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

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
16 May 2013 (16.05.2013)

WIPO | PCT

(10) International Publication Number
WO 2013/070793 A1

(51) International Patent Classification:
B62H 5/00 (2006.01) *G08B 13/00* (2006.01)
B60L 11/18 (2006.01) *B60R 25/10* (2006.01)

(21) International Application Number:
PCT/US2012/063979

(22) International Filing Date:
7 November 2012 (07.11.2012)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
61/557,176 8 November 2011 (08.11.2011) US

(71) Applicant: **GOGORO, INC.**; 2F., No. 276, Jinguo Road, Xindian Dist., New Taipei City, 231 (TW).

(72) Inventors; and
(71) Applicants *(for US only)*: **WU, Yi-Tsung**; 10F., No. 52, Lane 447, Section 1 Wenhua, 3rd Rd., Linkou District, New Taipei City, 244 (TW). **LUKE, Hok-Sum, Horace** [US/US]; 3763 77th Place Southeast, Mercer Island, Washington 98040 (US). **HUNG, Huang-Cheng**; 7F., No. 33, Zuang 1st Street Taoyuan County, Taoyuan City, 330 (TW). **TAYLOR, Matthew Whiting** [US/US]; 15135 Uplands Way Southeast, North Bend, Washington 98045 (US).

(74) Agents: **BAUNACH, Jeremiah, J.** et al.; Seed Intellectual Property Law Group PLLC, Suite 5400, 701 Fifth Avenue, Seattle, Washington 98104-7064 (US).

(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, DK, DM, DO, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, GT, HN, HR, HU, ID, IL, IN, IS, JP, KE, KG, KM, KN, KP, KR, KZ, LA, LC, LK, LR, LS, LT, 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, SC, SD, SE, SG, SK, SL, SM, ST, SV, SY, TH, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, 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, 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, ML, MR, NE, SN, TD, TG).

Declarations under Rule 4.17:

— *as to applicant's entitlement to apply for and be granted a patent (Rule 4.17(ii))*

— *as to the applicant's entitlement to claim the priority of the earlier application (Rule 4.17(iii))*

[Continued on next page]

(54) Title: APPARATUS, METHOD AND ARTICLE FOR SECURITY OF VEHICLES

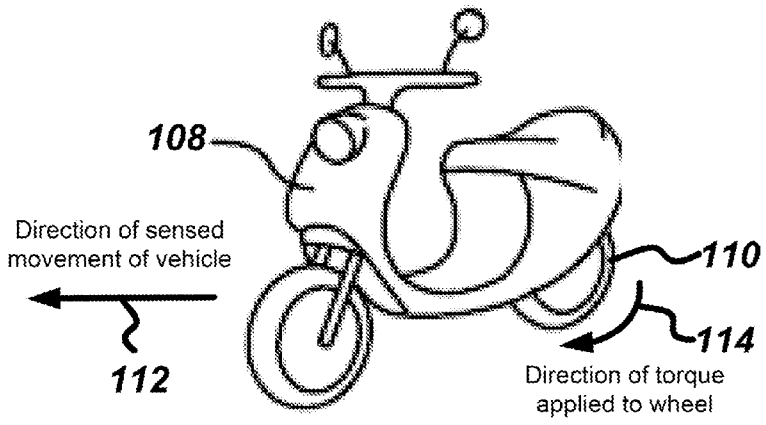

FIG. 1A

(57) Abstract: A vehicle has a security and anti-theft system that senses movement of the vehicle in a forward or backward direction when the vehicle is in a locked state, such as by detecting wheel rotation. Upon this detection, the security system signals the motor to counteract the wheel movement by rotating one or more wheels in the opposite direction of the direction of wheel rotation detected until the wheel rotation is no longer detected. The security and anti-theft system may determine whether the vehicle is in a locked state by detecting whether a key is present and/or by one or more communications received by an external wireless device.

WO 2013/070793 A1

Published:

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

— *before the expiration of the time limit for amending the claims and to be republished in the event of receipt of amendments (Rule 48.2(h))*

APPARATUS, METHOD AND ARTICLE FOR SECURITY OF VEHICLES

BACKGROUND

Technical Field

The present disclosure generally relates to security of vehicles, and particularly to prevention of vehicle theft.

Description of the Related Art

There are a wide variety of uses or applications for portable electrical power storage devices.

One such application is in the field of transportation. Hybrid and all-electric vehicles are becoming increasingly common. Such vehicles may achieve a number of advantages over traditional internal combustion engine vehicles. For example, hybrid or electrical vehicles may achieve higher fuel economy and may have little or even zero tail pipe pollution. In particular, all-electric vehicles may not only have zero tail pipe pollution, but may be associated with lower overall pollution. For example, electrical power may be generated from renewable sources (*e.g.*, solar, hydro). Also for example, electrical power may be generated at generation plants that produce no air pollution (*e.g.*, nuclear plants). Also for example, electrical power may be generated at generation plants that burn relatively "clean burning" fuels (*e.g.*, natural gas), which have higher efficiency than internal combustion engines, and/or which employ pollution control or removal systems (*e.g.*, industrial air scrubbers) which are too large, costly or expensive for use with individual vehicles.

Personal transportation vehicles such as combustion engine powered scooters and/or motorbikes are ubiquitous in many places, for example in the many large cities of Asia. Such scooters and/or motorbikes tend to be relatively inexpensive, particular as compared to automobiles, cars or trucks. Cities with high numbers of combustion engine scooters and/or

motorbikes also tend to be very densely populated and suffer from high levels of air pollution. When new, many combustion engine scooters and/or motorbikes are a relatively low polluting source of personal transportation. For instance, such scooters and/or motorbikes may have higher mileage ratings than larger vehicles. Some scooters and/or motorbikes may even be equipped with basic pollution control equipment (*e.g.*, catalytic converter). Unfortunately, factory specified levels of emission are quickly exceeded as the scooters and/or motorbikes are used and either not maintained and/or as the scooters and/or motorbikes are modified, for example by intentional or unintentional removal of catalytic converters. Often owners or operators of scooters and/or motorbikes lack the financial resources or the motivation to maintain their vehicles.

It is known that air pollution has a negative effect on human health, being associated with causing or exacerbating various diseases (*e.g.*, various reports tie air pollution to emphysema, asthma, pneumonia, cystic fibrosis as well as various cardiovascular diseases). Such diseases take large numbers of lives and severely reduce the quality of life of countless others.

Thus, use of hybrid or all electric vehicles may help diminish these negative environmental effects. However, owners or renters of electric vehicles such as electric scooters or motorbikes may often experience theft or compromised security of their vehicles due to their higher value and more expensive components.

BRIEF SUMMARY

A vehicle security system for a vehicle may be summarized as including at least one controller; and at least one communications module coupled to the at least one controller, wherein the at least one controller is configured to: receive information indicating whether the vehicle is in a state to allow operation of the vehicle; and in response to receiving the information whether the vehicle is in a state to allow operation of the vehicle, make a determination of whether to allow one or more wheels of the vehicle to roll based on the received information indicating whether the vehicle is in a state to allow operation of the vehicle.

The vehicle security system wherein the at least one controller may be further configured to: prevent the one or more wheels from rotating if the received information indicating whether the vehicle is in a state to allow operation of the vehicle indicates the vehicle is not in a state to allow operation of the vehicle.

The vehicle security system wherein the at least one controller may be configured to prevent the one or more wheels from rolling by being configured to: detect rotation of the one or more wheels in a first direction; and send a signal to a motor of the vehicle to rotate at least one of the one or more wheels in a second direction opposite of the first direction until the at least one controller no longer detects the rotation of the one or more wheels in the first direction.

The vehicle security system wherein the at least one controller may be configured to detect the motion of the one or more wheels in the first direction by being configured to: receive a motion detection signal from a motion sensor operably coupled to a drive system of the vehicle.

The vehicle security system wherein the at least one controller may be configured to detect the motion of the one or more wheels in the first direction by being configured to: receive a motion detection signal from a motion sensor configured to detect motion by using global positioning system data regarding location of the vehicle.

The vehicle security system may further include the motion sensor operably coupled to the at least one controller. The received information indicating whether the vehicle is in a state to allow operation of the vehicle may be information received indicating whether a key is present in an ignition of the vehicle and wherein the at least one controller is configured to prevent the one or more wheels from rolling if the received information indicates a key is not present in the ignition. The received information indicating whether the vehicle is in a state to allow operation of the vehicle may be information received wirelessly regarding authentication of an external device received via the communications module, and wherein the at least one controller is configured

to allow the one or more wheels to roll if the received information indicates the external device is authenticated and prevent the one or more wheels from rolling if the received information indicates the external device is not authenticated or indicates no external device is detected. The external device may be a key fob. The external device may be a mobile device.

The vehicle security system wherein the at least one controller may be configured to determine whether the received information indicates the external device is authenticated by being configured to: generate a challenge key to send to the external device; send the challenge key to the external device; receive a response from the external device to the sending of the challenge key, the response including a response code as part of the received information; generate an output from a secret algorithm using a secret key and the response code as input, the secret algorithm and the secret key configured to be known only to the vehicle security system and one or more authorized external devices; and compare the output from the secret algorithm to the response code, and wherein the at least one controller is configured to determine whether received information indicates the external device is authenticated based at least on the comparison. The at least one controller may be coupled to a motor of the vehicle. The vehicle may be an electric two-wheeled vehicle.

The vehicle security system wherein the at least one controller may be configured to prevent the one or more wheels from rolling by being configured to: detect motion of the vehicle in a first direction by being configured to receive a motion detection signal from a motion sensor; and send a signal to a motor of the vehicle to rotate at least one of the one or more wheels in a second direction associated with moving the vehicle in a direction opposite of the first direction until the at least one controller no longer detects the motion of the vehicle in the first direction from the motion sensor. The motion sensor may be operably coupled to the at least one controller and may be configured to detect the motion in the first direction via an accelerometer of the motion sensor.

A method of operating a vehicle security system for a vehicle may be summarized as including receiving information indicating whether the vehicle is in a state to allow operation of the vehicle; and preventing one or more wheels of the vehicle from rotating if the received information indicating whether the vehicle is in a state to allow operation of the vehicle indicates the vehicle is not in a state to allow operation of the vehicle. The state to allow operation of the vehicle may be a state in which a key is present in an ignition of the vehicle. The state to allow operation of the vehicle may be a state in which an authorized external device has been wirelessly authenticated by the vehicle security system.

