

DESCRIPTION

TITLE OF INVENTION: FRAUD DETECTION DEVICE, FRAUD DETECTION
SYSTEM, FRAUD DETECTION METHOD, AND PROGRAM

5 TECHNICAL FIELD

[0001]

The present disclosure relates to a fraud detection device, a fraud detection
system, a fraud detection method, and a program.

BACKGROUND ART

10 [0002]

Recently, a global navigation satellite system (GNSS) measuring a position of a
vehicle or the like on the basis of signals received from satellites has been widely used.

The GNSS is used, for example, in a charging process for a vehicle traveling on an
expressway. In the charging process using the GNSS, when a signal received from a

15 satellite is impersonated, the charging process cannot be correctly performed. As
impersonation countermeasures, for example, a technique of allowing onboard devices
(onboard units) mounted in two vehicles which are traveling to perform vehicle-to-
vehicle communication with each other and detecting impersonation of a signal on the
basis of the result of vehicle-to-vehicle communication is disclosed in Patent Document

20 1.

Citation List

Patent Document

[0003]

Patent Document 1: Japanese Patent No. 6942414

25 SUMMARY OF INVENTION

Technical Problem

[0004]

In a portable information terminal such as a smartphone, acquiring position information using the GNSS is generally performed. Accordingly, use of a portable information terminal for a charging system causes no great problem in hardware. However, even when a portable information terminal is used, there is also need for countermeasures against impersonation. On the other hand, in the technique described in Patent Document 1, since impersonation is detected through vehicle-to-vehicle communication, there is a problem in that it cannot cope with a case in which a portable information terminal is used.

[0005]

The present disclosure was invented to solve the aforementioned problem, and an objective thereof is to provide a fraud detection device, a fraud detection system, a fraud detection method, and a program that can detect impersonation when a portable information terminal is used.

Solution to Problem

[0006]

In order to achieve the aforementioned objective, a fraud detection device according to the present disclosure includes a first recording unit configured to receive and record first probe information including a plurality of time-series sets of first position information which is position information of a vehicle and first time information indicating a time at which the first position information is acquired and first identification information which is identification information of the vehicle from a portable information terminal placed in the vehicle, a second recording unit configured to receive and record second probe information including a plurality of time-series sets of second

position information which is position information of the vehicle and second time information indicating a time at which the second position information is acquired and second identification information which is identification information of the vehicle from an onboard device installed in the vehicle, a comparison unit configured to compare the first probe information and the second probe information in which the first identification information and the second identification information match, and a determination unit configured to determine whether there is a suspicion of impersonation in the first probe information on the basis of a comparison result from the comparison unit.

[0007]

- 10 A fraud detection system according to the present disclosure includes a fraud detection device including a first recording unit configured to receive and record first probe information including a plurality of time-series sets of first position information which is position information of a vehicle and first time information indicating a time at which the first position information is acquired and first identification information which
- 15 is identification information of the vehicle from a portable information terminal placed in the vehicle, a second recording unit configured to receive and record second probe information including a plurality of time-series sets of second position information which is position information of the vehicle and second time information indicating a time at which the second position information is acquired and second identification information
- 20 which is identification information of the vehicle from an onboard device installed in the vehicle, a comparison unit configured to compare the first probe information and the second probe information in which the first identification information and the second identification information match, and a determination unit configured to determine whether there is a suspicion of impersonation in the first probe information on the basis
- 25 of a comparison result from the comparison unit, and the onboard device.

[0008]

A fraud detection method according to the present disclosure includes a step of receiving and recording first probe information including a plurality of time-series sets of first position information which is position information of a vehicle and first time information indicating a time at which the first position information is acquired and first identification information which is identification information of the vehicle from a portable information terminal placed in the vehicle, a step of receiving and recording second probe information including a plurality of time-series sets of second position information which is position information of the vehicle and second time information indicating a time at which the second position information is acquired and second identification information which is identification information of the vehicle from an onboard device installed in the vehicle, a step of comparing the first probe information and the second probe information in which the first identification information and the second identification information match; and a step of determining whether there is a suspicion of impersonation in the first probe information on the basis of a comparison result.

