up unit;
requesting an authentication code/image input interface to be entered in the user device configured in the device;
entering an authentication code/image by the user on the user device within a predefined
5 time-out period;
transferring of the above user authentication input code/image to the microprocessor;
fetching and comparing the user authentication data and authentication data/code/image from the server by the programmed microprocessor enabling a cloud based / in-device authentication from the server;
10 detecting of events indicating an unauthorized entry into the device and notifying a control function to the alert signal unit;
executing programs by the embedded microprocessor programming logic; and
if necessary, providing the response to the event, based on authentication status by the authentication module,
15 wherein the response comprises of altering/allowing the signal from the workflow sensor/functional component to the integrated circuit controller of a device,
wherein the analog to digital converter is configured to read analogue signal values from the sensor/component and to convert the signal values into digital values to the microprocessor,
20 wherein the microprocessor sends the digital signal received from the sensor/component to the integrated circuit controller and allows normal function of the device, if the authentication status is valid/authentic, and
wherein the alteration of signal comprises of sending of digitally altered pre-configured signal to the integrated circuit controller for functioning of the device in
25 abnormal manner that is pre-defined in the microprocessor, if the authentication status is invalid/failed.

It is another aspect of the present invention to provide a method of working of the signal-based authentication system for electromechanical devices, wherein the electromechanical devices
30 comprise of steering lock device, electric starter mechanism, fuel supply system, automatic teller machine, secret locker device, authenticated medical devices for measuring/recording critical illness, vehicle anti-theft authentication system and the like.

It is another aspect of the present invention to provide a method for working of the signal-based smart vehicle anti-theft authentication system, comprising of the steps:

installation of the signal intervention/modification box/unit between the torque sensor and the electronic control unit of the vehicle;

5 turning on the ignition switch;

requesting an authentication code/image input interface to be entered in the user device configured in the vehicle;

entering an authentication code/image by the user on the user device within a predefined time-out period;

10 transferring of the above user authentication input code/image to the microprocessor;

fetching and comparing the user authentication data and authentication data/code/image from the server, by the programmed microprocessor enabling a cloud based / in-device authentication from the server;

15 detecting of events indicating an unauthorized entry into the vehicle and notifying a control function to the alert signal unit;

executing programs by the embedded microprocessor programming logic; and

providing response to the event, based on authentication status by the authentication module, wherein the response comprises of altering/allowing the signal from the torque sensor to the electronic control unit,

20 wherein the analog to digital converter (ADC) is configured to read analogue signal values from the sensor and to convert the signal values into digital values to the microprocessor.

wherein the microprocessor sends the digital signal received from the sensor to the electronic control unit and allows normal movement of the vehicle, if the authentication status is valid/authentic, and

25 wherein the alteration of signal comprises of sending of digitally altered pre-configured signal to the electronic control unit for driving the steering motor in only one direction either clockwise or anti-clockwise direction that is pre-defined in the microprocessor, if the authentication status is invalid/failed.

30 It is another aspect of the present invention to provide a method for working of the signal-based smart vehicle anti-theft authentication system, wherein the user has to authenticate within pre-

configured number of times, failing which, the authentication module is disabled from further access.

5 It is another aspect of the present invention to provide a method for working of the signal-based smart vehicle anti-theft authentication system, wherein the audio/visual alert is generated by the alert signal unit to alert the owner/main user device regarding one-way turning of the steering/vehicle.

10 It is another aspect of the present invention to provide a method for working of the signal-based smart vehicle anti-theft authentication system, wherein for re-authentication, the user unlocks the authentication module in the memory of the microprocessor using a special code/image known only to the owner/authorized user.

BRIEF DESCRIPTION OF THE DRAWINGS:

15 So that the manner in which the features, advantages and objects of the invention, as well as others which will become apparent, may be understood in more detail, more particular description of the invention briefly summarized above may be had by reference to the embodiment thereof which is illustrated in the appended drawings, which form a part of this specification. It is to be noted, however, that the drawings illustrate only a preferred embodiment of the invention and is therefore
20 not to be considered limiting of the invention's scope as it may admit to other equally effective embodiments.

Fig 1 illustrates an overview of the signal-based smart vehicle anti-theft authentication system in accordance with the present invention.

25 Fig. 2 illustrates the flow diagram of the detailed implementation of signal-based smart vehicle anti-theft authentication system in accordance with the present invention.

Fig. 3 illustrates the schematic block diagram of the signal-based smart vehicle anti-theft authentication system illustrating the signal intervention by the microprocessor in Signal intervention/modification box/unit.

30 Fig. 4 illustrates the vehicle movement in a circular path for the unauthorized user.

DESCRIPTION FOR DRAWINGS WITH REFERENCE NUMERALS:

[1] Electronic control unit

[2] Steering wheel

- [3] Steering motor
- [4] Sensors
- [5] Signal intervention/modification box/unit
- [6] Torque sensor output signal
- 5 [7] Gear box
- [8] Rack
- [9] User devices
- [10] Starter /Ignition switch
- [11] Server
- 10 [12] Microprocessor

DETAILED DESCRIPTION OF THE INVENTION:

The present invention relates to the field of authentication systems. More particularly, it relates to the electronic signal-based authentication system. It relates to an authentication system which integrates into devices in electro-mechanical systems without interfering with any of its internal functions and hence provides an ease of maintenance and upgradability. More particularly, the present invention relates to prevention of un-authorized usage of electro-mechanical systems.

The signal based authentication system for electromechanical devices, comprising of one or more power on/starter units, an integrated circuit controller, one or more converters, one or more user devices, one or more workflow sensors/functional components, a server, a memory, a power supply unit, a signal intervention/modification box/unit comprising one or more microprocessors with embedded computer instructions, input – output ports, one or more networking units, one or more communication units, one or more display units and one or more actuators, one or more authentication modules and one or more alert signal units.

The converters comprise of analog to digital converter, digital to analog converter and the like. The signal intervention/modification box/unit is installed between the workflow sensor/functional component and the integrated circuit controller of the device. The microprocessor is configured to load the instructions into the memory and to receive user authentication data from the user device and is programmed to fetch and compare the user authentication data against authentication data/code/image from the server/from the internal memory of microprocessor. The programmed microprocessor enables a cloud based / in-device authentication from the server and is configured to

detect events indicating an unauthorized entry into/operation of the device and notifying a control function to the alert signal unit. The signal intervention unit is configured to execute instructions at the microprocessor, to allow/alter the response to the event, based on authentication status by the authentication module. The response comprises of allowing/altering the signal from the workflow sensor/functional component to the integrated circuit controller of the device.

The analog to digital converter (ADC) is configured to read the analog signal values from the sensor/component and to convert the signal values into digital values and send the same to the microprocessor. The microprocessor is configured to send the converted digital signal received from the sensor/component to the integrated circuit controller and allows normal function of the device, if the authentication status is valid/authentic. The alteration of signal comprises of sending of digitally altered pre-configured signal to the integrated circuit controller for functioning the device in an abnormal manner that is pre-defined, if the authentication status is invalid/failed. The signal from the workflow sensor/component comprises of voltage signal, current signal, sensor signal, optical signal, wireless signal, magnetic signal and the like. The events comprise of successful authentication, failed authentication, hacking of programs, locking of programs, recording the credentials of user, timestamp, location of equipment, system shutdown forcing only authorized user to unlock / restart the system and the like. The events are stored in the memory real-time and offline/asynchronous. The electromechanical devices comprise of steering lock device, electric starter mechanism, fuel supply system, automatic teller machine, secret locker device, authenticated medical devices for measuring/recording critical illness, vehicle anti-theft authentication system and the like.