The method wherein the preventing the one or more wheels of the vehicle from rolling may include detecting rotation of the one or more wheels in a first direction; and sending a signal to a motor of the vehicle to rotate at least one of the one or more wheels in a second direction opposite of the first direction until the at least one controller no longer detects the rotation of the one or more wheels in the first direction.

A vehicle may be summarized as including a motor; at least two wheels operably coupled to the motor; a motor controller operably coupled to the motor; one or more driver controls operably coupled to the motor controller, and wherein the motor controller includes a vehicle security system configured to: receive information indicating whether the vehicle is in a state to allow operation of the vehicle; and in response to receiving the information whether the vehicle is in a state to allow operation of the vehicle, make a determination of whether to allow one or more wheels of the vehicle to roll based on the received information indicating whether the vehicle is in a state to allow operation of the vehicle.

The vehicle wherein the vehicle security system may be configured to prevent the one or more wheels from rolling by being configured to: detect rotation of one or more of the at least two wheels in a first direction; and send a signal to a motor of the vehicle to rotate at least one of the at least two wheels in a second direction opposite of the first direction until the vehicle

security system no longer detects the rotation of the one or more of the at least two wheels in the first direction.

BRIEF DESCRIPTION OF THE SEVERAL VIEWS OF THE DRAWINGS

In the drawings, identical reference numbers identify similar elements or acts. The sizes and relative positions of elements in the drawings are not necessarily drawn to scale. For example, the shapes of various elements and angles are not drawn to scale, and some of these elements are arbitrarily enlarged and positioned to improve drawing legibility. Further, the particular shapes of the elements as drawn, are not intended to convey any information regarding the actual shape of the particular elements, and have been solely selected for ease of recognition in the drawings.

Figure 1A is a perspective view of a vehicle being prevented by a security system of the vehicle from rolling in a first direction, according to one non-limiting illustrated embodiment.

Figure 1B is a perspective view of the vehicle of Figure 1A being prevented by a vehicle security system of the vehicle from rolling in a second direction, according to one non-limiting illustrated embodiment.

Figure 2 is a block diagram of the vehicle security system of the vehicle of Figure 1A and Figure 1B, according to one non-limiting illustrated embodiment.

Figure 3 is a schematic view of a motor controller of the vehicle security system of Figure 2, according to one non-limiting illustrated embodiment.

Figure 4 is a flow diagram showing a high level method of operating the vehicle security system of Figure 2, according to one non-limiting illustrated embodiment.

Figure 5 is a flow diagram showing a low level method of operating the vehicle security system of Figure 2, according to one non-limiting illustrated embodiment, including detecting rotation of one or more wheels of the vehicle, useful in the method of Figure 4.

Figure 6 is a flow diagram showing a low level method of operating the vehicle security system of Figure 2, according to one non-limiting illustrated embodiment, including receiving information indicating whether a key is present in an ignition of the vehicle, useful in the method of Figure 4.

Figure 7 is a flow diagram showing a low level method of operating the vehicle security system of Figure 2, according to one non-limiting illustrated embodiment, including receiving information indicating whether an authorized external device has been wirelessly authenticated, useful in the method of Figure 4.

DETAILED DESCRIPTION

In the following description, certain specific details are set forth in order to provide a thorough understanding of various disclosed embodiments. However, one skilled in the relevant art will recognize that embodiments may be practiced without one or more of these specific details, or with other methods, components, materials, etc. In other instances, well-known structures associated with vending apparatus, batteries, locking mechanisms, wireless technologies, supercapacitors or ultracapacitors, power converters including but not limited to transformers, rectifiers, DC/DC power converters, switch mode power converters, controllers, and communications systems and structures and networks have not been shown or described in detail to avoid unnecessarily obscuring descriptions of the embodiments.

Unless the context requires otherwise, throughout the specification and claims which follow, the word “comprise” and variations thereof, such as, “comprises” and “comprising” are to be construed in an open, inclusive sense that is as “including, but not limited to.”

Reference throughout this specification to “one embodiment” or “an embodiment” means that a particular feature, structure or characteristic described in connection with the embodiment is included in at least one embodiment. Thus, the appearances of the phrases “in one embodiment” or “in an embodiment” in various places throughout this specification are not necessarily all referring to the same embodiment.

The use of ordinals such as first, second and third does not necessarily imply a ranked sense of order, but rather may only distinguish between multiple instances of an act or structure.

The headings and Abstract of the Disclosure provided herein are for convenience only and do not interpret the scope or meaning of the embodiments.

Figure 1A shows a perspective view of a vehicle 108 being prevented by a security system of the vehicle from rolling in a first direction, according to one non-limiting illustrated embodiment.

Although Figure 1A shows an electric scooter or motorbike, the vehicle 108 may be any powered vehicle or powered device with at least two wheels, including motorcycles cars, trucks, airplanes, trains, tractors, utility vehicles, maintenance vehicles, powered toys, etc. The vehicle 108 has a security system (shown in Figure 2) that senses movement of the vehicle forward 112 when the vehicle is in a state that is not to allow operation of the vehicle (i.e., a "locked state"). This locked state may include or be triggered by a number of factors, including, but not limited to: when a key is not detected as being in the ignition, when a vehicle has been manually switched into a "locked" state by a user, when an authorized wireless external device such as a key fob or mobile device has not been detected by the vehicle security system (either immediately or over a particular period of time, etc.).

Detection of the movement may be, for example, by detection of rotation of at least one wheel 110 in a first direction associated with movement of the vehicle forward 112. For example, movement of a front wheel and/or a back wheel of the vehicle 108 may be individually detected, such that if a thief lifted the vehicle 108 so that only the front wheel or back wheel was rolling, this movement of the vehicle would also be detected. However, detection may be via other motion sensors of the vehicle security system, including those using accelerometers, and global positioning system (GPS) data, etc., of the vehicle security system. For example, the motion sensor may be configured to detect motion by using global positioning system data regarding location of the

vehicle. Upon the detection of the movement forward 112 (e.g., by detection of rotation of the at least one wheel 110 in the first direction), the vehicle security system causes the wheel 110 to rotate in a second direction opposite of the first direction (counteracting the rotation of the at least one wheel 110 in the first direction) until the vehicle security system no longer detects the rotation of the at least one wheel 110 in the first direction. In an embodiment in which a motion sensor, such as one using an accelerometer or GPS data, is used by the vehicle security system to detect movement of the vehicle 108 forward 112, the vehicle security system causes the at least one wheel 110 to rotate in the second direction opposite of the first direction (counteracting any rotation of the wheel in the first direction) until the vehicle security system no longer detects the movement forward by the motion sensor. In this manner, the at least one wheel 110 is prevented from rotating in the first direction when the vehicle is in the locked state. The vehicle security system thus hinders forward 112 rolling of the vehicle 108 to avoid theft and tampering of the vehicle 108 when the vehicle is in the locked state. Thus, the vehicle security system also prevents unintended forward rolling of the vehicle downhill or due to accidental bumping of the vehicle 108.

Figure 1B shows perspective view of the vehicle 108 of Figure 1A being prevented by the vehicle security system of the vehicle 108 from rolling in a second direction, according to one non-limiting illustrated embodiment.

As shown in Figure 2B, detection by the vehicle security system may be of backward movement 116 of the vehicle 108. For example, this detection of backward movement 116 may be by the vehicle security system detecting rotation of the at least one wheel 110 in a second direction opposite of the first direction associated with movement of the vehicle 108 forward 112. However, detection of movement may be via other motion sensors of the vehicle security system, including those using accelerometers, etc., of the vehicle security system. Upon the detection of the backward movement 116 (e.g., by detection of rotation of the at least one wheel 110 in the second direction opposite of the first direction), the vehicle security system causes the

at least one wheel 110 to rotate in the first direction opposite of the second direction (counteracting the rotation of the wheel in the second direction) until the vehicle security system no longer detects the rotation of the at least one wheel 110 in the second direction. In an embodiment in which a motion sensor, such as one using an accelerometer, is used by the vehicle security system to detect backward movement 116 of the vehicle 108, the vehicle security system causes the at least one wheel 110 to rotate in the first direction opposite of the second direction (counteracting any rotation of the wheel in the second direction) until the vehicle security system no longer detects the movement forward by the motion sensor. In this manner, the at least one wheel 110 is also prevented from rotating in the second direction when the vehicle 108 is in the locked state, and thus the vehicle security system hinders both backward 116 and forward 112 rolling of the vehicle 108 to avoid theft and tampering of the vehicle 108 when the vehicle is in the locked state. Thus, the vehicle security system also prevents unintended backward rolling of the vehicle downhill or due to accidental bumping of the vehicle 108.

Figure 2 shows a block diagram of the vehicle security system 200 of the vehicle 108 of Figure 1A and Figure 1B, according to one non-limiting illustrated embodiment.

Shown is a key sensor 202, a motion sensor 204, a motor controller 206, manual controls 208, a motor 212, a drive system 214, and an external device 216. The motor controller 206 has an input 226 from the key sensor 202, an input 222 from the motion sensor 204 and an input 228 from the manual controls 208. The motor 212 has an input 218 from the motor controller 206 and the drive system 214 has an input 220 from the motor 212. The motion sensor 204 also has an input 224 from the drive system 214. Also, the external device 216 is a wireless device that is in operable wireless communication with the motor controller 206 via a wireless signal 230. One or more of the connections between the components in the vehicle security system 200 may be logical or physical connections and communication

between the components of the vehicle security system 200 may be via any operable combination of analog, digital, wired or wireless signals.

The motor controller 206 is configured to control operation the motor 212 in one or more of a first direction and a second direction based on input received from the manual controls 208, key sensor 202, motion sensor 204 and/or external device 216. The motor 212 is configured to run the drive system 214 in order to rotate one or more wheels (e.g., the at least one wheel 110 shown in figure 1A and Figure 1B) of the vehicle 108 corresponding to a direction in which the motor 212 is running according to the input received from the motor controller 206. The drive system 214, for example, may include components (e.g., a transmission or other mechanical components) to transmit power from the motor to the one or more wheels.

