

DESCRIPTION

TITLE OF INVENTION: FRAUD PREVENTION DEVICE AND FRAUD
PREVENTION UNIT

5 CROSS REFERENCE TO RELATED APPLICATION

[0001]

This application is based on Japanese Patent Application No. 2016-210856 filed on October 27, 2016, the disclosure of which is incorporated herein by reference.

10

TECHNICAL FIELD

[0002]

The present disclosure relates to a fraud prevention device for preventing an unauthorized change of a device used in a vehicle, and a fraud
15 prevention unit including the fraud prevention device. In particular, the present disclosure relates to prevention of the unauthorized change of a product installed at a position easily visible to the user such as an ETC (Electronic Toll Collection, registered trademark) device, a vehicle navigation device, or the like.

20 BACKGROUND ART

[0003]

Conventionally, a technique that prevents an unauthorized change of a device used in a vehicle by using Near Field Communication (Near Field Communication: NFC) has been known. For example, Patent Literature 1
25 discloses a tamper detection system that detects whether an authenticated radiator is attached by reading out ID information by an ECU (Electronic Control Unit) transmitted from an RFID (Radio Frequency Identifier) attached to the radiator. Patent Literature 1 discloses a tamper detection system that detects an act deceiving the ECU by attaching the RFID in an unjust manner. The
30 tamper detection system detects the act deceiving the ECU using the RFID together with a noncontact temperature sensor and a contact temperature sensor. In this configuration, the tamper detection system compares temperature information acquired from the noncontact temperature sensor and

the contact temperature sensor with the correlation between the radiator surface temperature and the engine water temperature which is stored in advance. With this configuration, the tamper detection system determines whether the contact temperature sensor is properly attached to the radiator.

5

PRIOR ART LITERATURE

PATENT LITERATURE

[0004]

Patent Literature 1: JP 2007-22467 A

10

SUMMARY OF INVENTION

[0005]

In a tamper detection system of Patent Literature 1, ID information transmitted from RFID may be intercepted and the legitimate ID information may be forged. In this case, even when the authorized temperature is not forged, the tamper detection system can detect the fraud. The correlation between the radiator surface temperature and the engine water temperature is difficult to set because the characteristics differ depending on the vehicle and the characteristics differ due to the aged deterioration of the device.

20

[0006]

In the tamper detection system of Patent Literature 1, it is difficult to commonize the design. For example, a tamper detection system developed for a specific vehicle may be applied to another vehicle. In this case, it is necessary to re-examine the relationship between the radiator surface temperature and the engine water temperature for the vehicle, and to adjust the parameters in consideration of the influence of environmental disturbance, aging deterioration and variation. Thus, many design change steps are needed.

25

[0007]

In view of the foregoing difficulties, it is an object of the present disclosure to provide a fraud prevention device and a fraud prevention unit, each of which can easily and reliably prevent an unauthorized change of a device used in a vehicle using near field communication.

30

[0008]

According to an aspect of the present disclosure, a fraud prevention device for a vehicle includes a near field communication portion, a fraud determination portion, and a travel determination portion. The near field communication portion performs a near field communication with a wireless tag.

5 The wireless tag is used in the vehicle and transmits an identification code. The fraud determination portion determines whether there is an unauthorized change of a target device by verifying the identification code received by the near field communication portion from the wireless tag. The target device is constituted by a device to which the wireless tag or a device including the fraud
10 prevention device. The travel determination portion determines whether the vehicle is traveling. The near field communication portion causes the wireless tag to transmit the identification code by requesting the wireless tag to transmit the identification code. The near field communication portion does not cause the wireless tag to transmit the identification code until the travel determination
15 portion determines that the vehicle is traveling.

[0009]

With the fraud prevention device, the target device is fixed to the wireless tag or includes the fraud prevention device. Thus, the fraud determination portion can determine whether the presence or absence of the
20 unauthorized change of the target device by verifying the identification code received by the fraud prevention device from the wireless tag using near field communication. In order to counterfeit the identification code, it is considered that the identification code transmitted from the wireless tag is intercepted. It is difficult to intercept the identification code unless the vehicle is at a stop. On
25 the other hand, with the present disclosure, the identification code is not transmitted from the wireless tag until the travel determination portion determines that the vehicle is traveling. Thus, the configuration can make it difficult to counterfeit the identification code. As a result, the configuration can easily and reliably prevent the unauthorized change of the device used in the
30 vehicle using near field communication.

[0010]

According to another aspect of the present disclosure, a fraud prevention unit includes the fraud prevention device and the wireless tag. The

wireless tag is used in the same vehicle as the fraud prevention device. The wireless tag transmits the identification code. The fraud prevention unit includes the fraud prevention device so that the can easily and reliably prevent the unauthorized change of the device used in the vehicle using near field
5 communication.