The method of working of the signal-based authentication system for electromechanical devices, comprising of the following steps. The signal intervention/modification box/unit is installed between the workflow sensor/ functional component and the integrated circuit controller of a device. The start-up unit is switched on. An authentication code/image input is requested to be entered in the user device configured in the device. An authentication code/image is entered by the user on the user device within a predefined time-out period. The above user authentication input code/image is transferred to the microprocessor. The user authentication data and authentication data/code/image are fetched and compared from the server by the programmed microprocessor enabling a cloud based / in-device authentication from the server. The events indicating an unauthorized entry into the device is detected and a control function is notified to the alert signal unit. The programs are

executed by the embedded microprocessor programming logic. The response is provided to the event, based on authentication status by the authentication module.

5 The response comprises of allowing/altering the signal from the workflow sensor/functional component to the integrated circuit controller of a device. The analog to digital converter is configured to read analogue signal values from the sensor/component and to convert the signal values into digital values to the microprocessor. The microprocessor sends the digital signal received from the sensor/component to the integrated circuit controller and allows normal function of the device, if the authentication status is valid/authentic. The alteration of signal comprises of
10 sending of digitally altered pre-configured signal to the integrated circuit controller for functioning the device in abnormal manner that is pre-defined in the microprocessor, if the authentication status is invalid/failed.

General Processing steps:

- 15 a) Choose device functions (can be multiple or complete device) to be secured.
- b) Install (or use existing) standard microprocessor (control unit) in the electrical line between the operator starting/signal device/master device and the functional device's functions to be secured.
- c) Install / Integrate embedded security software in to the microprocessor.
- d) Store reference authentication data in data store attached to microprocessor/cloud.
- 20 e) Upon start of equipment, accept authentication from operator / signal device / master device.
- f) Authenticate the user against data from the microprocessor data store / cloud.
- g) Upon successful authentication, allow normal operation of device.
- h) Upon failure of authentication, prevent usage of device or device's target functions.

25 **Exemplary embodiment:**

The present invention relates to the field of authentication systems. The present invention relates to a vehicle anti-theft authentication system which integrates into a vehicle's electro-mechanical systems without interfering with any of its internal functions and hence provides an ease of maintenance and upgradability.

30 Referring to fig 1 an overview of the signal-based smart vehicle anti-theft authentication system in accordance with the present invention is illustrated. Referring to fig. 3 the schematic block diagram of the signal-based smart vehicle anti-theft authentication system illustrating the signal intervention

by the microprocessor is explained. Referring to fig. 2 & 3, the signal-based vehicle anti-theft authentication system, comprising of one or more ignition switches [10], one or more converters, one or more user devices [9], one or more torque sensors [4], a server, a memory, a power supply unit, , a steering wheel [2], a gear box [7], a rack [8], a steering column shaft, a steering motor [3], a
 5 global positioning system (GPS), a signal intervention/modification box/unit [5] comprising one or more microprocessors with embedded computer instructions, input – output ports, one or more networking units, one or more communication units, one or more display units one or more authentication modules and one or more alert signal units.

10 The converters comprise of analog to digital converter, digital to analog converter and the like. The signal intervention/modification box/unit [5] is installed between the torque sensor [4] and the electronic control unit [1] of the steering motor [3] to steer the wheels. The microprocessor [12] is located inside the signal intervention/modification box/unit [5]. The microprocessor [12] is configured to load the instructions into the memory and to receive user authentication data from the
 15 user device [9] and is programmed to fetch and compare the user authentication data against the authentication data/code/image from a server [11]/from the internal storage of microprocessor. The programmed microprocessor [12] enables a cloud based / in-device authentication from the server [11] and is configured to detect events indicating an unauthorized entry into the vehicle and notifying a control function to the alert signal unit. The signal intervention unit [5] is configured to
 20 execute instructions at the microprocessor [12] with computer instructions, to allow/alter the response to the event, based on authentication status by the authentication module. The response comprises of allowing/ altering the signal [6] from the torque sensor [4] to the electronic control unit [1] of the vehicle.

25 The analog to digital converter (ADC) is configured to read the analog signals from the sensor [4] and to convert the signal values [6] into digital values to the microprocessor [12]. The microprocessor [12] sends the converted digital signal received from the sensor [4] to the electronic control unit [1] and allows normal movement of the vehicle, if the authentication status is valid/authentic. The alteration of signal comprises of sending of digitally altered pre-configured
 30 signal to the electronic control unit [1] for driving the steering motor [3] in only one direction either clockwise or anti-clockwise direction that is pre-defined in the microprocessor [12], if the authentication status is invalid/failed. The signal from the sensor [4] comprises of voltage signal, current signal, sensor signal, optical signal, wireless signal, magnetic signal and the like. The events

comprise of successful authentication, failed authentication, hacking of programs, locking of programs, recording of credentials of user, timestamp, location of vehicle, shutting down the microprocessor, unlocking a locked program, restarting the microprocessor which is shut down and the like. The events are stored in the memory real-time and offline/asynchronous.

5

The steering motor [3] is configured to receive signal from the electronic control unit [1] and to drive the steering motor [3] to steer the wheel in clockwise, anti-clockwise or straight direction. The signal-based vehicle anti-theft authentication system is configured for extraneous conditions to allow the driver/user to enter special authentication code and to send SOS alert to the owner/main user device/law enforcement device with location of the vehicle using the GPS. The extraneous conditions comprise of vehicle hijack, accidents, breakdowns and the like. The complete lockdown of the vehicle is performed with secure authentication, which can be unlocked and driven by users/drivers duly authenticated. The signal intervention/modification box/unit [5] is configured to be installed by the original equipment manufacturer/dealer at point of sale into new vehicles and the signal intervention/modification box/unit [5] is retrofitted in the circuit of the existing vehicles. The embedded microprocessor [12] sends an audio/visual alert to the main user device/law enforcement user device on the security network configured in the device upon receiving failed authentication code by the user/driver. The user is authenticated by checking the personal identification details which comprise of name, mobile number, user credentials such as driving license and the like for operating the signal-based device. The authentication modules comprise of smart device, bio-metric unit, Bluetooth unit, near field communication unit, face recognition sensor, finger print sensor, and the like. The successful/failed attempts in the usage are recorded in in-vehicle/cloud database. The authentic data collected can be used for variety of purposes as listed in Benefits section below. The authentication data comprises of password, bio-metric, voice command, video command, one-time password, driving license, National Unique ID (e.g., Aadhar in India), face recognition, finger print and the like.

Anti-theft authentication system uses an automobile's steering system torque sensor, its electronic control unit, steering motor and a highly secure authentication mechanism to prevent it from being burgled and driven away.

The operation of the EPAS (Electronic Power Assisted Steering) is achieved by firstly sensing the amount of effort, or torque, applied to the steering wheel by means of a torque sensor. This torque

sensor is easily incorporated within the steering column. An electric circuit is able to relay this information into an electronic control unit (ECU). The control algorithm generates a signal that drives the electric motor to provide steering assistance.

- 5 If the input received from the user is authentic, then the voltage signal received from the torque sensor is transmitted without modification to the electronic control unit and the steering of vehicle behaves normally.

If the user is not authenticated, the embedded microprocessor programming logic passes a
10 configured voltage to the electronic control unit which drives the motor in only one direction that is pre-defined in the microprocessor.

Referring to Fig. 2, the flow diagram of the detailed implementation of signal-based smart vehicle anti-theft authentication system in accordance with the present invention is illustrated. Referring to
15 Fig. 4 the vehicle movement in a circular path for the unauthorized user is illustrated. The method for working of the signal-based smart vehicle anti-theft authentication system, comprising of the following steps.