The motion sensor 204 is configured to detect movement of the vehicle 108 in a forward and/or backward direction. In one embodiment, this detection of the movement may be, for example, by detection of rotation of at least one wheel in a first direction associated with movement of the vehicle forward. Also, movement of a front wheel and/or a back wheel of the vehicle 108 may be individually detected, such that if a thief lifted the vehicle 108 so that only the front wheel or back wheel was rolling, this movement of the vehicle would also be detected. Detection of rotation of the at least one wheel, may be via the input 224 from the drive system 214. The input 224 may be mechanical or electronic. For example, the drive system 224 may include a separate drive cable, or shared drive cable of a speedometer, tachometer, or odometer of the vehicle 108 connected to a set of gears in the transmission of the drive system 214, so that when the at least one wheel of the vehicle rotates, the gears turn a mandrel inside a flexible shaft of the drive cable. For example, the drive cable may be connected to the motion sensor 204 as the input line 224. The direction of rotation of the mandrel thus communicates the corresponding direction of the rotation of the at least one wheel to the motion sensor 204. In other embodiments, the drive cable may be driven directly by rotation of the at least one wheel or wheel axle (including that of either a front wheel or a back wheel)

via a gear assembly (not shown) operably coupled to the drive cable and wheel or axle. In yet other embodiments, a mechanical or electric wheel rotation detection system may be coupled directly to and driven directly by one or more other wheels or wheel axles, or to a wheel or wheel axle that is not operably coupled to the drive system 214 (including that of a front wheel or a back wheel).

Any method or system for mechanically or electrically, or electronically detecting the direction of rotational movement of a wheel of a vehicle may be used, including those systems using an electric rotation sensor mounted in the transmission of the drive system 214 that delivers a series of electronic pulses whose frequency or amplitude correspond to the direction of rotation the driveshaft of the drive system 214 or wheel axle. Also, detection of wheel rotation may be made by the motion sensor 204 mechanically and/or electronically detecting rotation or phase change of the motor 212. The rotation or phase change of the motor 212 may be caused by the drive system 214 being mechanically coupled to the wheel and the motor, or in some embodiments, the wheel being directly coupled to the axle or armature of the motor 212. Thus, the rotation of the motor 212 causes rotation of the wheel and, vice versa, the rotation of the wheel may cause rotation or phase change of the motor 212. Any method or system that mechanically, electrically or electronically detects rotational movement or phase change of the motor 212, and/or the direction thereof, may be used. For example, the motion sensor 204, being electronically and/or mechanically coupled directly or indirectly to the motor 212 and/or drive system 214, may directly or indirectly detect changes or disturbances in magnetic fields caused by the rotation or phase change of the motor 212 or detect electrical current caused by the rotation or phase change of the motor 212. The properties of the detected disturbances in magnetic fields caused by the rotation or phase change of the motor 212 and/or the properties of the electrical current caused by the rotation or phase change of the motor 212 (e.g., the direction of the electrical current) may correspond to, and thus indicate to the motion sensor 204, the direction of the rotation of the wheel.

The motion sensor 204 being electronically and/or mechanically coupled directly to the motor 212 may be represented by another connection line (not shown) in Figure 2 between the motion sensor 204 and the motor 214.

In other embodiments, when the vehicle 108 goes into a locked state an electronic or mechanical switch (not shown) within of the motion sensor 204, or coupled to an input of the motion sensor 204, and coupled to the motor 212 may electronically or mechanically be set to one state by the motor controller 206 or manual controls 208. This switch may then be mechanically or electronically switched to another state caused by the rotation or phase change of the motor 212.

Also included may be systems that otherwise use sensors to sense magnetic fields, as the at least one wheel rotates, of one or more magnets coupled to the at least one wheel (including a front wheel or a back wheel). However, detection by the motion sensor 204 may be via other sensors of the motion sensor 204, including one or more accelerometers, a sensor configured to detect motion by GPS data regarding location of the vehicle, etc., to detect movement and/or direction of movement of the vehicle. Upon the detection of the movement forward or backward (e.g., by detection of rotation of the at least one wheel in the first direction or the second direction), the motion sensor 204 communicates the current direction of movement to the motor controller 206.

If the vehicle 108 is in a locked state, the motor controller 206 may then send a signal via the input 218 to the motor 212 to operate the drive system 214 to rotate (i.e., apply torque to) the at least one wheel (including, in various embodiments having various different drive systems, applying torque to the front wheel, back wheel and/or all wheels) in a direction opposite of that detected by the motion sensor (counteracting any rotation of the at least one wheel) until the motor controller 206 no longer receives input from the motion sensor regarding the movement of the vehicle by the motion sensor 204, or until the motion sensor 204 communicates to the motor controller 206 that the vehicle 108 is no longer moving forward or backward. For example, the input

220 may be a mechanical input or mechanical connection between the motor 212 and the drive system that causes the drive system 214 to rotate the at least one wheel of the vehicle 108 in the appropriate direction.

The motor controller 206 is configured to receive information regarding whether the vehicle is in a locked state from one or more of the key sensor 202, the manual controls 208 and/or the external device 216. For example, they key sensor 202 may detect an electrical signal caused by a physical key being placed in an ignition or other key hole in the vehicle 108, or by otherwise detecting a physical key being present in the vehicle 108. The key sensor 202 may then communicate this via input 226 to the controller to indicate that the vehicle 108 is not in a locked state. The key sensor 202 may also or instead communicate the absence of a key via input 226 to the motor controller 206 to indicate that the vehicle 108 is in a locked state. Various manual controls 208 of the vehicle 108 such as switches or buttons operated or enabled by keys, etc., may also be used to indicate via input 228 to the motor controller 206 whether the vehicle 108 is in a locked state.

A wireless external device 216 including, but not limited to: card keys, access cards, credit cards, access control key fobs, mobile computing devices, cellular telephones, personal digital assistants (PDAs), smart phones, battery chargers, other access control devices, etc., may be used to communicate over a wireless signal 230 to indicate whether the vehicle 108 is in a locked state and/or to communicate authentication information of the external device 216 and/or the motor controller 206. The external device 216 may include a communications subsystem (not shown), for example, a communications subsystem including components enabling short range (*e.g.*, via Bluetooth, near field communication (NFC), radio frequency identification (RFID) components and protocols) or longer range wireless communications (*e.g.*, over a wireless LAN, satellite, or cellular network). The communications subsystem of the external device 216 may include one or more modems or one or more Ethernet or other types of communications cards or components for doing so to communicate with the motor controller 206. Also, the absence of

the wireless signal 230 (either immediately, or over a period of time) authorizing or indicating the motor controller is in an unlocked state, or putting the vehicle 108 into an unlocked state may cause the motor controller 206 to automatically determine that the vehicle 108 is in a locked state.

In some embodiments, the wireless signal 230 received from the external device 216 may include a code that may be authenticated by the motor controller 206 in order to ensure the signal 230 is being received from an authorized device. For example, the code may be time-sensitive code such as a “hopping” code or a “rolling” code to provide such security. In the case of a 40-bit rolling code, forty bits provide 240 (about 1 trillion) possible codes. However, codes of other bit lengths may be used instead. The external device 216 memory (e.g., ROM 212) may hold the current 40-bit code. The external device 216 then sends that 40-bit code to the motor controller 206 for the motor controller 206 to determine whether the vehicle 108 is in an unlocked state. The motor controller 206 also holds the current 40-bit code. If the motor controller 206 receives the 40-bit code it expects, it then determines the vehicle 108 is in an unlocked state. If the motor controller 206 does not receive the 40-bit code it expects, it then determines the vehicle 108 is in a locked state. In some embodiments, the motor controller 206 determines the vehicle 108 is in a locked state if the motor controller 206 does not receive the 40-bit code it expects, or is not able to receive any authorized or authenticated wireless signal 230 over a determined period of time.

Both the external device 216 and the motor controller 206 use the same pseudo-random number generator (e.g., implemented by the respective processors of the external device 216 and the motor controller 206) to generate the 40-bit code. When the motor controller 206 receives a valid code form the external device 216, it uses the same pseudo-random number generator to generate the next code relative to the valid code received and communicates wirelessly with the external device 216 to instruct it to also generate the next code using the same pseudo-random number generator, which the external device 216 stores for the next use. In this way, the external device 216 and the

motor controller 206 are synchronized. In some embodiments, the motor controller 206 only determines the vehicle 108 is in an unlocked state if it receives the code it expects.

In some embodiments, the motor controller 206 may accept any of the next 256 possible valid codes in the pseudo-random number sequence. This way, if the motor controller 206 and the external device 216 for some reason become unsynchronized by 256 rolling codes or less, the motor controller 206 would still accept the transmission from the external device 216, and generate the next code relative to the valid code received.

In some embodiments, the motor controller 206 and the external device 216 store a common secret key or code and use a common secret algorithm for authentication of the external device 216. The common secret algorithm, for example, can be a hash function or other algorithm which takes the secret key and at least one other key or code as input and generates different output based on the secret key and different input. The common secret algorithm may be executed by respective processors of the motor controller 206 and the external device 216 using stored instructions on respective computer readable media of the motor controller 206 and the external device 216 or on respective configured hardware or firmware components of the of motor controller 206 and external device 216. The common secret algorithm and common secret key or code may be initially encoded, programmed or installed in the motor controller 206 and external device 216 in a secure fashion such that they are irretrievable or otherwise protected from being discovered. The common secret algorithm and common secret key or code are not communicated between the motor controller 206 and external device 216 during the authentication process.

In response to receiving an authentication beacon or request from the external device 216 via the wireless signal 230 (which may have been sent in response to a wireless signal or beacon received from the motor controller 206), the motor controller 206 generates a challenge key and sends this challenge key to the external device 216. In response to receiving the

challenge key, the external device 216 uses the secret algorithm and the common secret key to generate a response value and sends this response value to the motor controller 206. The motor controller 206 then verifies the response value by using the generated challenge key and secret key as input to the secret algorithm to generate an output value from the secret algorithm. The motor controller 206 then compares this output value from the secret algorithm to the response value received from the external device 216. If the output from the secret algorithm generated by the motor controller 206 and the response value received from the external device 216 match, then the external device 216 is authenticated and the motor controller 206 may then take actions accordingly, such as determining the vehicle 108 is in an unlocked state. If the output from the secret algorithm generated by the motor controller 206 and the response value received from the external device 216 do not match, then the external device 216 is not authenticated and the motor controller 206 may then take no action, or take other actions accordingly, such as determining the vehicle 108 is in a locked state. In some embodiments, the particular action to take (e.g., determining that the vehicle 108 is in a locked state, or determining that the vehicle 108 is in an unlocked state) may be sent as a lock or unlock command from the external device 216 along with the authentication information.