BRIEF DESCRIPTION OF DRAWINGS

[0011]

The above and other objects, features and advantages of the present
10 disclosure will become more apparent from the following detailed description made with reference to the accompanying drawings. In the drawings:

FIG. 1 is a diagram showing an example of a schematic configuration of a vehicle system;

FIG. 2 is a diagram showing an example of a schematic configuration of
15 a vehicle unit;

FIG. 3 is a diagram showing an example of a schematic configuration of a fraud prevention processing portion;

FIG. 4 is a flowchart showing an example of a flow of fraud determination related processing performed by a fraud prevention device;

FIG. 5 is a diagram showing an example of a configuration of a
20 modification;

FIG. 6 is a diagram showing an example of a schematic configuration of a vehicle system; and

FIG. 7 is a diagram showing an example of a schematic configuration of
25 a vehicle unit.

DETAILED DESCRIPTION

[0012]

A plurality of embodiments and a plurality of modifications for disclosure
30 will be described with reference to the drawings. For convenience of explanation, parts having functions identical to functions of parts shown in figures previously referred to for description among the plurality of embodiments and the plurality of modifications are given identical reference numbers.

Description of these parts is omitted in some cases. Description of other embodiments or other modifications may be referred to for parts given identical reference numbers.

[0013]

5 (First Embodiment)

(Schematic Configuration of Vehicle System 3)

The first embodiment of the present disclosure is described with reference to the drawings. As shown in FIG. 1, a vehicle system 3 includes a vehicle unit 1 used in a vehicle A and a center 2. The vehicle unit 1 includes an
10 NFC (Near Field Communication) tag 10 and an in-vehicle device 20. Details of the vehicle unit 1 will be described later. In the present embodiment, a car is exemplified as the vehicle A. Alternatively, a vehicle such as a motorcycle other than the car may be applied.

[0014]

15 The center 2 includes a server device such as a company, a store, a public institution or the like. The center 2 provides a predetermined service for a user using the in-vehicle device 20 by communicating with the in-vehicle device 20 via a public communication network and a base station. For example, the predetermined service may include a service that automatically performs
20 settlement of the road pricing or the parking fee based on information such as the position of the vehicle A obtained from the in-vehicle device 20. The center 2 may include multiple server devices.

[0015]

(Schematic Configuration of Vehicle Unit 1)

25 The vehicle unit 1 will be described. The vehicle unit 1 includes the NFC tag 10 and the in-vehicle device 20 as described above. The NFC tag 10 corresponds to a wireless tag, and the in-vehicle device 20 corresponds to a target device.

[0016]

30 The NFC tag 10 is constituted by a wireless tag fixed to the vehicle A and performs Near Field Communication (NFC) with the in-vehicle device 20 existing within a communication range. Near field communication is performed according to the NFC standard, and the communication distance is limited to

about 10 cm. Near field communication can also be paraphrased as near field type wireless communication.

[0017]

The NFC tag 10 may include an active wireless tag or a passive wireless tag. In the present embodiment, the passive wireless tag is employed which converts a radio wave from the in-vehicle device 20 into electric power. As an example, the NFC tag 10 is attached to a glass such as a windshield of the vehicle A, a body part, or the like in a state difficult to remove. The state difficult to remove represents a state where it is difficult to remove without breakage, a state where it is difficult to remove itself, or the like. The NFC tag 10 stores a unique password in the nonvolatile memory. When receiving a password matching this unique password, the NFC tag 10 transmits an identification code by near field communication. The password corresponds to authentication information.

15 [0018]

The in-vehicle device 20 is attached in the vicinity of the NFC tag 10 as shown in FIG. 1 so that a near field communication device 25, which will be described, included in the in-vehicle device 20 can perform near field communication with the NFC tag 10. For example, the in-vehicle device 20 may be detachably attached to a support such as a bracket fixed to the vehicle A. The schematic configuration of the in-vehicle device 20 will be described below.

[0019]

(Schematic Configuration of In-vehicle Device 20)

Here, a schematic configuration of the in-vehicle device 20 is described with reference to FIG. 2. As shown in FIG. 2, the in-vehicle device 20 includes a control device 22, a gyro sensor 23, an acceleration sensor 24, the near field communication device 25, a center communication device 26, a positioning device 27, and a display device 28.

[0020]

30 The gyro sensor 23 detects an angular velocity occurring in the in-vehicle device 20. For example, the gyro sensor 23 detects the rotational angular velocity around the vertical axis of the vehicle A in a state where the in-vehicle device 20 is attached to the vehicle A in a predetermined attitude.