- a) The signal intervention/modification box/unit [5] is installed between the torque sensor [4] and the electronic control unit [1] of the vehicle.
- 20 b) Install embedded security software in the processor.
- c) Store authentication data in data store attached to microprocessor/cloud.
- d) The ignition switch [10] is switched on.
- e) An authentication code/image input interface is requested to be entered in the user device [9] configured in the vehicle.
- 25 f) An authentication code/image is entered by the user on the user device [9] within a predefined time-out period.
- g) The above user authentication input code/image is transferred to the microprocessor [12].
- h) The user authentication data and authentication data/code/image are fetched and compared from the server [11], by the programmed microprocessor [12] enabling a cloud based / in-device
30 authentication from the server [11]. The events indicating an unauthorized operation of the vehicle are detected and a control function is notified to the alert signal unit. The programs are executed by the embedded microprocessor programming logic [12]. The response is provided to the event, based

on authentication status by the authentication module. The response comprises of allowing/altering the signal [6] from the torque sensor [4] to the electronic control unit [1].

i) The analogue to digital converter (ADC) is configured to read signal values [6] from the sensor [4] and to convert the signal values [6] into digital values and send to the microprocessor [12].

j) The microprocessor [12] sends the digital signal received from the sensor [4] to the electronic control unit [1] and allows normal movement of the vehicle, if the authentication status is valid/authentic. The alteration of signal comprises of sending of digitally altered pre-configured signal to the electronic control unit [1] for driving the steering motor [3] in only one direction either clockwise or anti-clockwise direction that is pre-defined in the microprocessor [12], if the authentication status is invalid/failed.

The user has to authenticate within pre-configured number of times, failing which, the authentication module is disabled from further access. The audio/visual alert is generated by the alert signal unit to alert the owner/main user device regarding unidirectional steering of the vehicle (Refer Fig.4) and prevent the vehicle being driven away and alert the owner through SMS and the like as configured in the software etc. For re-authentication, the user unlocks the authentication module in the memory of the microprocessor [12] using a special code/image known only to the owner/authorized user.

In vehicle hijack conditions, driver sends an extra SOS byte / use button to send SOS to law agencies and owner.

The authentication can be merged into existing vehicle entry control mechanisms such as key fob, or can be made an additional layer of security such as Smartphone etc.

The present invention is secure and seamlessly integrates with the above described EPAS function, microprocessor based black box that sits in between the steering column torque sensor and the electric/electronic control unit that drives the steering shaft motor to steer the wheels.

Key Features:

Patent is designed for electro-mechanical systems with functional flow intervention. The analogue / digital signals flow is to the device are controlled, (for example voltage) using secure embedded

software logic. Coalesces into device's natural functioning & controls the same without interference. Virtually hack proof as the solution integrates seamlessly in to the device's existing hardware / software. Authentication flexibility - Existing security mechanisms can be used or new ones can be implemented - Future proof. The present invention is easily Retrofittable. The usage data collection is facilitated by owner/law enforcement for effective device security management. The innovative extensions are provided to device security - Providing action alerts to stall forced usage under duress. The present invention has very low additional incremental and maintenance effort and cost.

For the vehicle anti-theft, the signal intervention/modification box/unit is installed in between torque sensor and electronic control unit to control the direction of steering motor rotation. The authentication microprocessor is integrated in the vehicle to control function. The authentication system is integrated in the ignition system of new vehicle or retrofitted in older vehicles. Seamless vehicle security features are offered to Original equipment manufacturer. The vehicle wheel steering direction is controlled based on authentication. Authentication mechanism is built into/for natural function of vehicle. The recovery assistance from anti theft device is achieved without use of GPS. Access control devices assist to collect authentic usage data (Eg., odometer can be fudged). For example, access control device can assist in collecting and storing log information and the microprocessor can store such log of all events.

Sequence of operation:

1. Driver starts the ignition.
2. Vehicle battery powers up all electric components including the security device which is a microprocessor. Security code is loaded and runs in microprocessor (or can be executed from a secure remote server / cloud depending on portability to ECU computing architecture)
3. The security program configures (Refer Vehicle Security and Configuration Setup) the signal to ECU to drive the Steering electric motor to rotate in one-direction (steering directional lock is set) which will make the vehicle wheels steer only in one direction.
4. Security program requests authentication details and waits for authentication inputs from (or communicates with) the mobile device which the driver would use to enter authentication data. This can be a password, bio metric, voice command, OTP etc. If the authentication data is not received within authentication time-out period (Refer Vehicle Security and Configuration Setup), the security code is unloaded. The operator has to start the ignition again to initiate authentication.

5. Upon receiving authentication data, security program will access the authentication data registered in vehicle database or access a secure external database (Eg., RTO database for verifying smart card-based driving license etc) for comparison (Refer Vehicle Security and Configuration Setup).

6. At this point, this program also reads the torque sensor signal. This signal is only read and not processed. If the operator credentials are not valid, request is sent to operator to provide correct credentials. Number of such retries is configurable (Refer Vehicle Security and Configuration Setup).

7. If authentication succeeds, the steering directional lock is not applied and the security program passes the torque sensor signal value without modification to steering ECU / drive motor for normal steering direction and vehicle can be driven away.

8. If authentication fails, the steering directional lock is set, which makes a single way steering direction signal to ECU / drive assist motor. Also, an audio-visual signal alerts the operator about steering directional lock and uni-directional steering. Since the ignition is already on, the operator may tend to ignore audio-visual warning and generally tries to drive the vehicle, to move forward or backward. During this process, operator will necessarily have to steer the vehicle either left or right to manoeuvre the vehicle by turning the steering wheel. Since the steering directional lock is already on, this ensures vehicle security. Despite the driver turning the steering wheel in either direction upon engaging the gear, irrespective of whether the steering wheel is turned right or left, vehicle wheel turns only in one configured direction (Refer Vehicle Security and Configuration Setup) and hence the vehicle cannot be driven away. After the detection of authentication failure, after a configured number of attempts, the engine will automatically shut down and microprocessor feeding the voltage signals to ECU is also shut down (Refer Vehicle Security and Configuration Setup).

9. If the steering directional lock is set after the specified failed attempts, the Supervisor/Owner of vehicle has to authorize with a special code, before restart of the vehicle.

10. The operator, can try to authenticate number of times (Refer Vehicle Security and Configuration Setup). An alert is sent to the owner of the vehicle for every successful/failed attempt. Beyond a certain number of failures (Refer Vehicle Security and Configuration Setup), an alert can be made to be sent to law enforcement agency.

Real life Scenarios of Embodiment:

1) Stationery Vehicle:

When a stationary vehicle in off condition is started, an authentication mechanism forces the driver to enter an authentication code in his hand-held device such as mobile phone using Bluetooth stack or use bio-metric or use any other security mechanism configured in the vehicle. The system then fetches a bio-metric image or an authentication code (or any other relevant data) from secure cloud storage/ in vehicle storage and compares the same with the information entered / image captured by the driver.

If the match (and hence authentication) is SUCCESSFUL, embedded microprocessor- based programming logic allows the voltage signals from the torque sensor of steering system to be passed on to the electronic control unit of the vehicle to drive the steering motor under normal conditions.

If the authentication FAILS, the programming logic built in to the microprocessor passes a pre-configured voltage to the electronic control unit which uses the input to drive the motor in only one direction after a configured number of attempts to authenticate. This forces the vehicle to turn in only one direction and hence the vehicle cannot be driven away. After each success/failure, alert is sent to owner's mobile. After repeated failures, alert is sent to law enforcing agencies.