If the motor controller 206 determines the vehicle 108 is not in a locked state, the motor controller 206 will ignore the input received from the motion sensor 204 sent for purposes of counteracting wheel movement. Also, in some embodiments, the motion sensor 204 will be configured to not operate at all unless the vehicle 108 is in an unlocked state.

Figure 3 is a schematic view diagram of the motor controller 206 of the vehicle security system 200 of Figure 2, according to one non-limiting illustrated embodiment.

The motor controller 206 includes a controller 310, a communications subsystem 306, and a power interface 420.

The controller 310, for example, is a microprocessor, microcontroller, programmable logic controller (PLC), programmable gate array (PGA), application specific integrated circuit (ASIC) or another controller capable of receiving signals from various sensors, performing logical operations, and sending signals to various components. Typically, the controller 310 may take the form of a microprocessor (*e.g.*, INTEL, AMD, ATOM). The motor controller 206 may also be coupled to one or more non-transitory processor- or computer-readable storage media, for example read only memory (ROM) 312, random access memory (RAM) 314, and other storage 316 (*e.g.*, solid-state storage media such as flash memory or EEPROM, or spinning storage media such as hard disk). The non-transitory processor- or computer-readable storage media 312, 314, 316 may be in addition to any non-transitory storage medium (*e.g.*, registers) which is part of the controller 310. The motor controller 206 may include one or more buses 318 (only one illustrated) coupling various components together, for example one or more power buses, instruction buses, data buses, etc. As shown, the controller includes inputs 228 from the manual controls 208, input 222 from the motion sensor, and input 226 from the key sensor 202 (shown in Figure 2).

As illustrated, the ROM 312, or some other one of the non-transitory processor- or computer-readable storage media 312, 314, 316, stores instructions and/or data or values for variables or parameters. The sets of data may take a variety of forms, for example a lookup table, a set of records in a database, etc. The instructions and sets of data or values are executable by the controller 310. Execution of the instructions and sets of data or values causes the controller 310 to perform specific acts to determine whether the vehicle is in a locked state based on the input received via input 228 from the manual controls 208, input 222 from the motion sensor and/or input 226 from the key sensor 202 (shown in Figure 2). Execution of the instructions and sets of data or values also causes the controller 310 to perform specific acts to perform authentication of external devices and cause the motor controller 206 to generate control signals to drive a motor of the vehicle 108 in one or more

directions. Also, such acts may include, for example, operations implementing a pseudo-random number to generate a rolling code as described above. Specific operation of the motor controller 206 is described herein and also below with reference to various flow diagrams (Figures 4-7).

The controller 310 may use RAM 314 in a conventional fashion, for volatile storage of instructions, data, etc. The controller 310 may use data store 316 to log or retain information, for example, information regarding current rotational direction of wheels of the vehicle, motion sensor input, information regarding currently sensed direction of movement of the vehicle, vehicle profile information, vehicle specifications, motor information and/or motor specifications, security codes, credentials, security certificates, passwords, other vehicle information, etc. The instructions are executable by the controller 310 to control operation of the motor controller 206 in response to input from remote systems such as those of external devices described herein, including those embedded in portable electronic storage device collection, charging and distribution machines.

The controller 310 may also receive signals from various sensors and/or components of an external device via the communications subsystem 306 of the motor controller 206. This information may include information that characterizes or is indicative of the authenticity, authorization level, operation, status, or condition of such components and/or external devices.

The communications subsystem 306 may include one or more communications modules or components which facilitate communications with the various components of the external device 216 of Figure 2 (*e.g.*, such as to receive a security code) and/or of other external devices and also, such that data may be exchanged between the motor controller 206 and the external device 216 for authentication purposes. The communications subsystem 306 may provide wired and/or wireless communications. The communications subsystem 306 may include one or more ports, wireless receivers, wireless transmitters or wireless transceivers to provide wireless signal paths to the various remote components or systems. The communications subsystem 306

may, for example, include components enabling short range (*e.g.*, via Bluetooth, near field communication (NFC), radio frequency identification (RFID) components and protocols) or longer range wireless communications (*e.g.*, over a wireless LAN, satellite, or cellular network) and may include one or more modems or one or more Ethernet or other types of communications cards or components for doing so. The remote communications subsystem 306 may include one or more bridges or routers suitable to handle network traffic including switched packet type communications protocols (TCP/IP), Ethernet or other networking protocols.

Figure 4 shows a high level method 400 of operating the vehicle security system 200 of Figure 2, according to one non-limiting illustrated embodiment.

At 402, the vehicle security system 200 receives information indicating whether the vehicle is in a state to allow operation of the vehicle.

At 404, the vehicle security system 200 prevents one or more wheels of the vehicle from rolling if the received information indicating whether the vehicle is in a state to allow operation of the vehicle indicates the vehicle is not in a state to allow operation of the vehicle.

Figure 5 shows a low level method 500 of operating the vehicle security system 200 of Figure 2, according to one non-limiting illustrated embodiment, including detecting rotation of one or more wheels of the vehicle, useful in the method 400 of Figure 4.

At 502, the vehicle security system 200 detects motion of the one or more wheels in a first direction.

At 504, the vehicle security system 200 sends a signal to a motor of the vehicle to rotate at least one of the one or more wheels in a second direction opposite of the first direction until the at least one controller no longer detects the motion of the one or more wheels in the first direction.

Figure 6 shows a low level method 600 of operating the vehicle security system 200 of Figure 2, according to one non-limiting illustrated

embodiment, including receiving information indicating whether a key is present in an ignition of the vehicle, useful in the method of Figure 4.

At 602, the vehicle security system 200 receives information indicating whether a key is present in an ignition of the vehicle.

At 604 the vehicle security system 200 prevents the one or more wheels from rolling if the received information indicates a key is not present in the ignition.

Figure 7 shows a low level method 700 of operating the vehicle security system 200 of Figure 2, according to one non-limiting illustrated embodiment, including receiving information indicating whether an authorized external device has been wirelessly authenticated, useful in the method of Figure 4.

At 702, the vehicle security system 200 receives information indicating whether an authorized external device has been wirelessly authenticated by the vehicle security system.

At 704, the vehicle security system 200 allows the one or more wheels to roll if the received information indicates the external device is authenticated and prevents the one or more wheels from rolling if the received information indicates the external device is not authenticated, or indicates no external device is detected

The various methods described herein may include additional acts, omit some acts, and/or may perform the acts in a different order than set out in the various flow diagrams.

The foregoing detailed description has set forth various embodiments of the devices and/or processes via the use of block diagrams, schematics, and examples. Insofar as such block diagrams, schematics, and examples contain one or more functions and/or operations, it will be understood by those skilled in the art that each function and/or operation within such block diagrams, flowcharts, or examples can be implemented, individually and/or collectively, by a wide range of hardware, software, firmware, or virtually any combination thereof. In one embodiment, the present subject matter may be

implemented via one or more microcontrollers. However, those skilled in the art will recognize that the embodiments disclosed herein, in whole or in part, can be equivalently implemented in standard integrated circuits (*e.g.*, Application Specific Integrated Circuits or ASICs), as one or more computer programs executed by one or more computers (*e.g.*, as one or more programs running on one or more computer systems), as one or more programs executed by on one or more controllers (*e.g.*, microcontrollers) as one or more programs executed by one or more processors (*e.g.*, microprocessors), as firmware, or as virtually any combination thereof, and that designing the circuitry and/or writing the code for the software and/or firmware would be well within the skill of one of ordinary skill in the art in light of the teachings of this disclosure.

When logic is implemented as software and stored in memory, logic or information can be stored on any non-transitory computer-readable medium for use by or in connection with any processor-related system or method. In the context of this disclosure, a memory is a nontransitory computer- or processor-readable storage medium that is an electronic, magnetic, optical, or other physical device or means that non-transitorily contains or stores a computer and/or processor program. Logic and/or the information can be embodied in any computer-readable medium for use by or in connection with an instruction execution system, apparatus, or device, such as a computer-based system, processor-containing system, or other system that can fetch the instructions from the instruction execution system, apparatus, or device and execute the instructions associated with logic and/or information.

In the context of this specification, a “computer-readable medium” can be any physical element that can store the program associated with logic and/or information for use by or in connection with the instruction execution system, apparatus, and/or device. The computer-readable medium can be, for example, but is not limited to, an electronic, magnetic, optical, electromagnetic, infrared, or semiconductor system, apparatus or device. More specific examples (a non-exhaustive list) of the computer readable medium would include the following: a portable computer diskette (magnetic, compact flash

card, secure digital, or the like), a random access memory (RAM), a read-only memory (ROM), an erasable programmable read-only memory (EPROM, EEPROM, or Flash memory), a portable compact disc read-only memory (CDROM), and digital tape.