[0021]

The acceleration sensor 24 is constituted by a triaxial acceleration sensor that detects acceleration acting in three orthogonal axes directions. For the sake of convenience, the three axial directions for detecting the acceleration
5 are referred to as the X axis, the Y axis, and the Z axis direction. The acceleration sensor 24 corresponds to an inertial sensor. The acceleration sensor 24 is included in a housing of the in-vehicle device 20.

[0022]

The near field communication device 25 performs near field
10 communication according to the NFC standard. The near field communication device 25 transmits the unique password to the NFC tag 10 through near field communication. When the NFC tag 10 transmits the identification code through near field communication, the near field communication device 25 receives the identification code. The near field communication device 25 functions as a
15 reader of the NFC tag 10. The near field communication device 25 corresponds to a near field communication portion. The center communication device 26 communicates with the center 2 via the public communication network and the base station.

[0023]

20 The positioning device 27 sequentially measures a position of the vehicle A including the positioning device 27 (hereinafter referred to as a vehicle position) based on a received position signal transmitted by positioning satellites constituting GNSS (Global Navigation Satellite System). The positioning device 27 may measure the vehicle position using the measurement results of
25 the gyro sensor 23 and the acceleration sensor 24. The display device 28 is constituted by a display such as a liquid crystal display, for example, and displays text.

[0024]

The control device 22 includes a processor, a volatile memory, a
30 nonvolatile memory, an I/O, and a bus that connects those devices. The control device 22 performs various processes by executing a control program stored in the nonvolatile memory. The control device 22 includes a fraud prevention processing portion 200 that performs a process related to prevention of an

unauthorized change of the in-vehicle device 20. The fraud prevention processing portion 200, the acceleration sensor 24, and the near field communication device 25 function as the fraud prevention device 21. The configuration that includes the fraud prevention device 21 and the NFC tag 10
 5 corresponds to a fraud prevention unit.

[0025]

(Schematic Configuration of Fraud Prevention Processing Portion 200)

A schematic configuration of the fraud prevention processing portion 200 is described with reference to FIG. 3. As shown in FIG. 3, the fraud prevention
 10 processing portion 200 includes a registration portion 201, a vehicle position acquisition portion 202, a travel determination portion 203, a transmission control portion 204, a code acquisition portion 205, a fraud determination portion 206, a notification portion 207, and a deactivation instruction unit 208.

[0026]

15 The registration portion 201 is constituted by a nonvolatile memory and stores the unique password (hereinafter simply referred to as the password) of the NFC tag 10, an authorized identification code of the NFC tag 10, a vehicle registration number of the vehicle A, or the like. The vehicle registration number corresponds to identification information. The vehicle position
 20 acquisition portion 202 sequentially acquires the vehicle position measured by the positioning device 27.

[0027]

The travel determination portion 203 determines whether the vehicle A is traveling by monitoring the value of the acceleration detected by the acceleration
 25 sensor 24. The travel determination portion 203 may determine that the vehicle A is traveling when the acceleration sensor 24 detects the acceleration equal to or greater than a predetermined value. The predetermined value represents a value of acceleration that occurs while the vehicle A is traveling but does not occur during the stop of the vehicle A.

30 [0028]

The travel determination portion 203 may determine that the vehicle A is traveling when the acceleration sensor 24 detects acceleration (that is, motion) over a predetermined period of time in a constant direction. This configuration

is to prevent erroneous determination that the vehicle A is traveling due to acceleration caused by a person shaking the vehicle A. For example, the motion in the constant direction may be determined when the continuous state in which the deviation amount of the direction of the combined vector of accelerations in the three axial directions detected by the acceleration sensor 24 is within the threshold range continues. The predetermined period may be defined as a period of time in which a temporary motion in a constant direction caused by a shake of a person and a continuous motion in a constant direction caused by a continuous travel in a constant direction of the vehicle A can be distinguished.

[0029]

When the travel determination portion 203 determines that the vehicle A is traveling, the transmission control portion 204 reads out the password from the registration portion 201 and causes the near field communication device 25 to transmit the password. When the travel determination portion 203 does not determine that the vehicle A is traveling, the transmission control portion 204 does not cause the near field communication device 25 to transmit the password until the travel determination portion 203 determines that the vehicle A is traveling.

[0030]

The NFC tag 10 receives the password, when the near field communication device 25 transmits the password. When the received password matches the password stored in the nonvolatile memory, the NFC tag 10 transmits the identification code. The transmission of the password from the transmission control portion 204 corresponds to a request of the transmission of the identification code. When the NFC tag 10 transmits the identification code, the code acquisition portion 205 receives the identification code via the near field communication device 25.