2) Under forced hijack conditions:

When stopped at gun/knife point, driver of the vehicle needs to first switch off ignition. When forced to restart, he can use an SOS authentication code that is either a different pass code or his bio-metric with a special button in his mobile to drive the vehicle. The microprocessor then interprets and differentiates the SOS pass code from the normal one and sends an alert to connected police network and even to another mobile (For E.g., vehicle owner's mobile or multiple mobile numbers such as call center etc.) configured in the system. The steering directional lock is not applied, and optionally turn on GPS recording and the vehicle can run normally. The alert will enable the law enforcement authority to locate the vehicle and intercept appropriately to save the driver and prevent the vehicle from being stolen and driven away.

3) Vehicles violating traffic rules:

As the vehicle is fitted with the registration details which are electronically transmittable, the law enforcing authorities can implement suitable detection system at traffic signal, to detect vehicles violating signals and issue tickets resulting in better law enforcement. (Linking of this system to any vehicle tracking system E.g., FASTag can also be done).

This invention provides the flexibility to OEM to seamlessly add additional security features, devices and solutions to enhance vehicle security.

5 Vehicle Security and Configuration Setup:

This invention provides for configuring the vehicle security parameters either in the plant assembly by the OEM, at dealer point or by the owner authorized to modify the factory set-up. These data can either be stored in-vehicle in a secure storage or in cloud / remote server.

1. During vehicle registration-
 - 10 a) Record the owner's credentials (E.g., Driving license, Mobile number etc)
 - b) The default direction of turning (Left or right) during directional lock of steering. This may depend on left-hand or right-hand driving.
 - c) Configure device(s) for authentication E.g., cell phone, biometric etc
 - d) The law-enforcement authority to whom alert will be sent, in case of attempted theft.
- 15 2. Initial setup by owner of vehicle.
 - a) List of authorized persons and their authentication details. Details of driver/s that have been removed from service or are no more authorized to drive the vehicle can be easily removed.
 - b) Set/Modify Supervisor password, to restart the vehicle after authentication failure.
 - c) Contact details (E.g., Cell-phone) for sending alert message during every success/failure of

20 vehicle start.
 - d) Configure audio-visual alert during authentication failure.
 - e) Time-out period after ignition start before user authentication.
 - f) Number of attempts allowed before authentication failure is recognized.
 - g) Configure data storage (local/ cloud storage for operator credentials, access to RTO database

25 etc.)
 - h) Configure the extent of data collected (E.g., odometer reading, start/stop timing, incidents occurred)

Working example:

- 30 The following is a specific implementation (Working example) of the Exemplary Embodiment described earlier

A working model is made with a turning knob, (that simulates a steering), Dual Sensor that generate two voltage signals when knob is turned, a DC/stepper motor, motor drive integrated circuit, two wheels representing vehicle wheels. This model closely represents real life working.

- 5 In an exemplary embodiment of the present invention, following implementation of the solution is described below. For illustration of Signal based vehicle anti-theft authentication system is implemented in a working example with the following components:

SL	Component	Newly Added /Replacement	Specification/ Representation	Remarks
1	Turn Knob	Replacement	Represents and simulates steering wheel	Turning the Knob helps achieve wheel turning.
2	Dual sensor	Replacement	Represents steering torque sensor Creates two sensor outputs when knob is turned	Provides sensor signal outputs similar to main and aux steering torque sensor
3	Column Shaft	Replacement	Represents steering column shaft	This is attached to the Knob at one end and activates the dual sensors at the other end.
4	Microprocessor	Newly Added	1. Raspberry Pi 3 Model B - Raspbian OS - BCM 2837 64-bit processor - 1 GB RAM - Broadcom Wireless LAN and Bluetooth Low Energy On board - GPIO pins for reading (input) and writing (output) digital signals	- On power up, loads the vehicle security program into memory and executes the same - Reads ADC (Analog to Digital) IC for voltage values, - Checks authentication input from the user mobile against an authentication value pre-stored in the microprocessor - If user is authenticated, sends the digital voltage value received from dual sensors to

			- SPI – Serial Peripheral Interface	the Motor Controller IC - If user is not authenticated, changes the voltage signal to force the motor to rotate the wheel in only the pre-configured direction (left or right) and sends the same to Motor Controller IC
5	Analog to Digital Converter (ADC)	Newly Added	MCP3008 ADC IC - 8 channels for connecting 8 analogue input devices	Two of the 8 channels used to read analogue signal from dual sensor, convert to digital values and send as digital output to Microprocessor.
6	Motor Controller IC	Newly Added	ULN2003A motor drive controller IC having digital and analogue pins that can be read from and written to	Receives the analogue signal and sends signal to steering motor wheel mechanism to steer the wheels
7	Drive Motor	Replacement	Stepper motor that helps rotate the wheel. This is similar to steering motor	Depending on the extent of Knob rotation, the signal received from the Motor Controller IC drives the steering mechanism attached to drive motor to steer the vehicle wheel left or right or straight. In straight drive conditions motor does not rotate
8	Battery	Replacement	Power supply 5 V	Power supply to drive the ADC, microprocessor components and drive motor IC and mechanism
9	Mobile Phone1	Newly Added	Standard Android	This mobile is used by the

			mobile phone with WIFI, Bluetooth paired with the Microprocessor, an authentication input entry app	vehicle user who needs to authenticate himself with the microprocessor authentication system
10	Mobile Phone2	Newly Added	Standard Android mobile phone with WIFI connection and an app to display the alert messages from the security software	This mobile is used for receiving alerts on possible theft attempts and such alerts are sent by the security software running in the microprocessor. These mobiles can be with the owner and law enforcing agencies or call centres

Note – MCP3008 ADC IC, Raspberry PI, and ULN2003 motor driver IC together represents EPS ECU (Power Steering Electronic Control Unit) performs its functions, besides authenticating the user.

5

Process described below simulates the implementation of the core functionality described in Fig 3. It uses the components detailed above to perform specific actions.

1. Power is switched on (this is the same as the user starting the ignition in a vehicle)
Microprocessor, ADC, Motor Controller and Motor are powered on by the power supply.
- 10 Security Software is loaded in to the microprocessor memory
2. ADC is used to read voltage signal, starts receiving the signal from Dual sensors when the turn knob attached is rotated
3. Dual sensor sends analogue voltage signals to ADC. However, no further action happens at this stage as this voltage signal remains in ADC and is not read by the Microprocessor or any
- 15 other component
4. Security software reads critical pre-configured parameters from its local data storage. These parameters are reference authentication data, direction of wheel rotation when authentication fails, Maximum Number of attempts at authentication and Timeout period waiting for authentication input from the driver.

5. Security software initializes the Serial Peripheral Interface to send and receive data from ADC, Bluetooth socket connection to receive authentication input from Mobile Phone 1 from the user and waits for authentication input. It also creates client Wi-Fi socket connection to send alert messages to Mobile Phone 2.
- 5 6. GPIO pins needed for communication with ADC and motor drive controller IC s are also initialized for operation
7. User executes the authentication app in Mobile Phone 1 to enter the authentication pass code to be verified
8. If the user does not provide authentication input within the configured timeout value read in
10 step 7, microprocessor sends an alert message to mobile phone 1 and shuts down the microprocessor. System needs to be powered on again and the user needs to re-authenticate.
9. If the user enters authentication input before timeout, security software receives the authentication input in Microprocessor's Bluetooth socket.
10. This input is checked against the reference authentication read in step 4 above
- 15 11. If the authentication match is successful,
 - a) Security software reads analogue voltage signal in equivalent digital values from the ADC. SPI (Serial Peripheral Interface) driver in the OS is used to read this input in digital format
 - b) Security software retains the voltage digital value read from ADC without
20 change. These values are checked as follows and appropriate GPIO pins are enabled / disabled:
 - i. for left turn - 0 to <2.5v in sensor input 1 and >2.5v to 5v in sensor input 2
 - ii. for straight drive – both sensor inputs are 2.5v
 - iii. for right turn - > 2.5v to 5v in sensor input 1 and 0 to <2.5v in sensor input 2.
 - 25 Above pin values (signals) are passed on to motor controller IC.
 - c) Motor-controller IC based on the values received, drives the stepper motor and thus turns the wheels as intended by the user
12. If the authentication fails
 - a) Security software checks if maximum number of retries for authentication is
30 reached. If the maximum number of retries is not reached, security software allows the user to enter authentication input again from mobile phone 1.
 - b) If maximum retries is reached, security software sends an alert message on possible (vehicle) theft attempt to mobile phone 1.