The various embodiments described above can be combined to provide further embodiments. To the extent that they are not inconsistent with the specific teachings and definitions herein, all of the U.S. patents, U.S. patent application publications, U.S. patent applications, foreign patents, foreign patent applications and non-patent publications referred to in this specification and/or listed in the Application Data Sheet, including but not limited to: U.S. provisional patent application Serial No. 61/557,176 entitled "APPARATUS, METHOD AND ARTICLE FOR SECURITY OF VEHICLES" and filed November 8, 2011 (Attorney Docket No. 170178.409P1); U.S. patent application Serial No. 13/559,314 entitled "APPARATUS, METHOD AND ARTICLE FOR COLLECTION, CHARGING AND DISTRIBUTING POWER STORAGE DEVICES, SUCH AS BATTERIES" and filed July 26, 2012 (Attorney Docket No. 170178.401); U.S. patent application Serial No. 13/559,091 entitled "APPARATUS, METHOD AND ARTICLE FOR REDISTRIBUTING POWER STORAGE DEVICES, SUCH AS BATTERIES, BETWEEN COLLECTION, CHARGING AND DISTRIBUTION MACHINES" and filed July 26, 2012 (Attorney Docket No. 170178.402); U.S. patent application Serial No. 13/559,038 entitled "APPARATUS, METHOD AND ARTICLE FOR AUTHENTICATION, SECURITY AND CONTROL OF POWER STORAGE DEVICES SUCH AS BATTERIES" and filed July 26, 2012 (Attorney Docket No. 170178.403); U.S. patent application Serial No. 13/559,010 entitled "APPARATUS, METHOD AND ARTICLE FOR AUTHENTICATION, SECURITY AND CONTROL OF POWER STORAGE DEVICES, SUCH AS BATTERIES, BASED ON USER PROFILES" and filed July 26, 2012 (Attorney Docket No. 170178.404); U.S. patent application Serial No. 13/559,259 entitled "THERMAL MANAGEMENT OF COMPONENTS IN ELECTRIC MOTOR DRIVE VEHICLES" and filed July 26, 2012 (Attorney Docket No. 170178.406); U.S.

patent application Serial No. 13/559,264, entitled "DYNAMICALLY LIMITING VEHICLE OPERATION FOR BEST EFFORT ECONOMY" and filed July 26, 2012 (Attorney Docket No. 170178.407); U.S. patent application Serial No. 13/559,054 entitled "APPARATUS, METHOD AND ARTICLE FOR PHYSICAL SECURITY OF POWER STORAGE DEVICES IN VEHICLES" and filed July 26, 2012 (Attorney Docket No. 170178.408); U.S. patent application Serial No. 13/559,125 entitled "APPARATUS, METHOD AND ARTICLE FOR A POWER STORAGE DEVICE COMPARTMENT" and filed July 26, 2012 (Attorney Docket No. 170178.412); U.S. patent application Serial No. 13/559,390 entitled "APPARATUS, METHOD AND ARTICLE FOR PROVIDING VEHICLE DIAGNOSTIC DATA" and filed July 26, 2012 (Attorney Docket No. 170178.417); U.S. patent application Serial No. 13/559,333 entitled "APPARATUS, METHOD AND ARTICLE FOR PROVIDING LOCATIONS OF POWER STORAGE DEVICE COLLECTION, CHARGING AND DISTRIBUTION MACHINES" and filed July 26, 2012 (Attorney Docket No. 170178.418); U.S. patent application Serial No. 13/559,343 entitled "APPARATUS, METHOD AND ARTICLE FOR PROVIDING INFORMATION REGARDING AVAILABILITY OF POWER STORAGE DEVICES AT A POWER STORAGE DEVICE COLLECTION, CHARGING AND DISTRIBUTION MACHINE" and filed July 26, 2012 (Attorney Docket No. 170178.419); and U.S. patent application Serial No. 13/559,064 entitled "APPARATUS, METHOD AND ARTICLE FOR RESERVING POWER STORAGE DEVICES AT RESERVING POWER STORAGE DEVICE COLLECTION, CHARGING AND DISTRIBUTION MACHINES" and filed on July 26, 2012 (Attorney Docket No. 170178.423); U.S. patent application Serial No. 13/646,320 entitled "DETECTIBLE INDICATION OF AN ELECTRIC MOTOR VEHICLE STANDBY MODE" and filed on October 5, 2012 (Attorney Docket No. 170178.405); U.S. patent application Serial No. 13/650,498 entitled "ELECTRIC DEVICES" and filed on October 12, 2012 (Attorney Docket No. 170178.414); U.S. patent application Serial No. 13/650,392 entitled "DRIVE ASSEMBLY FOR ELECTRIC DEVICE" and filed on October 12, 2012 (Attorney Docket No. 170178.413); U.S. patent application

Serial No. 13/650,395 entitled "ELECTRIC DEVICE DRIVE ASSEMBLY AND COOLING SYSTEM FOR ELECTRIC DEVICE DRIVE" and filed on October 12, 2012 (Attorney Docket No. 170178.415); U.S. patent application Serial No. 13/559,054 entitled "ELECTRIC DEVICE DRIVE ASSEMBLY AND COOLING SYSTEM FOR ELECTRIC DEVICE DRIVE" and filed on July 26, 2012 (Attorney Docket No. 170178.408); U.S. patent application Serial No. 13/559,125 entitled "ELECTRIC DEVICE DRIVE ASSEMBLY AND COOLING SYSTEM FOR ELECTRIC DEVICE DRIVE" and filed on July 26, 2012 (Attorney Docket No. 170178.412) are incorporated herein by reference, in their entirety. Aspects of the embodiments can be modified, if necessary, to employ systems, circuits and concepts of the various patents, applications and publications to provide yet further embodiments.

While generally discussed in the environment and context of physical security of personal transportation vehicles such as all-electric scooters and/or motorbikes, the teachings herein can be applied in a wide variety of other environments, including other vehicular as well as non-vehicular environments.

The above description of illustrated embodiments, including what is described in the Abstract of the Disclosure, is not intended to be exhaustive or to limit the embodiments to the precise forms disclosed. Although specific embodiments and examples are described herein for illustrative purposes, various equivalent modifications can be made without departing from the spirit and scope of the disclosure, as will be recognized by those skilled in the relevant art.

These and other changes can be made to the embodiments in light of the above-detailed description. In general, in the following claims, the terms used should not be construed to limit the claims to the specific embodiments disclosed in the specification and the claims, but should be construed to include all possible embodiments along with the full scope of equivalents to which such claims are entitled. Accordingly, the claims are not limited by the disclosure.

CLAIMS

I claim:

1. A vehicle security system for a vehicle, comprising:

at least one controller; and

at least one communications module coupled to the at least one controller, wherein the at least one controller is configured to:

receive information indicating whether the vehicle is in a state to allow operation of the vehicle; and

in response to receiving the information whether the vehicle is in a state to allow operation of the vehicle, make a determination of whether to allow one or more wheels of the vehicle to roll based on the received information indicating whether the vehicle is in a state to allow operation of the vehicle.

2. The vehicle security system of claim 1 wherein the at least one controller is further configured to:

prevent the one or more wheels from rotating if the received information indicating whether the vehicle is in a state to allow operation of the vehicle indicates the vehicle is not in a state to allow operation of the vehicle.

3. The vehicle security system of claim 1 wherein the at least one controller is configured to prevent the one or more wheels from rolling by being configured to:

detect rotation of the one or more wheels in a first direction; and

send a signal to a motor of the vehicle to rotate at least one of the one or more wheels in a second direction opposite of the first direction until the at least one controller no longer detects the rotation of the one or more wheels in the first direction.

4. The vehicle security system of claim 3 wherein the at least one controller is configured to detect the motion of the one or more wheels in the first direction by being configured to:

receive a motion detection signal from a motion sensor operably coupled to a drive system of the vehicle or coupled to a motor of the vehicle.

5. The vehicle security system of claim 1 wherein the at least one controller is configured to detect the motion of the one or more wheels in the first direction by being configured to:

receive a motion detection signal from a motion sensor configured to detect motion by using global positioning system data regarding location of the vehicle.

6. The vehicle security system of claim 5, further comprising the motion sensor operably coupled to the at least one controller.

7. The vehicle security system of claim 1 wherein the received information indicating whether the vehicle is in a state to allow operation of the vehicle is information received indicating whether a key is present in an ignition of the vehicle and wherein the at least one controller is configured to prevent the one or more wheels from rolling if the received information indicates a key is not present in the ignition.

8. The vehicle security system of claim 1 wherein the received information indicating whether the vehicle is in a state to allow operation of the vehicle is information received wirelessly regarding authentication of an external device received via the communications module, and wherein the at least one controller is configured to allow the one or more wheels to roll if the received information indicates the external device is authenticated and prevent the one or more wheels from rolling if the received

information indicates the external device is not authenticated or indicates no external device is detected.

9. The vehicle security system of claim 8 wherein the external device is a key fob.

10. The vehicle security system of claim 8 wherein the external device is a mobile device.

11. The vehicle security system of claim 8 wherein the at least one controller is configured to determine whether the received information indicates the external device is authenticated by being configured to:

generate a challenge key to send to the external device;

send the challenge key to the external device;

receive a response from the external device to the sending of the challenge key, the response including a response code as part of the received information;

generate an output from a secret algorithm using a secret key and the response code as input, the secret algorithm and the secret key configured to be known only to the vehicle security system and one or more authorized external devices; and

compare the output from the secret algorithm to the response code, and wherein the at least one controller is configured to determine whether received information indicates the external device is authenticated based at least on the comparison.

12. The vehicle security system of claim 1 wherein the at least one controller is coupled to a motor of the vehicle.

13. The vehicle security system of claim 1 wherein the vehicle is an electric two-wheeled vehicle.

14. The vehicle security system of claim 1 wherein the at least one controller is configured to prevent the one or more wheels from rolling by being configured to:

detect motion of the vehicle in a first direction by being configured to receive a motion detection signal from a motion sensor; and

send a signal to a motor of the vehicle to rotate at least one of the one or more wheels in a second direction associated with moving the vehicle in a direction opposite of the first direction until the at least one controller no longer detects the motion of the vehicle in the first direction from the motion sensor.

15. The vehicle security system of claim 14 wherein the motion sensor is operably coupled to the at least one controller and is configured to detect the motion in the first direction via an accelerometer of the motion sensor.

16. A method of operating a vehicle security system for a vehicle, the method comprising:

receiving information indicating whether the vehicle is in a state to allow operation of the vehicle; and

preventing one or more wheels of the vehicle from rotating if the received information indicating whether the vehicle is in a state to allow operation of the vehicle indicates the vehicle is not in a state to allow operation of the vehicle.

17. The method of claim 16 wherein the state to allow operation of the vehicle is a state in which a key is present in an ignition of the vehicle.

18. The method of claim 16 wherein the state to allow operation of the vehicle is a state in which an authorized external device has been wirelessly authenticated by the vehicle security system.

19. The method of claim 16, wherein the preventing the one or more wheels of the vehicle from rolling includes:

detecting rotation of the one or more wheels in a first direction; and

sending a signal to a motor of the vehicle to rotate at least one of the one or more wheels in a second direction opposite of the first direction until the at least one controller no longer detects the rotation of the one or more wheels in the first direction.

20. A vehicle, comprising:

a motor;

at least two wheels operably coupled to the motor;

a motor controller operably coupled to the motor;

one or more driver controls operably coupled to the motor controller, and wherein the motor controller includes a vehicle security system configured to:

receive information indicating whether the vehicle is in a state to allow operation of the vehicle; and

in response to receiving the information whether the vehicle is in a state to allow operation of the vehicle, make a determination of whether to allow one or more wheels of the vehicle to roll based on the received information indicating whether the vehicle is in a state to allow operation of the vehicle.