[0031]

The fraud determination portion 206 verifies whether the identification code acquired by the code acquisition portion 205 matches the authorized identification code stored in the registration portion 201. When the identification codes match (that is, when code verification is established), the

fraud determination portion 206 determines that there is no unauthorized change of the in-vehicle device 20. When the identification codes do not match, the fraud determination portion 206 determines that there is the unauthorized change of the in-vehicle device 20.

5 [0032]

When the fraud determination portion 206 determines that there is the unauthorized change of the in-vehicle device 20, the notification portion 207 reads out the vehicle registration number of the vehicle A from the registration portion 201 and causes the center communication device 26 to transmit the
10 vehicle registration number to the center 2. Since the in-vehicle device 20 transmits the vehicle registration number, the center 2 specifies the vehicle A including the in-vehicle device 20 in which the unauthorized change has occurred. The notification portion 207 may transmit the vehicle position of the vehicle A acquired by the vehicle position acquisition portion 202 in case that the
15 notification portion 207 causes the center communication device 26 to transmit the vehicle registration number to the center 2. Since the in-vehicle device 20 transmits the vehicle position of the vehicle A, the center 2 specifies the position of the vehicle A having the in-vehicle device 20 in which the unauthorized change has occurred. With this configuration, the public agency may set up
20 crackdown on the vehicle A in which the unauthorized change has occurred based on the information of the vehicle A specified by the center 2 and the information of the position of the vehicle A.

[0033]

When the fraud determination portion 206 determines that there is the
25 unauthorized change of the in-vehicle device 20, the notification portion 207 may cause the display device 28 to display an indication that the unauthorized change of the in-vehicle device 20 has occurred. The notification portion 207 may display on the meter or the like of the vehicle A an indication that the unauthorized change of the in-vehicle device 20 has occurred.

30 [0034]

When the fraud determination portion 206 determines that there is the unauthorized change of the in-vehicle device 20, the deactivation instruction portion 208 deactivates the function of the in-vehicle device 20. For example,

the deactivation instruction portion 208 may deactivate the function, from the functions of the in-vehicle device 20, related to the service used by the user received by the in-vehicle device 20. Alternatively, the deactivation instruction portion 208 may deactivate the entire function of the in-vehicle device 20. It is more preferable that the deactivation of the function of the in-vehicle device 20 caused by the deactivation instruction portion 208 is not canceled by restarting after turning off the power. For example, the in-vehicle device 20 of which the deactivation instruction portion 208 has deactivated the function may cancel the deactivation of the function by a special operation at a service factory or the like certified by a public agency or vehicle manufacturer.

[0035]

(Fraud Determination Related Processing in Fraud Prevention Device 21)

With reference to a flowchart in FIG. 4, an example of a flow of a processing related to determination of the unauthorized change of the in-vehicle device 20 in the fraud prevention device 21 (hereinafter referred to as fraud determination related processing) will be described. The flowchart of FIG. 4 may start when a power supply of the in-vehicle device 20 is turned on. The power supply of the in-vehicle device 20 may be turned on when the ignition power of the vehicle A is turned on. In this case, the flowchart of FIG. 4 starts when the ignition power of the vehicle A is turned on.

[0036]

In S1, the travel determination portion 203 monitors the value of the acceleration detected by the acceleration sensor 24 and determines whether the vehicle A is traveling. When the travel determination portion 203 determines that the vehicle A is traveling (YES in S1), the flowchart proceeds to S2. When the travel determination portion 203 does not determine that the vehicle A is traveling (NO in S1), the flowchart proceeds to S7.

[0037]

In S2, the transmission control portion 204 causes the near field communication device 25 to transmit the password. The NFC tag 10 receives the password transmitted from the near field communication device 25. When the received password matches the password stored in the NFC tag 10, the NFC

tag 10 transmits the identification code.

[0038]

In S3, when the code acquisition portion 205 acquires the identification code transmitted from the NFC tag 10 via the near field communication device 25 (YES in S3), the flowchart proceeds to S4. When the code acquisition portion 205 does not acquire the identification code (NO in S3), the flowchart proceeds to S7. As an example, after the near field communication device 25 transmits the password, the code acquisition portion 205 may not acquire the identification code within a predetermined time period. In this case, the code acquisition portion 205 determines that the identification code is not received.

[0039]

In S4, the fraud determination portion 206 verifies whether the identification code acquired by the code acquisition portion 205 matches the authorized identification code stored in the registration portion 201. In S5, when the code verification in S4 is established (YES in S5), the flowchart proceeds to S6. When the code verification in S4 is not established (NO in S5), the flowchart proceeds to S8.