- c) Software then sets an exception escalation flag to stop execution of software further and Microprocessor is shutdown
- d) Security software needs to be unlocked to be executed as intended again by a person authorized to do so through a special code only from a pre-configured mobile device. This ensures the software is secured from being hacked or stolen in locked condition
- e) Security software sets an appropriate set of GPIO pins as enabled or disabled to send signals to motor controller IC to rotate the motor in only the pre-configured direction (left or right) despite the user turning the knob (steering wheel) both ways
- f) Above pin values (signals) are passed on to the motor controller IC
- g) Motor controller IC drives the stepper motor to rotate only in the pre-configured direction (left or right) thus forcing the wheels to turn only in that direction despite the user attempting to turn the knob (wheel) in both direction
- h) Above locking ensures that the system (vehicle) is secured and cannot be stolen

13. All events, including successful authentication, failed attempts and locking of software, are logged for future audit of security incidents

14. Under extraneous conditions such as a vehicle hijack using arms, driver can enter a special pass code for authenticating successfully that will send an alert to mobile phone 2, and there by law enforcement agencies, as SOS alert message with vehicle location using GPS

Benefits:

The signal-based device can be used for a variety of purposes, (as the vehicles are being driven by only authorized persons and their identity of the driver is known) such as:

1. Help collect data to control maintenance cost/incidents during the driving of a driver (for fleet owners).
2. Can trace the driver/owner of vehicle involved in an incident, especially hit and run or in crimes, carrying contraband goods etc.
3. Facilitate the creation and maintenance of KYD (Know Your Driver) database – Driver's driving habits and incident record which can be used by RTO (Road Transport Office) to take decisions regarding renewal of license and rate a driver (similar to credit score for a financial system). Just as a credit score database helps lenders identify potential borrowers with good credit score, KYD database will help vehicle owners identify drivers with safe

driving score. This KYD database can be designed to prevent persons with criminal background own/drive vehicles.

4. Can help trigger alert regarding movement of criminals when they use vehicles.
5. Can be extended to communicate about an accident to the nearest control room and the driver concerned, which info can be used by Insurance companies to validate claims. Besides Insurance companies can come up with new schemes for vehicles/drivers predominantly driven by single user with few / no incidents.
6. Can facilitate the law enforcing authorities to track vehicles violating signals and one-way violation etc.
7. Allows integration with vehicle remote start mechanism that is needed for cold countries. In cold climatic conditions it is not possible to enter the vehicle under very cold conditions without heating the interior and warming up the engine before entering the vehicle. Owner / driver can use a remote start provided by the manufacturer for these aspects and this invention works seamlessly with the remote start feature. Physical presence of the driver inside the vehicle to authenticate and secure the vehicle is not mandatory as the security program will await authentication inputs from the driver after starting the vehicle and will not release the wheel rotation lock till authentication is successful. The same is applicable for very hot regions. As the duration for which the engine can be run without authentication is pre-configured, the engine is also protected.
8. Intermittent re-authentication by the authenticated driver can be automatically executed by the security program at configured time intervals. Vehicle will be permitted to run for a specific time to enable the driver to pull over and park the vehicle to avoid accidents at signal intersections. This feature can also be linked to vehicle hijack condition forcing the hijacker to authenticate again. And integrated with other mechanisms such as reducing vehicle speed or reducing gradually fuel flow to engine to force the driver to stop within a preconfigured time for providing alert, can also be considered.
9. Authentication can be open-ended (no time limit) or for a fixed period of time/distance (to cover service personnel, valet parking etc.)
10. In addition to engine start, authentication inputs can also be taken when the driver occupies driver seat (using seat sensor signal), a camera to capture driver image when vehicle is started etc.

11. Invention provides for flexible vehicle security that can be configured by OEM or at sales / service point. On ignition start, following additional options can be provided by the security program:

- Ignition key / remote can contain the finger print reader. When the finger print reader sends authentication signal that is verified successfully, the steering lock is not applied.
- Only authorized Bluetooth device (BT device address is unique) can initiate the authentication data verification. Inputs from any other BT device can be rejected or not taken
- Specific Bluetooth device ID s or addresses can be configured for verification in the security software. These BT addresses can be searched to accept authentication only from configured driver mobile devices. Such BT devices can alone be paired and allowed to exchange messages with the security software. Standard Bluetooth message encryption and security layer would prevent authentication message hacking.

12. Anti-theft security is increased by the fact that there is no data communication line between the security control unit and the steering lock (ECU / drive motor) which is accessible by a malicious code from outside by a hacker and which can be manipulated by unauthorized persons. Besides, the time available for any hacker to intrude is limited by the timeout feature. Flow intervention in the security program ensures that even if a thief manages to gain entry and start the vehicle, steering uni-directional lock is applied, prohibiting normal driving if authentication fails.

13. Driver/equipment operator identification can include - PIN code, driving license, finger print reader, facial recognition, questions only the correct driver can answer and the like. Driver license is suggested as valid check for automobiles, as this ensures validated knowledge of driving skill and prevents under-age driving. Even if the owner authorizes an under-age person to drive, he becomes liable.

14. Event log for tracing can be implemented. This can include authentication success or failure, number of attempts with time stamp, vehicle hijack SOS event, from and to locations based on GPS etc. GPS can be optionally enabled only when an incident such as an accident or hijack conditions happen. Event log analysis can be used to provide additional alerts, security or even restrict vehicle usage. This log can also help insurance authorities, besides help devise schemes for responsible driving.

15. If the security program reads a voltage value from torque sensor that falls beyond a pre-defined upper and lower circuit values, the vehicle can still be left locked, despite

authentication succeeding, and a risk alert to the driver and other stake holders such as service center configured.

- 5 16. Embedded microprocessor security software for authentication and functional flow intervention to lock / unlock steering direction control helps in making the security very high. Security software can either be hosted in a separate secure microprocessor or can be embedded in the steering EPS ECU controller and this ECU can be secured. For a connected vehicle, this software can be executed from a secure remote / cloud environment (likely to be the future scenario).

- 10 Although, the invention has been described and illustrated with respect to the exemplary embodiments thereof, it should be understood by those skilled in the art that the foregoing and various other changes, omissions and additions may be made therein and thereto, without parting from the spirit and scope of the present invention.