21. The vehicle of claim 20 wherein the vehicle security system is configured to prevent the one or more wheels from rolling by being configured to:

detect rotation of one or more of the at least two wheels in a first direction; and

send a signal to a motor of the vehicle to rotate at least one of the at least two wheels in a second direction opposite of the first direction until the vehicle security system no longer detects the rotation of the one or more of the at least two wheels in the first direction.

22. The vehicle of claim 21 wherein the vehicle security system is configured to detect rotation of one or more of the at least two wheels in a first direction by being configured to:

detect rotation or phase change of the motor caused by the rotation of the one or more of the at least two wheels.

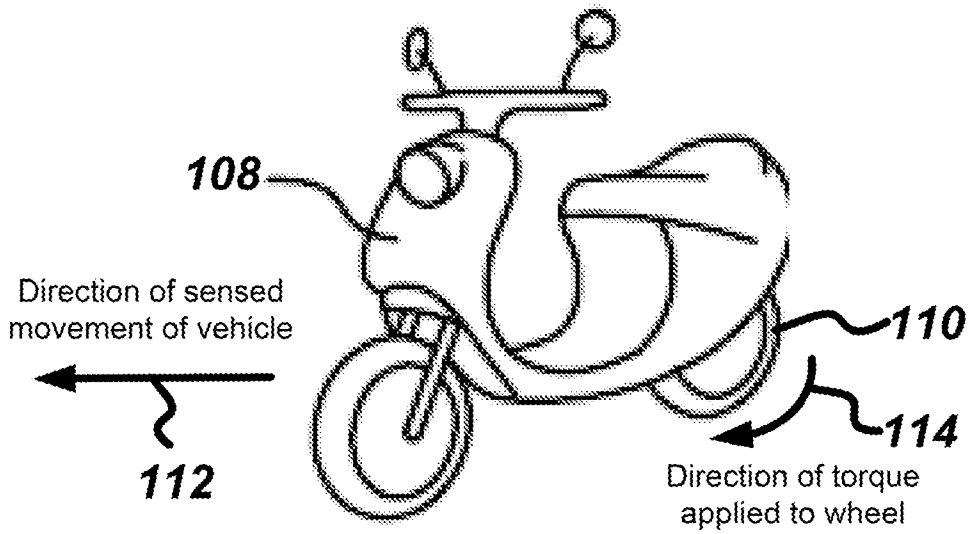
108
Direction of sensed movement of vehicle
112
110
114
Direction of torque applied to wheel

FIG. 1A

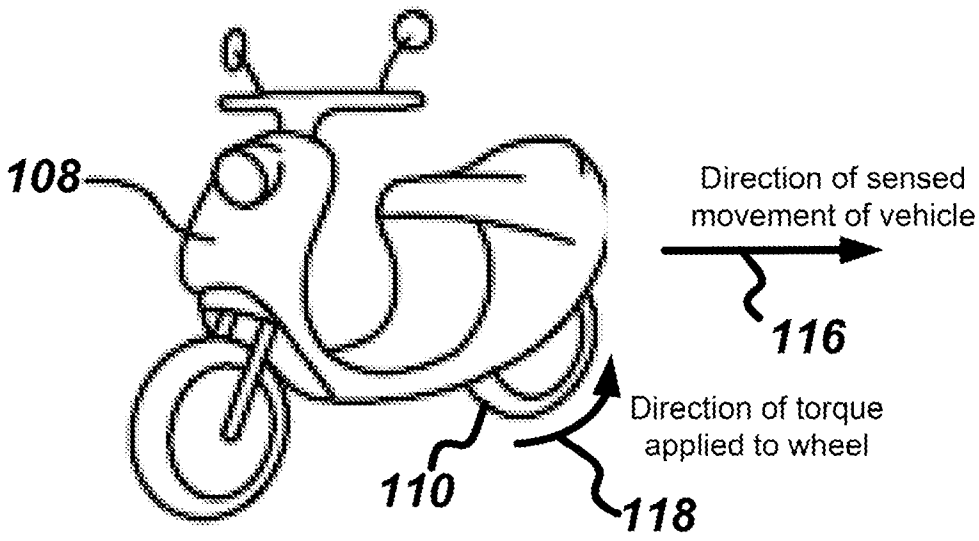
108
Direction of sensed movement of vehicle
116
Direction of torque applied to wheel
110
118

FIG. 1B

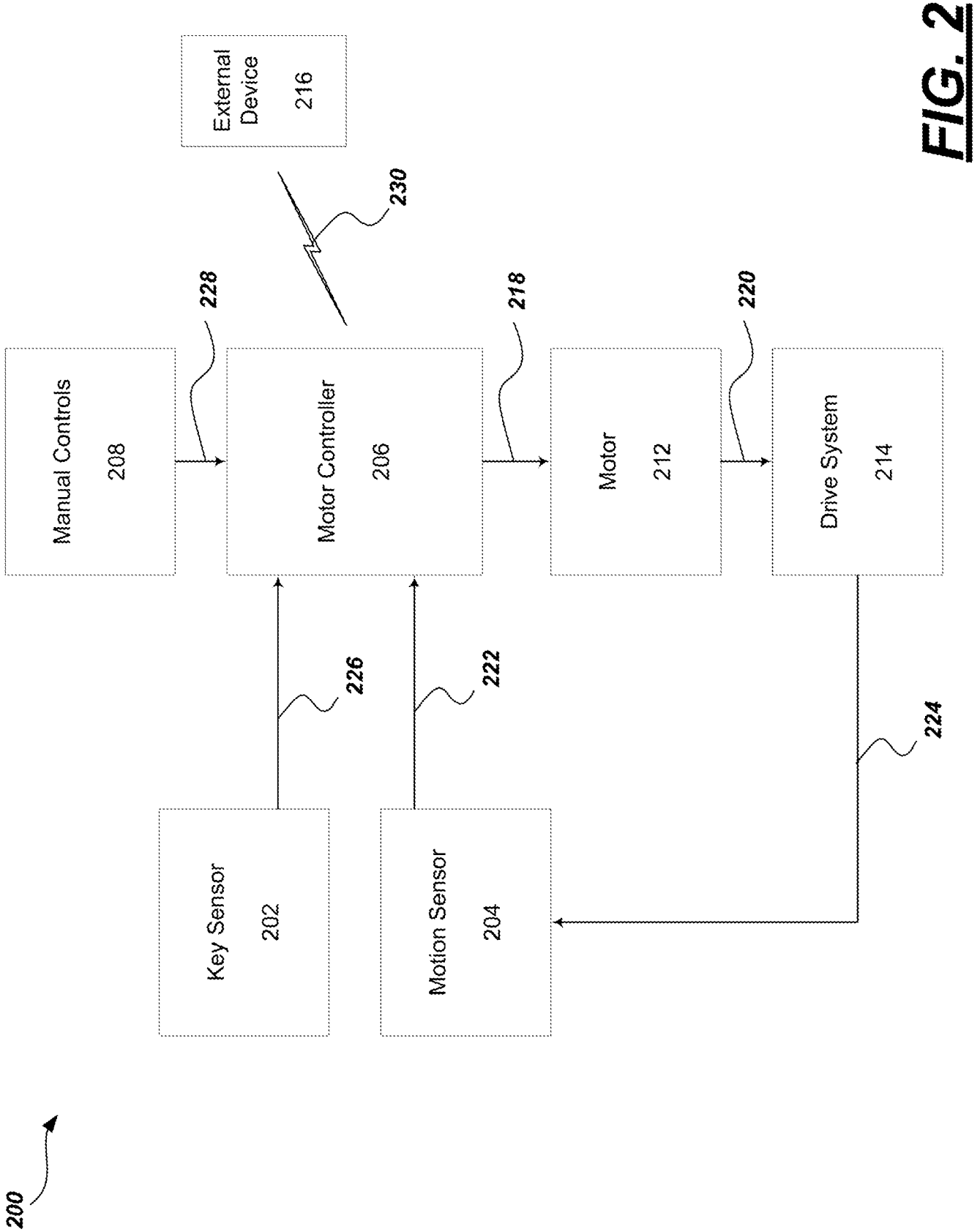
200
Key Sensor
202
Motion Sensor
204
Manual Controls
208
Motor Controller
206
Motor
212
Drive System
214
External Device
216
226
222
228
218
220
230
224