[0040]

In S6, the fraud determination portion 206 determines that there is no unauthorized change of the in-vehicle device 20. In S7, when an end time point of the fraud determination related processing arrives (YES in S7), the fraud determination related processing is terminated. When an end time point of the fraud determination related processing does not arrive (NO in S7), the process returns to S1 to repeat the process from the beginning. An example of the time point for terminating the fraud determination related processing includes a state that the power source of the in-vehicle device 20 is turned off.

[0041]

When the code verification in S4 is not established, in S8, the fraud determination portion 206 determines that there is the unauthorized change of the in-vehicle device 20. In S9, the notification portion 207 causes the center communication device 26 to transmit the vehicle registration number of the vehicle A read out from the registration portion 201 and the vehicle position of the vehicle A acquired by the vehicle position acquisition portion 202 to the

center 2. In S10, the deactivation instruction portion 208 deactivates the function of the in-vehicle device 20 and terminates the fraud determination related processing.

[0042]

5 (Summary of First Embodiment)

According to the configuration of the first embodiment, the fraud prevention device 21 is included in the in-vehicle device 20. The fraud prevention device 21 verifies whether the identification code received by the fraud prevention device 21 from the NFC tag 10 using near field communication matches the authorized identification code stored in the fraud prevention device 21. Based on the fact that the unauthorized change of the in-vehicle device 20 has occurred and the verification is not established, the presence or absence of the unauthorized change of the in-vehicle device 20 can be determined.

[0043]

15 A method and a countermeasure for deceiving the fraud prevention device 21 and performing the unauthorized change will be described. In order to perform the unauthorized change of the in-vehicle device 20, it is necessary to counterfeit the NFC tag 10. In order to read out the memory of the NFC tag 10 with the password as in the present embodiment, the near field communication device 25 transmits a set of a Read command and the password to the NFC tag 10. In this configuration, a so-called replay attack can be considered for counterfeiting the NFC tag 10 with the password. First, a device for intercepting wireless communication is installed in the vicinity of the NFC tag 10, and intercepts the communication content between the NFC tag 10 and the near field communication device 25. Next, the intercepted communication content is written to another wireless tag or an electronic circuit that functions in the same manner as the NFC tag 10 so as to replay the intercepted communication content. The counterfeited wireless tag or electronic circuit is attached to the in-vehicle device 20.

30 [0044]

In response to such an unauthorized change attempt, according to the configuration of the first embodiment, when the password transmitted from the fraud prevention device 21 to the NFC tag 10 using the near field communication

device 25 mismatches the password stored in the NFC tag 10, the NFC tag 10 does not transmit the identification code. With this configuration, it is difficult to read out the authorized identification code from the NFC tag 10 illegally.

[0045]

5 Further, according to the configuration of the first embodiment, until the travel determination portion 203 determines that the vehicle A is traveling, the NFC tag 10 does not transmit the identification code. The NFC tag 10 and the near field communication device 25 can communicate with each other only while the vehicle is traveling. While the vehicle is traveling, it is difficult to attach the
10 device for interception to the vehicle because a legitimate user (that is, a driver) is in the vehicle compartment. The device for interception may be attached to the vehicle while the vehicle is parking and there is no legitimate user. In this situation, the legitimate user can easily notice that the device for interception is attached when the legitimate user returns. With this configuration, the
15 unauthorized change can be prevented by a means such as removing the device for interception by the legitimate user. Further, since the NFC tag 10 and the near field communication device 25 do not communicate with each other while the vehicle is stopping, interception cannot be performed.

[0046]

20 As described above, according to the configuration of the first embodiment, until the travel determination portion 203 determines that the vehicle A is traveling, the NFC tag 10 does not transmit the identification code. Thus, the configuration can make it difficult to counterfeit the authorized identification code. As a result, the configuration can easily and reliably prevent
25 the unauthorized change of the in-vehicle device 20 using near field communication.

[0047]

Furthermore, according to the configuration of the first embodiment, the travel determination portion 203 determines whether the vehicle A is traveling
30 based on the detection result of the acceleration sensor 24 included in the in-vehicle device 20. Thus, the configuration can make it more difficult to pretend that the vehicle A is traveling. The details are described as follows. For example, assume that the travel determination portion 203 determines that

the vehicle A is traveling while the ignition (hereinafter, IG) power source of the vehicle A is in on state. In this case, the state that the vehicle A is traveling can be pretended by disconnecting the fraud prevention device 21 and the IG power source and then connecting to another power source. Assume that the travel
5 determination portion 203 determines that the vehicle A is traveling based on an output of an accelerator sensor of the vehicle A or the like. In this case, the state that the vehicle A is traveling can be pretended by inputting a pseudo signal from the outside of the fraud prevention device 21.