15

I CLAIM:

1. A signal-based authentication system for electromechanical devices, comprising of:

one or more power on/starter units;

an integrated circuit controller;

5 one or more signal converters;

one or more user devices;

one or more authentication input and alert signal receiver units;

one or more workflow sensors/functional components;

a server;

10 a memory;

a power supply unit;

characterized in that, a signal intervention/modification box/unit comprising one or more microprocessors with embedded computer instructions, input – output ports, one or more networking units, one or more communication units, one or more display units;

15 one or more authentication modules;

one or more actuators: and

one or more alert signal units,

wherein the converters comprise of analog to digital converter, digital to analog converter and the like,

20 wherein the signal intervention/modification box/unit is installed between the workflow sensor/functional component and the integrated circuit controller of the device, the microprocessor in the signal intervention / modification box/unit is configured to load the security program instructions into the memory and to receive user authentication data from the user device and is programmed to fetch and
25 compare the user authentication data against authentication data/code/image from the server/from the internal memory of microprocessor, the programmed microprocessor enables a cloud based / in-device authentication from the server and is configured to detect events indicating an unauthorized entry into/operation of the device and notifying a control function to the alert signal unit,

30 wherein the signal intervention unit is configured to execute instructions at the microprocessor, to provide the response to the event, based on authentication status by the authentication module, and

wherein the response comprises of altering/allowing the signal from the workflow sensor/functional component to the integrated circuit controller of the device.

2. The signal-based authentication system for electromechanical devices as claimed in claim 1,
5 wherein the analog to digital converter (ADC) is configured to read the analog signal values from the sensor/component and to convert the signal values into digital values and send the same to the microprocessor.
3. The signal-based authentication system for electromechanical devices as claimed in claim 1,
10 wherein the microprocessor is configured to send the converted digital signal received from the sensor/component to the integrated circuit controller and allows normal function of the device, if the authentication status is valid/authentic.
4. The signal-based authentication system for electromechanical devices as claimed in claim 1,
15 wherein the alteration of signal comprises of sending of digitally altered pre-configured signal to the integrated circuit controller for functioning the device in an abnormal manner that is pre-defined, if the authentication status is invalid/failed.
5. The signal-based authentication system for electromechanical devices as claimed in claim 1,
20 wherein the signal from the workflow sensor/component comprises of voltage signal, current signal, sensor signal, optical signal, wireless signal, magnetic signal and the like.
6. The signal-based authentication system for electromechanical devices as claimed in claim 1,
25 wherein the events comprise of successful authentication, failed authentication, hacking of programs, locking of programs, recording the credentials of user, timestamp, location of equipment, system shutdown forcing only authorised user to unlock / restart the system and the like.
7. The signal-based authentication system for electromechanical devices as claimed in claim 6,
30 wherein the events are stored in the memory real-time and offline/asynchronous.
8. The signal-based authentication system for electromechanical devices as claimed in claim 1,
wherein the electromechanical devices comprise of steering lock device, electric starter mechanism,

fuel supply system, automatic teller machine, secret locker device, authenticated medical devices for measuring/recording critical illness, vehicle anti-theft authentication system and the like.

9. A signal-based vehicle anti-theft authentication system as claimed in claim 8, comprising of:

- 5 one or more ignition switches [10];
- one or more converters;
- one or more user devices [9];
- one or more torque sensors [4];
- a server;
- 10 a memory;
- a power supply unit;
- an electronic control unit [1];
- a steering wheel [2];
- a gear box [7];
- 15 a rack [8];
- a steering column shaft;
- a steering motor [3];
- a global positioning system (GPS);
- characterized in that, a signal intervention/modification box/unit [5] comprising one or more
- 20 microprocessors with embedded computer instructions, input – output ports, one or more
- networking units, one or more communication units, one or more display units ;
- one or more authentication modules; and
- one or more alert signal units,
- wherein the converters comprise of analog to digital converter, digital to analog
- 25 converter and the like,
- wherein the signal intervention/modification box/unit [5] is installed between the
- torque sensor [4] and the electronic control unit [1] of the steering motor [3] to turn
- the wheels, the microprocessor [12] is configured to load the instructions into the
- memory and to receive user authentication data from the user device [9] and is
- 30 programmed to fetch and compare the user authentication data against authentication
- data/code/image from a server [11]/from the internal storage of microprocessor, the
- programmed microprocessor [12] enables a cloud based / in-device authentication

from the server [11] and is configured to detect events indicating an unauthorized entry into the vehicle and notifying a control function to the alert signal unit, wherein the signal intervention unit [5] is configured to execute instructions at the microprocessor [12] with computer instructions enabled functional flow intervention module, to provide the response to the event, based on authentication status by the authentication module, and wherein the response comprises of allowing/altering the signal [6] from the torque sensor [4] to the electronic control unit [1] of the vehicle.

10 10. The signal-based vehicle anti-theft authentication system as claimed in claim 9, wherein the analog to digital converter (ADC) is configured to read the analog signals from the sensor [4] and to convert the signal values [6] into digital values to the microprocessor [12].

15 11. The signal-based vehicle anti-theft authentication system as claimed in claim 9, wherein the microprocessor [12] sends the converted digital signal received from the sensor [4] to the electronic control unit [1] and allows normal movement of the vehicle, if the authentication status is valid/authentic.

20 12. The signal-based vehicle anti-theft authentication system as claimed in claim 9, wherein the alteration of signal comprises of sending of digitally altered pre-configured signal to the electronic control unit [1] for driving the steering motor [3] in only one direction either clockwise or anti-clockwise direction that is pre-defined in the microprocessor [12], if the authentication status is invalid/failed.

25 13. The signal-based vehicle anti-theft authentication system as claimed in claim 9, wherein the signal from the sensor [4] comprises of voltage signal, current signal, sensor signal, optical signal, wireless signal, magnetic signal and the like.

30 14. The signal-based vehicle anti-theft authentication system as claimed in claim 9, wherein the events comprise of successful authentication, failed authentication, hacking of programs, locking of programs, recording of credentials of user, timestamp, location of vehicle, shutting down the microprocessor, unlocking a locked program, restarting the microprocessor which is shutdown and the like.

15. The signal-based vehicle anti-theft authentication system as claimed in claim 14, wherein the events are stored in the memory real-time and offline/asynchronous.

5 16. The signal-based vehicle anti-theft authentication system as claimed in claim 9, wherein the electronic control unit [1] is configured to receive the analog signals and send signal to the steering motor [3] to steer the wheels in clockwise, anti-clockwise or straight direction.

10 17. The signal-based vehicle anti-theft authentication system as claimed in claim 9, wherein the signal-based vehicle anti-theft authentication system is configured for extraneous conditions to allow the driver/user to enter special authentication code and to send SOS alert to the owner user device/ law enforcement user device with location of the vehicle using the GPS.

15 18. The signal-based vehicle anti-theft authentication system as claimed in claim 17, wherein the extraneous conditions comprise of vehicle hijack, accidents, breakdowns and the like.

19. The signal-based vehicle anti-theft authentication system as claimed in claim 9, wherein the complete lockdown of the vehicle is performed with secure authentication which is unlocked and driven by users/drivers duly authenticated.

20 20. The signal-based vehicle anti-theft authentication system as claimed in claim 9, wherein the signal intervention/modification box/unit [5] is configured to be installed by the original equipment manufacturer/dealer at point of sale into new generation devices/vehicles and the signal intervention/modification box/unit [5] is retrofitted in the circuit of the existing devices/vehicles.

25 21. The signal-based vehicle anti-theft authentication system as claimed in claim 9, wherein the embedded microprocessor [12] sends an audio/visual alert by the alert signal unit to the main user device/law enforcement user device on the security network configured in the device upon receiving failed authentication code by the user/driver.

30 22. The signal-based vehicle anti-theft authentication system as claimed in claim 9, wherein the user is authenticated by checking the personal identification details comprises of name, mobile number, user credentials such as license and the like for operating the signal-based device.

23. The signal-based vehicle anti-theft authentication system as claimed in claim 9, wherein the authentication modules comprise of smart device, bio-metric unit, Bluetooth unit, near field communication unit, face recognition sensor, finger print sensor, identification unit, and the like.