FIG. 2

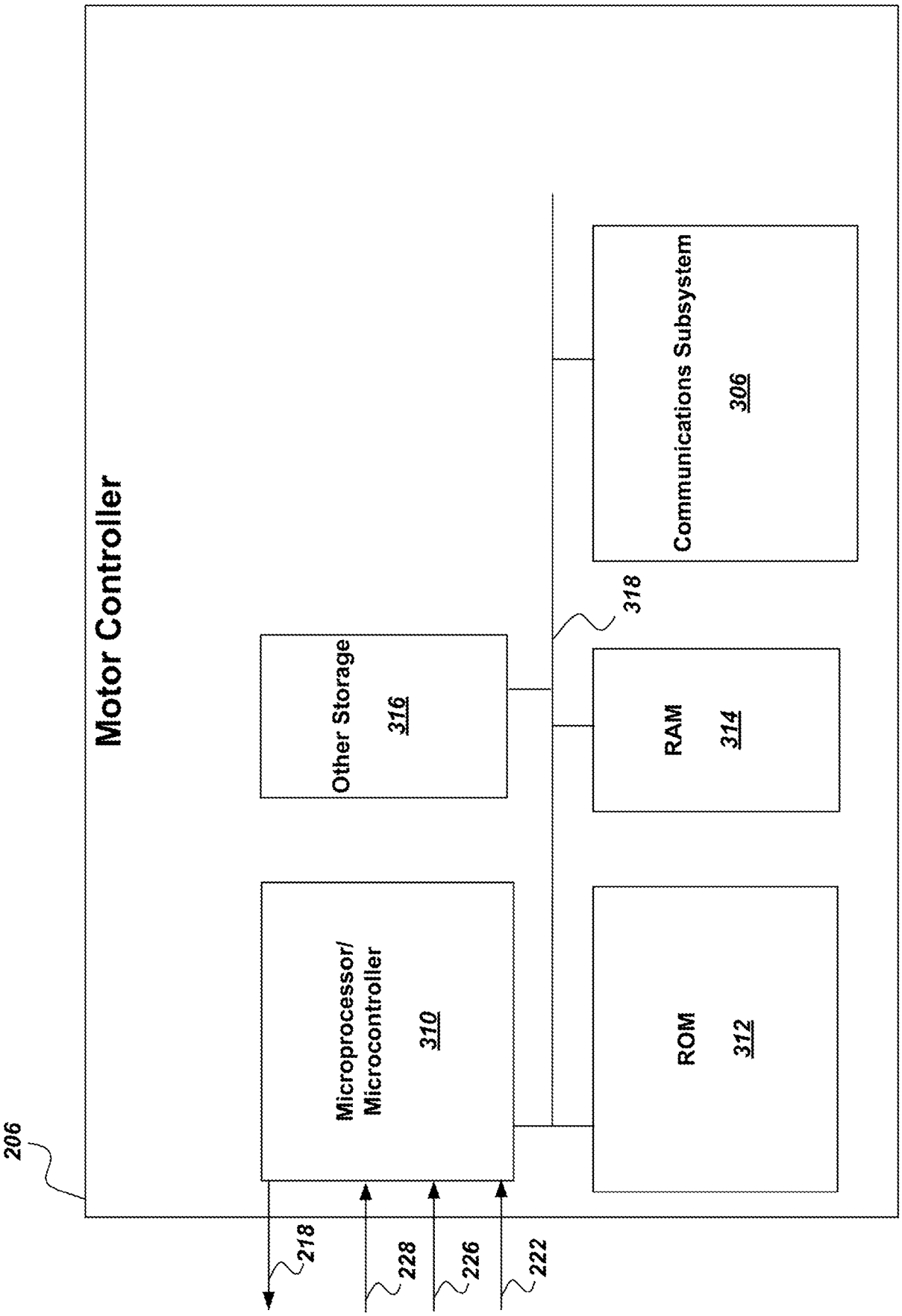
Motor Controller
206
Microprocessor/
Microcontroller
310
ROM
312
RAM
314
Other Storage
316
Communications Subsystem
306
318
218
228
226
222

FIG. 3

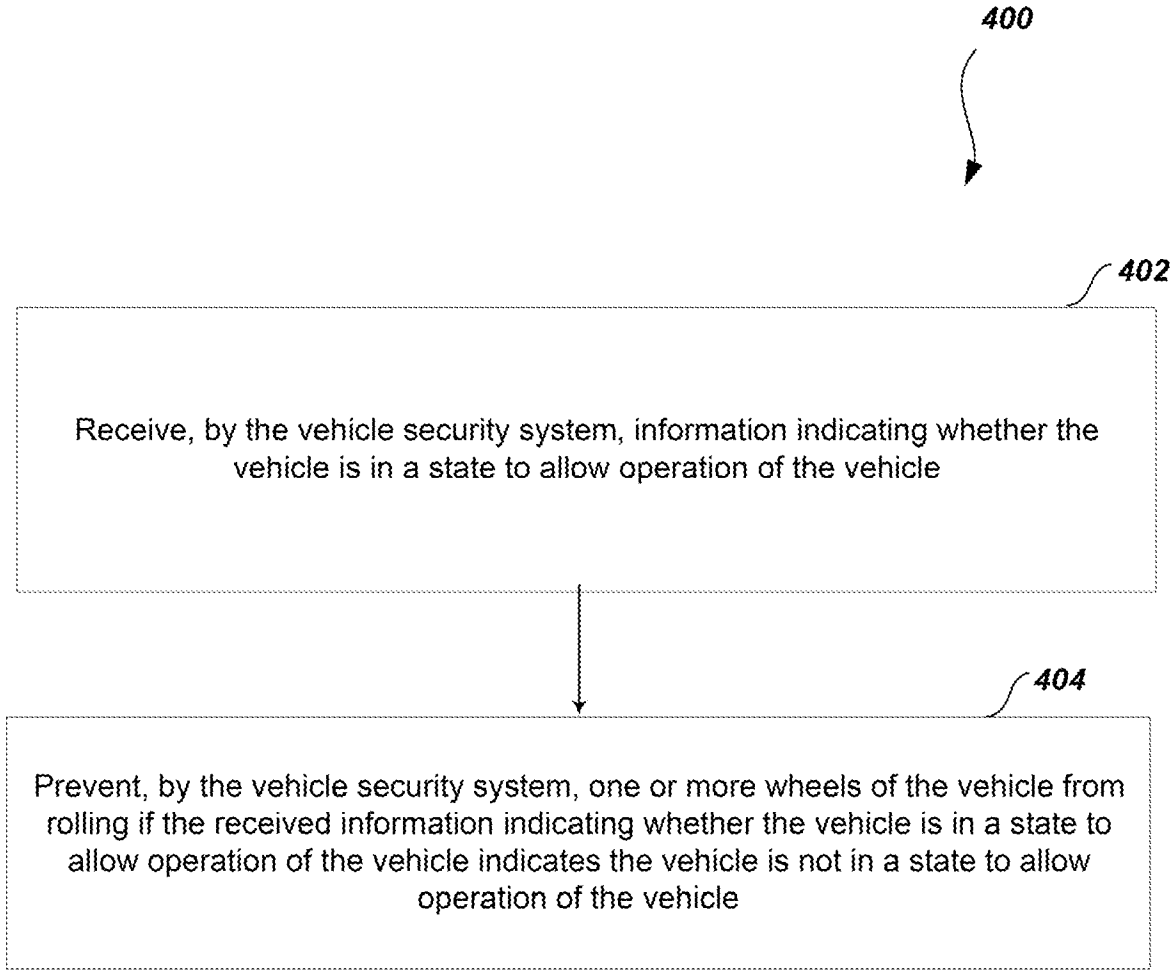
400
402
Receive, by the vehicle security system, information indicating whether the vehicle is in a state to allow operation of the vehicle
404
Prevent, by the vehicle security system, one or more wheels of the vehicle from rolling if the received information indicating whether the vehicle is in a state to allow operation of the vehicle indicates the vehicle is not in a state to allow operation of the vehicle

FIG. 4

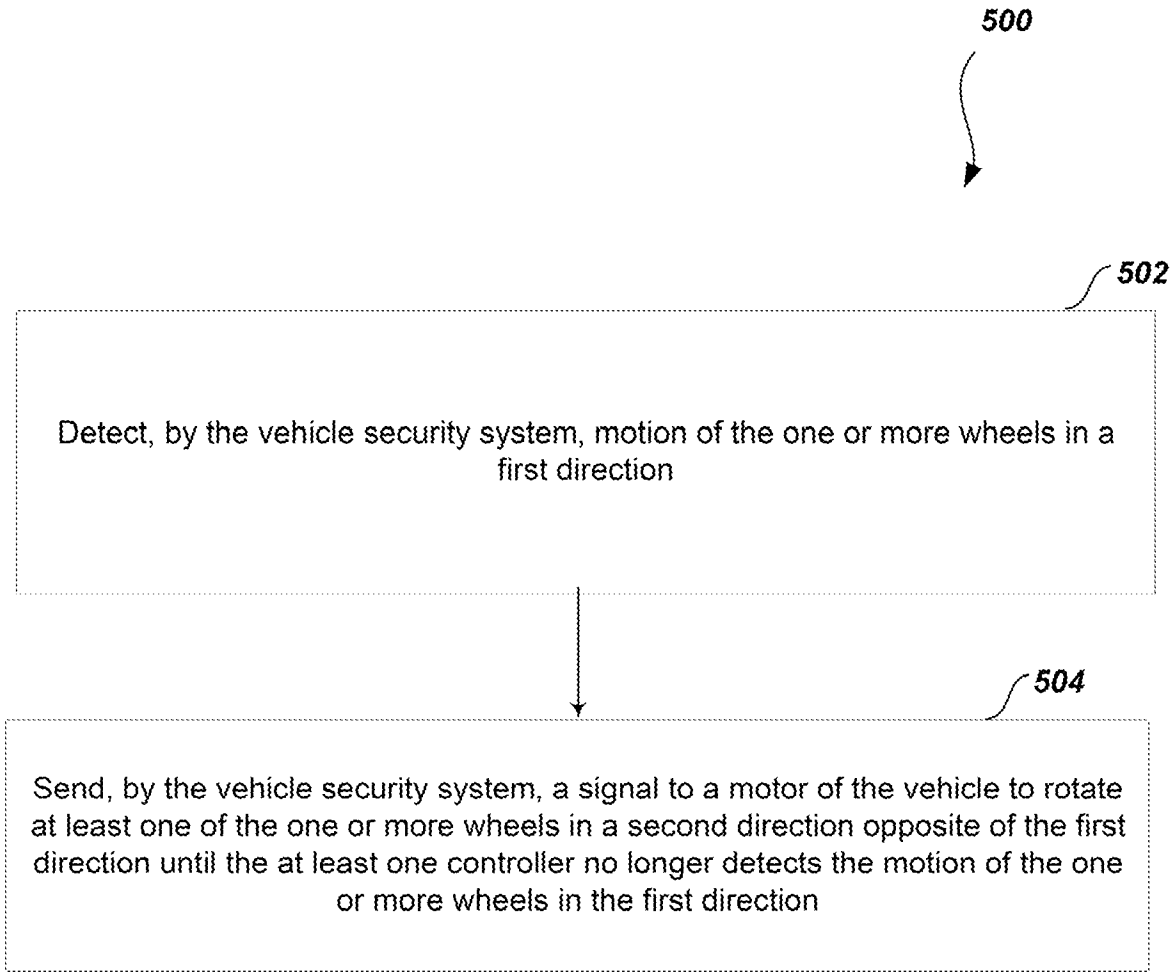
500
502
Detect, by the vehicle security system, motion of the one or more wheels in a first direction
504
Send, by the vehicle security system, a signal to a motor of the vehicle to rotate at least one of the one or more wheels in a second direction opposite of the first direction until the at least one controller no longer detects the motion of the one or more wheels in the first direction