[0048]

10 With the configuration of the first embodiment, the travel determination portion 203 determines whether the vehicle A is traveling based on the detection result of the acceleration sensor 24 included in the in-vehicle device 20. Thus, the configuration can prevent performing the disguise, and make it more difficult to pretend that the vehicle A is traveling. As an example of erroneous
15 determination that the fraud prevention device 21 is in the traveling state, it is considered that acceleration is applied by the shake of the vehicle. In this embodiment, the configuration does not determine that the vehicle is traveling unless the acceleration is in a constant direction so as to make it difficult to disguise.

20 [0049]

(First Modification)

In the first embodiment, the in-vehicle device 20 is constituted by one housing, but the configuration is not limited to this specific example. For example, the in-vehicle device 20 may be constituted by a plurality of housings
25 (hereinafter, referred to as a first modification). An example of the configuration of the first modification will be described with reference to FIG. 5. In FIG. 5, the in-vehicle device 20 may be detachably attached to a support such as a bracket fixed to the front glass (see B in FIG. 5).

[0050]

30 As shown in FIG. 5, the housing of the in-vehicle device 20 may be divided into a holder case 20a and a main case 20b and connected by an arm 20c. As an example, the holder case 20a may include the gyro sensor 23, the acceleration sensor 24, the near field communication device 25, the center

communication device 26, the positioning device 27, and a control device that functions as the fraud prevention processing portion 200. The main case 20b may include the display device 28 and a control device that controls the display device 28. For example, the arm 20c may be constituted by a tubular flexible member. A flexible cable that connects an electronic component of the holder case 20a with an electronic component of the main case 20b passes through the inside of the arm 20c. The user may bend the flexible arm 20c to change the angle of the main case 20b with respect to the holder case 20a.

[0051]

10 (Second Embodiment)

In the first embodiment, the configuration in which the fraud determination related processing is performed on a device to be a target for determining the presence or absence of the unauthorized change (hereinafter, target device) has been described, however the present disclosure is not necessarily limited to this specific example. For example, a configuration in which the fraud determination related processing is performed on a device other than the target device may be adopted (hereinafter, a second embodiment).

[0052]

(Schematic Configuration of Vehicle System 3a)

20 The second embodiment of the present disclosure will be described with reference to the drawings. As shown in FIG. 6, a vehicle system 3a includes a vehicle unit 1a used in the vehicle A and the center 2. The vehicle unit 1a includes an NFC tag 10a, a fraud prevention device 21a, a center communication device 26a, a positioning device 27a, a display device 28a, and an in-vehicle device 30. Details of the vehicle unit 1a will be described later. The center 2 is similar to the center 2 of the first embodiment except that the center 2 provides a predetermined service for a user using the in-vehicle device 30 by communicating with the in-vehicle device 30. The predetermined service may include, as described below, a service that automatically performs settlement of the road pricing and the parking fee.

[0053]

(Schematic Configuration of Vehicle Unit 1a)

The vehicle unit 1a will be described with reference to FIG. 7. As

described below, the vehicle unit 1a includes the NFC tag 10a, the fraud prevention device 21a, the center communication device 26a, the positioning device 27a, the display device 28a, and the in-vehicle device 30. The NFC tag 10a corresponds to the wireless tag, and the in-vehicle device 30 corresponds to the target device.

[0054]

The NFC tag 10a is similar to the NFC tag 10 except that the NFC tag 10a is fixed to the in-vehicle device 30 and performs near field communication with the fraud prevention device 21a existing in the communication range. The NFC tag 10a is attached to the in-vehicle device 30 in a state difficult to remove. The state difficult to remove represents a state in which it is difficult to remove without breakage, a state where it is difficult to remove itself, or the like. The fraud prevention device 21a functions similarly to the fraud prevention device 21 of the first embodiment. The fraud prevention device 21a may be fixed to the vehicle A. Alternatively, the fraud prevention device 21a may be detachably attached to the vehicle A. Details of the fraud prevention device 21a will be described below.

[0055]

The center communication device 26a is similar to the center communication device 26 of the first embodiment except that the center communication device 26a is connected to the fraud prevention device 21a without being included in the target device. The positioning device 27a is similar to the positioning device 27 of the first embodiment except that the positioning device 27a is connected to the fraud prevention device 21a without being included in the target device. The display device 28a is constituted by a display such as a liquid crystal display, for example, provided on a meter of the vehicle A or the like and displays text.

[0056]

For example, the in-vehicle device 30 may be detachably attached to a support such as a bracket fixed to the vehicle A. Further, as described above, the NFC tag 10a is fixed to the in-vehicle device 30 in the state difficult to remove.

[0057]

(Schematic Configuration of Fraud Prevention Device 21a)

A schematic configuration of the fraud prevention device 21a is described with reference to FIG. 7. As shown in FIG. 7, the fraud prevention device 21a includes a control device 22a, a gyro sensor 23a, an acceleration
5 sensor 24a, and the near field communication device 25a.