5

24. The signal-based vehicle anti-theft authentication system as claimed in claim 9, wherein the authentication data comprises of password, bio-metric, voice command, video command, one-time password, driving license, National Unique ID (e.g., Aadhar in India), face recognition, finger print and the like.

10

25. A method of working of the signal-based authentication system for electromechanical devices, comprising of the steps:

switching on of the start-up unit;

installation of the signal intervention/modification box/unit between the workflow sensor/
functional component and the integrated circuit controller of a device;

15

requesting an authentication code/image input interface to be entered in the user device configured in the device;

entering an authentication code/image by the user on the user device within a predefined time-out period;

20

transferring of the above user authentication input code/image to the microprocessor;

fetching and comparing the user authentication data and authentication data/code/image from the server by the programmed microprocessor enabling a cloud based / in-device authentication from the server;

detecting of events indicating an unauthorized entry into the device and notifying a control function to the alert signal unit;

25

executing programs by the embedded microprocessor programming logic; and

providing the response to the event, based on authentication status by the authentication module,

wherein the response comprises of allowing/altering the signal from the workflow sensor/functional component to the integrated circuit controller of a device,

30

wherein the analog to digital converter is configured to read analogue signals from the sensor/component and to convert the signal values into digital values to the microprocessor,

wherein the microprocessor sends the digital signal received from the sensor/component to the integrated circuit controller and allows normal function of the device, if the authentication status is valid/authentic, and

wherein the alteration of signal comprises of sending of digital altered pre-configured signal to the integrated circuit controller for functioning of the device in abnormal manner that is pre-defined in the microprocessor, if the authentication status is invalid/failed.

26. The method of working of signal-based authentication system for electromechanical devices as claimed in claim 25, wherein the electromechanical devices comprise of steering lock device, electric starter mechanism, fuel supply system, automatic teller machine, secret locker device, authenticated medical devices for measuring/recording critical illness, vehicle anti-theft authentication system and the like.

27. A method for working of the signal-based smart vehicle anti-theft authentication system as claimed in claim 25, comprising of the steps:

installation of the signal intervention/modification box/unit [5] between the torque sensor [4] and the electronic control unit [1] of the vehicle;

turning on the ignition switch [10];

requesting an authentication code/image input interface to be entered in the user device [9] configured in the vehicle;

entering an authentication code/image by the user on the user device [9] within a predefined time-out period;

transferring of the above user authentication input code/image to the microprocessor [12];

fetching and comparing the user authentication data and authentication data/code/image from the server [11], by the programmed microprocessor [12] enabling a cloud based / in-device authentication from the server [11];

detecting of events indicating an unauthorized entry into the vehicle and notifying a control function to the alert signal unit;

executing programs by the embedded microprocessor programming logic [12]; and

providing response to the event, based on authentication status by the authentication module, wherein the response comprises of allowing/altering the signal [6] from the torque sensor [4] to the electronic control unit [1],

wherein the analog to digital converter (ADC) is configured to read analogue signal values [6] from the sensor [4] and to convert the signal values [6] into digital values to the microprocessor [12].

wherein the microprocessor [12] sends the digital signal received from the sensor [4] to the electronic control unit [1] and allows normal movement of the vehicle, if the authentication status is valid/authentic, and

wherein the alteration of signal comprises of sending of digitally altered pre-configured signal to the electronic control unit [1] for driving the steering motor [3] in only one direction either clockwise or anti-clockwise direction that is pre-defined in the microprocessor [12], if the authentication status is invalid/failed.

28. The method for working of the signal-based smart vehicle anti-theft authentication system as claimed in claim 27, wherein the user has to authenticate within pre-configured number of times, within pre-configured amount of time, failing which, the authentication module is disabled from further access.

29. The method for working of the signal-based smart vehicle anti-theft authentication system as claimed in claim 27, wherein the audio/visual alert is generated by the alert signal unit to alert the owner/main user device regarding one-way turning of the steering/vehicle.

30. The method for working of the signal-based smart vehicle anti-theft authentication system as claimed in claim 27, wherein for re-authentication, the user unlocks the authentication module in the memory of the microprocessor [12] using a special code/image known only to the owner/authorized user.

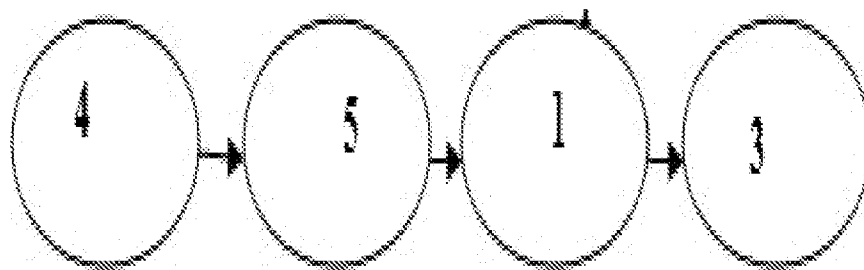
FIGURE 1:

FIGURE 2:

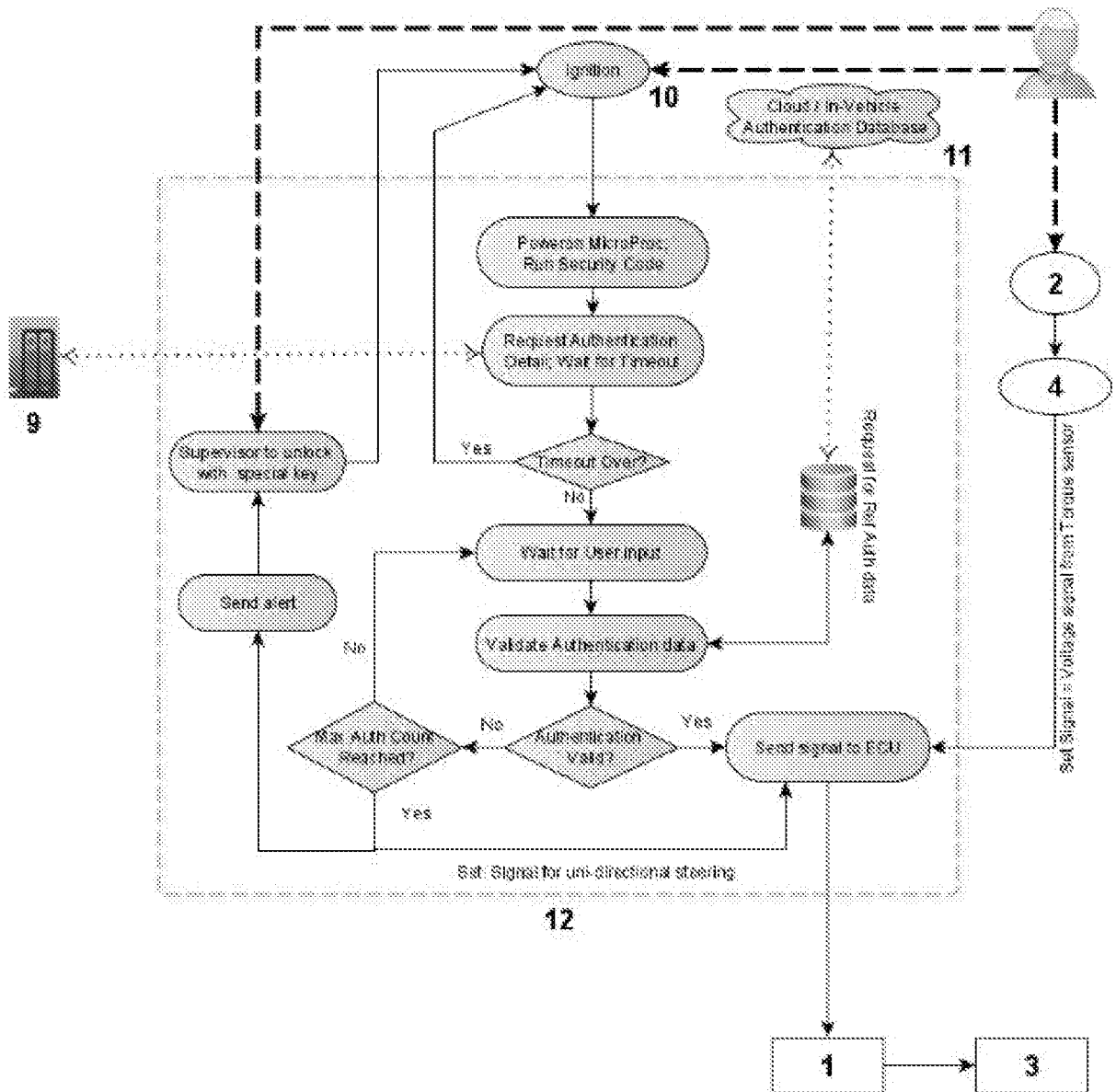


FIGURE 3:

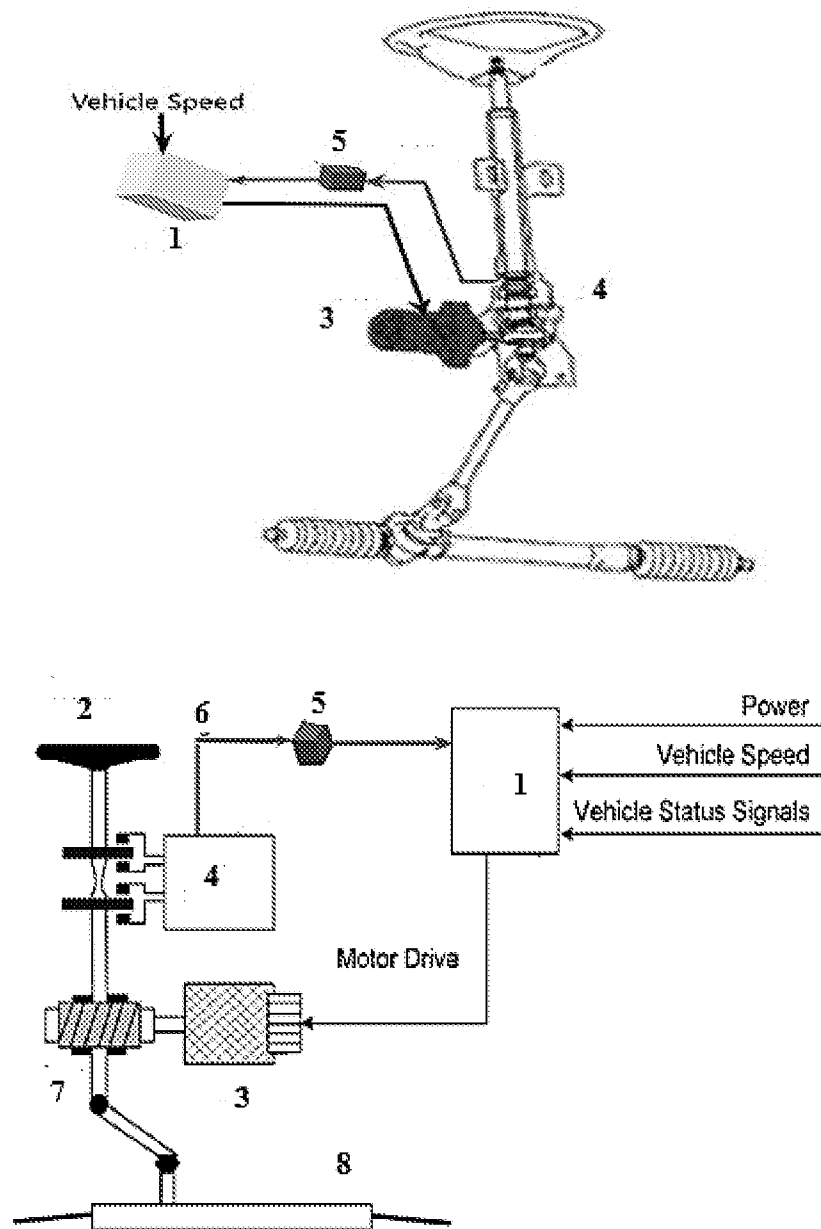
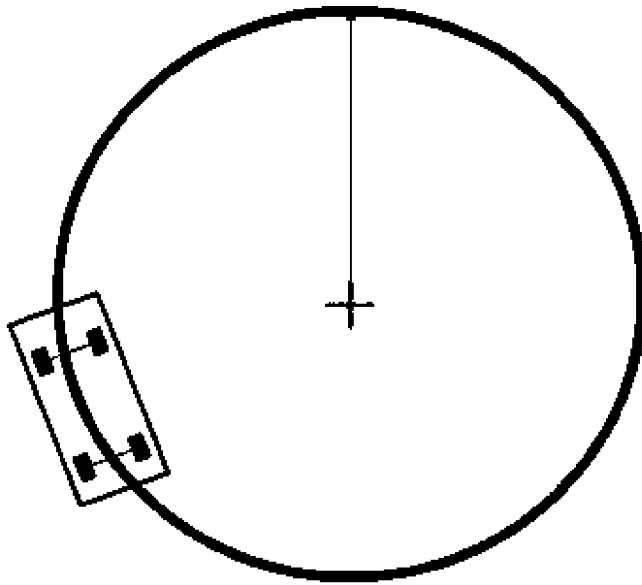


FIGURE 4:



INTERNATIONAL SEARCH REPORT

International application No.
PCT/IN2021/050112

A. CLASSIFICATION OF SUBJECT MATTER
G01D3/08, B60R25/10, G06F7/00 Version=2021.01

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)

B60R, G01D, G06F

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)

DATABASES: IPO INTERNAL DATABASE, TOTALPATENT ONE

KEYWORDS: IN-BUILT, INTEGRATED, VEHICLE, ANTI-THEFT, ELECTROMECHANICAL

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
Y	US7233227 B2 (Hertz Corp) 19 JUNE 2007 (19-06-2007) WHOLE DOCUMENT	1-30
Y	WO2019165489 A1 (DAVIS, STEVEN JOHN ET AL.) 06 SEPTEMBER 2019 (06-09-2019) WHOLE DOCUMENT	1-30

☐ Further documents are listed in the continuation of Box C. ☒ 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

"D" document cited by the applicant in the international application

"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

01-04-2021

Date of mailing of the international search report

01-04-2021

Name and mailing address of the ISA/

Indian Patent Office
Plot No.32, Sector 14, Dwarka, New Delhi-110075
Facsimile No.

Authorized officer

Saurabh Dwivedi

Telephone No. +91-1125300200

INTERNATIONAL SEARCH REPORT
Information on patent family members

International application No.
PCT/IN2021/050112

Citation	Pub.Date	Family	Pub.Date
US 7233227 B2	19-06-2007	AU 2003300639 B2	11-06-2009
		CA 2511244 C	05-07-2011
		CN 100345712 C	31-10-2007
		EP 1581414 B1	08-07-2020
		FR 2848951 B1	08-09-2006
		JP 4718839 B2	06-07-2011
		WO 2004056621 A1	08-07-2004
		ZA 200505230 B	27-12-2006
WO 2019165489 A1	06-09-2019	AU 2019227079 A1	10-09-2020
		CA 3092195 A1	06-09-2019
		EP 3758985 A1	06-01-2021
		US 2021086722 A1	25-03-2021