FIG. 5

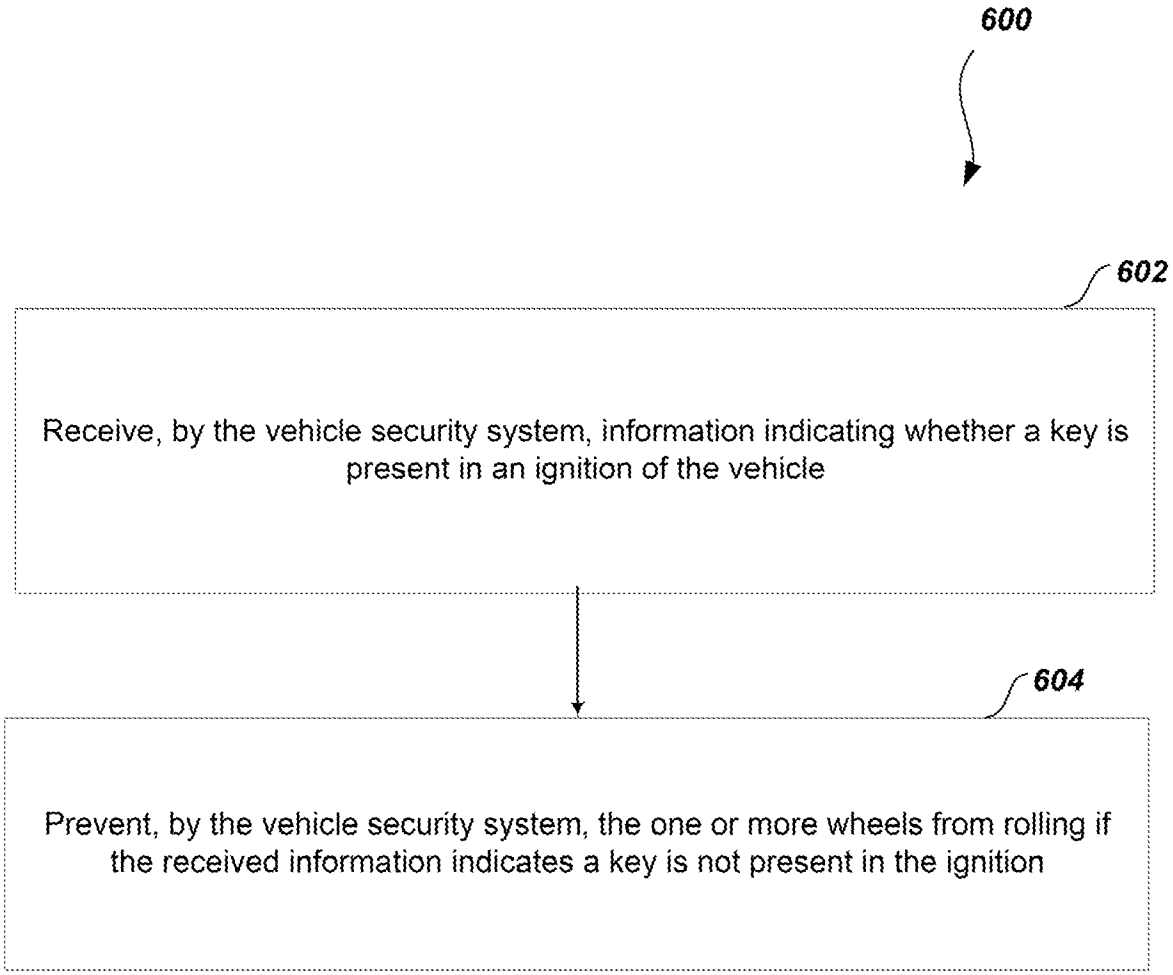
600
602
Receive, by the vehicle security system, information indicating whether a key is present in an ignition of the vehicle
604
Prevent, by the vehicle security system, the one or more wheels from rolling if the received information indicates a key is not present in the ignition

FIG. 6

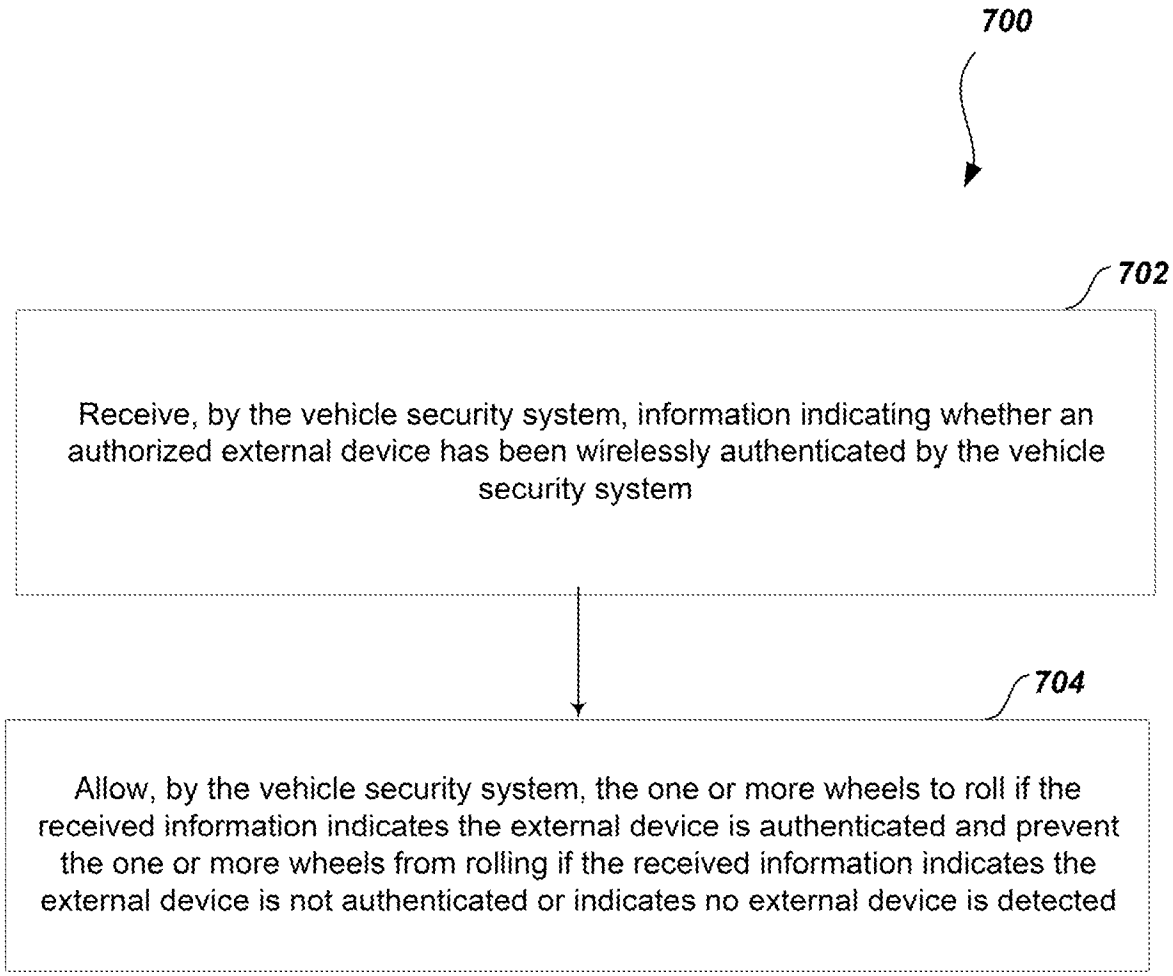
700
702
Receive, by the vehicle security system, information indicating whether an authorized external device has been wirelessly authenticated by the vehicle security system
704
Allow, by the vehicle security system, the one or more wheels to roll if the received information indicates the external device is authenticated and prevent the one or more wheels from rolling if the received information indicates the external device is not authenticated or indicates no external device is detected

FIG. 7

INTERNATIONAL SEARCH REPORT

International application No.
PCT/US2012/063979

A. CLASSIFICATION OF SUBJECT MATTER

B62H 5/00(2006.01)i, B60L 11/18(2006.01)i, G08B 13/00(2006.01)i, B60R 25/10(2006.01)i

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)

B62H 5/00; B60R 25/10; B60Q 1/00

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Korean utility models and applications for utility models

Japanese utility models and applications for utility models

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)

eKOMPASS(KIPO internal) & Keywords: vehicle, security, motor, motion, sensor, controller, communication

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X Y A	KR 10-0971278 B1 (DONG-A UNIV. RESEARCH FOUNDATION FOR INDUSTRY-ACADEMY COOPERATION) 20 July 2010 See paragraph 32 - paragraph 74 and figures 1 - 4.	1-2,7-10,12-13,16-18,20 5-6 3-4,11,14-15,19,21-22
Y A	US 7,567,166 B2 (LAURENT BOURGINE DE MEDER) 28 July 2009 See column 3, line 15 - column 10, line 21 and figures 1 - 3.	5-6 1-4,7-22
A	JP 2005-067453 A (HONDA MOTOR CO., LTD.) 17 March 2005 See paragraph 1 - paragraph 42 and figures 1 - 8.	1-22
A	US 6,515,580 B1 (NAOYA ISODA et al.) 04 February 2003 See column 3, line 61 - column 5, line 15 and figures 1 - 6.	1-22

☐ 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

"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 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	Date of mailing of the international search report
26 FEBRUARY 2013 (26.02.2013)	**04 MARCH 2013 (04.03.2013)**
Name and mailing address of the ISA/KR Korean Intellectual Property Office 189 Cheongsa-ro, Seo-gu, Daejeon Metropolitan City, 302-701, Republic of Korea Facsimile No. 82-42-472-7140	Authorized officer KIM, Jong Yun Telephone No. 82-42-481-5467

Form PCT/ISA/210 (second sheet) (July 2009)

INTERNATIONAL SEARCH REPORT

Information on patent family members

International application No.

PCT/US2012/063979

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
KR 10-0971278 B1	20.07.2010	CN 102009714 A	13.04.2011
		JP 2011-057202 A	24.03.2011
		US 2011/0060481 A1	10.03.2011
US 7,567,166 B2	28.07.2009	AU 2003-273429 A1	09.02.2004
		EP 1523434 A1	20.04.2005
		FR 2842493 A1	23.01.2004
		FR 2842493 B1	09.09.2005
		US 2006/0164217 A1	27.07.2006
		WO 2004/009415 A1	29.01.2004
JP 2005-067453 A	17.03.2005	None	
US 6,515,580 B1	04.02.2003	CN 1334210 A0	06.02.2002
		EP 1177955 A2	06.02.2002
		EP 1177955 A3	19.05.2004
		JP 2002-037028 A	06.02.2002
		TW 500673 A	01.09.2002