[0058]

The gyro sensor 23a detects an angular velocity occurring in the fraud prevention device 21a. For example, the gyro sensor 23a detects the rotational angular velocity around the vertical axis of the vehicle A in a state where the
10 fraud prevention device 21a is attached to the vehicle A in a predetermined attitude. Alternatively, the fraud prevention device 21a may not include the gyro sensor 23a. The acceleration sensor 24a is similar to the acceleration sensor 24 of the first embodiment except that the acceleration sensor 24a is included in the housing of the fraud prevention device 21a. The acceleration sensor 24a
15 corresponds to the inertial sensor. The near field communication device 25a is similar to the near field communication device 25 of the first embodiment except that the near field communication device 25a is not included in the target device but included in the fraud prevention device 21a. The near field communication device 25a corresponds to the near field communication portion.

20 [0059]

The control device 22a includes a processor, a volatile memory, a nonvolatile memory, an I/O, and a bus that connects those devices. The control device 22a performs various processes by executing a control program stored in the nonvolatile memory. The control device 22a includes the fraud prevention
25 processing unit 200 similarly to the first embodiment. The control device 22a performs a process related to prevention of an unauthorized change of the in-vehicle device 30 similarly to the fraud determination related processing of the first embodiment using near field communication between the NFC 10a and the near field communication device 25a.

30 [0060]

In the fraud prevention device 21a, the fraud determination portion 206 verifies whether the identification code of the NFC 10a acquired by the code acquisition portion 205 matches the authorized identification code stored in the

registration portion 201. When these codes do not match with one another, the fraud determination portion 206 determines that there is the unauthorized change of the in-vehicle device 30. When the fraud determination portion 206 determines that there is the unauthorized change of the in-vehicle device 30, the deactivation instruction portion 208 transmits an instruction to deactivate the function of the in-vehicle device 30 to the in-vehicle device 30 via a communication module communicating wirelessly or by wire and causes the in-vehicle device 30 to deactivate the function in a similar manner to the first embodiment.

[0061]

In the configuration of the second embodiment, until the travel determination portion 203 determines that the vehicle A is traveling, the NFC tag 10a does not transmit the identification code. Thus, the configuration can easily and reliably prevent the unauthorized change of the in-vehicle device 30 using near field communication.

[0062]

(Second Modification)

In the above-described embodiments, the acceleration sensor 24, 24a is constituted by the three axial acceleration sensor. However, the present disclosure is not limited to this specific example. For example, when the in-vehicle device 20 and the fraud prevention device 21a is employed in the vehicle A so as that the detection axis of the acceleration sensor 24, 24a matches the front-rear direction of the vehicle A, the acceleration sensor 24, 24a may be constituted by a two axial acceleration sensor or a single axis acceleration sensor.

[0063]

(Third Modification)

In the above-described embodiments, the travel determination portion 203 determines whether the vehicle A is traveling based on the detection result of the acceleration sensor 24 of the in-vehicle device 20 or the acceleration sensor 24a of the fraud prevention device 21a. However, the present disclosure is not limited to this specific example. The travel determination portion 203 may determine whether the vehicle A is traveling based on the

detection result of the gyro sensor 23 of the in-vehicle device 20 or the gyro sensor 23a of the fraud prevention device 21a (hereinafter referred to as a third modification). The configuration of the third modification may be employed. In this case, the travel determination portion 203 determines that the vehicle A is traveling when the gyro sensor 23, 23a may detect the acceleration equal to or greater than a predetermined value. In order to prevent erroneous determination that the vehicle A is traveling due to acceleration caused by the shake of the vehicle A, the travel determination portion 203 determines that the vehicle A is traveling when the gyro sensor 23, 23a detects the turn (that is, motion) over a predetermined period of time in a constant direction. The gyro sensor 23, 23a corresponds to the inertial sensor. When the third modification is employed in the second embodiment, the fraud prevention device 21a may not include the acceleration sensor 24a.

[0064]

(Fourth Modification)

The travel determination portion 203 may determine whether the vehicle A is traveling based on the turn on and off of the IG power supply of the vehicle A. Alternatively, the travel determination portion 203 may determine whether the vehicle A is traveling based on a signal obtained from the signal line of the vehicle A. The signal obtained from the signal line of the vehicle A may include a signal of an accelerator sensor, a signal of a vehicle speed sensor, or the like.

[0065]

(Fifth Modification)

In the above-described embodiments, when the password transmitted from the fraud prevention device 21, 21a to the NFC tag 10, 10a does not match the password stored in the NFC tag 10, 10a, the NFC tag 10, 10a does not transmit the identification code. However, the present disclosure is not limited to this specific example. For example, when receiving the transmission request of the identification code from the fraud prevention device 21, 21a, the NFC tag 10, 10a may transmit the identification code. In this case, in the fraud prevention device 21, 21a, the near field communication device 25, 25a may transmit the transmission request of the identification code instead of the password.

[0066]

(Sixth Modification)

In the above-described embodiments, when the fraud determination portion 206 determines that there is the unauthorized change of the in-vehicle device 20, 30, the fraud prevention device 21, 21a notifies the center 2 and deactivates the function of the in-vehicle device 20, 30. However, the present disclosure is not limited to this specific example. For example, the fraud prevention device 21, 21a may notify the center 2 but may not deactivate the function of the in-vehicle device 20, 30. Alternatively, the fraud prevention device 21, 21a may not notify the center 2 but deactivate the function of the in-vehicle device 20, 30.

[0067]

(Seventh Modification)

The in-vehicle device 20, 30 may include a communication module that performs wireless communication with a roadside device providing a predetermined service (that is, road-to-vehicle communication). The in-vehicle device 20, 30 may provide a service to the user via the road-to-vehicle communication with the roadside device. In this case, the service may include automatic settlement for drive-through, automatic settlement of parking fee in a toll parking lot, support of traveling in an intersection, provision of congestion information, or the like. For example, as road-to-vehicle communication between the in-vehicle device 20, 30 and the roadside device, wireless communication conforming to the standard of WAVE (Wireless Access in Vehicular Environment) may be used.

25 [0068]

While the present disclosure has been described with reference to embodiments thereof, it is to be understood that the disclosure is not limited to the embodiments and constructions. The present disclosure covers various modification examples and equivalent arrangements. In addition, while the various elements are shown in various combinations and configurations, which are exemplary, other combinations and configurations, including more, less or only a single element, are also within the spirit and scope of the present disclosure.

CLAIMS

1. A fraud prevention device for a vehicle comprising:

a near field communication portion configured to perform a near field communication with a wireless tag, the wireless tag being used in the vehicle and transmitting an identification code;

a fraud determination portion configured to determine whether there is an unauthorized change of a target device by verifying the identification code received by the near field communication portion from the wireless tag, the target device being constituted by a device to which the wireless tag is fixed or a device including the fraud prevention device; and

a travel determination portion configured to determine whether the vehicle is traveling, wherein

the near field communication portion causes the wireless tag to transmit the identification code by requesting the wireless tag to transmit the identification code, and does not cause the wireless tag to transmit the identification code until the travel determination portion determines that the vehicle is traveling.

2. The fraud prevention device according to claim 1, further comprising an inertial sensor, wherein

the travel determination portion determines whether the vehicle is traveling based on a detection result of the inertial sensor.

3. The fraud prevention device according to claim 2, wherein:

the inertial sensor is constituted by an acceleration sensor; and

the travel determination portion determines that the vehicle is traveling when the acceleration sensor detects a motion over a predetermined period of time in a constant direction.

4. The fraud prevention device according to any one of claims 1 to 3, further comprising:

a deactivation instruction portion configured to deactivate a function of the target device when the fraud determination portion determines

that there is the unauthorized change of the target device.

5. A fraud prevention unit comprising:
the fraud prevention device according to any one of claims 1 to 4; and
the wireless tag used in the vehicle as the fraud prevention device, and
configured to transmit the identification code.

6. The fraud prevention unit according to claim 5, wherein
the target device is used in the vehicle, and constituted by the device to
which the wireless tag is fixed.

7. The fraud prevention unit according to claim 5, wherein:
the wireless tag is fixed to the vehicle; and
the target device is used in the vehicle, and constituted by the device
including the fraud prevention device .

8. The fraud prevention unit according to any one of claims 5 to 7,
wherein:

the near field communication portion of the fraud prevention device
transmits authentication information used for an authentication in the wireless
tag when the near field communication portion requests the wireless tag to
transmit the identification code; and

the wireless tag transmits the identification code when the wireless tag
succeeds in the authentication by the authentication information transmitted
from the near field communication portion.

9. The fraud prevention unit according to any one of claims 5 to 8,
further comprising

a center communication device configured to communicate with a center,
wherein

the center communication device transmits identification information for
identifying the vehicle to the center when the fraud determination portion of the

fraud prevention device determines that there is the unauthorized change of the target device.

10. The fraud prevention unit according to claim 9, further comprising a positioning device configured to measure a position of the vehicle, wherein

the center communication device transmits the position of the vehicle measured by the positioning device together with the identification information to the center when the fraud determination portion of the fraud prevention device determines that there is the unauthorized change of the target device.