[0009]

A program according to the present disclosure causes a computer to perform a step of receiving and recording first probe information including a plurality of time-series sets of first position information which is position information of a vehicle and first time information indicating a time at which the first position information is acquired and first identification information which is identification information of the vehicle from a portable information terminal placed in the vehicle, a step of receiving and recording second probe information including a plurality of time-series sets of second position information which is position information of the vehicle and second time information

indicating a time at which the second position information is acquired and second identification information which is the identification information of the vehicle from an onboard device installed in the vehicle, a step of comparing the first probe information and the second probe information in which the first identification information and the second identification information match, and a step of determining whether there is a suspicion of impersonation in the first probe information on the basis of a comparison result.

Advantageous Effects of Invention

[0010]

10 With the fraud detection device, the fraud detection system, the fraud detection method, and the program according to the present disclosure, it is possible to detect impersonation when a portable information terminal is used.

BRIEF DESCRIPTION OF DRAWINGS

[0011]

15 [FIG. 1] A diagram illustrating an entire configuration of a fraud detection system according to an embodiment of the present disclosure.

 [FIG. 2] A diagram illustrating an example of portable information terminal information according to the embodiment of the present disclosure.

20 [FIG. 3] A diagram illustrating an example of onboard device information according to the embodiment of the present disclosure.

 [FIG. 4] A diagram illustrating an example of roadside antenna information according to the embodiment of the present disclosure.

25 [FIG. 5] A diagram illustrating the entire configuration of the fraud detection system and a functional configuration of a fraud detection device according to the embodiment of the present disclosure.

[FIG. 6] A first flowchart illustrating an example of a process flow that is performed by the fraud detection device according to the embodiment of the present disclosure.

[FIG. 7] A second flowchart illustrating an example of the process flow that is performed by the fraud detection device according to the embodiment of the present disclosure.

[FIG. 8] A third flowchart illustrating an example of the process flow that is performed by the fraud detection device according to the embodiment of the present disclosure.

[FIG. 9] A fourth flowchart illustrating an example of the process flow that is performed by the fraud detection device according to the embodiment of the present disclosure.

DESCRIPTION OF EMBODIMENTS

[0012]

Hereinafter, a fraud detection system 1 and a fraud detection device 20 according to an embodiment of the present disclosure will be described with reference to the accompanying drawings.

FIG. 1 is a diagram illustrating an entire configuration of a fraud detection system according to an embodiment of the present disclosure.

As illustrated in FIG. 1, the fraud detection system 1 includes an onboard device 10 for an electronic toll collection system that is mounted in a vehicle V, a portable information terminal 30 such as a smartphone that is placed in the vehicle V, a roadside antenna device 11 that is provided on a roadside of a road R on which the vehicle V is traveling, and a fraud detection device 20 that is independent from the vehicle V and the roadside antenna device 11. The onboard device 10 is an example of an “onboard

device” in the present disclosure. In FIG. 1, one vehicle V and one roadside antenna device 11 are illustrated, but the number of vehicles V and the number of roadside antenna devices 11 may be two or more.

[0013]

5 The fraud detection system 1 and the fraud detection device 20 determine whether there is a suspicion of impersonation (disguise) in position information or time information included in portable information terminal information D1 received from the portable information terminal 30 by comparing the portable information terminal information D1 with onboard device information D2 or roadside antenna information D3.

10 The fraud detection system 1 and the fraud detection device 20 are used for a charging system of a toll road, a charging area, or the like and are also installed in a regular road for daily enforcement. In the present embodiment, it is assumed that the fraud detection system 1 and the fraud detection device 20 are used for a charging system 50 of a toll road, a charging area, or the like. The roadside antenna device 11 according to the

15 present embodiment is installed, for example, at an entrance or an exit of a toll road or a charging area or junctions with a plurality of roads.

[0014]

 The portable information terminal 30 is, for example, a smartphone having a positioning function using a GNSS as described above. The portable information

20 terminal 30 is a terminal carried by a user who has been registered in advance in a charging system 50 by executing application software (hereinafter simply referred to as an application) for the charging system 50. In this case, an account ID (identification information) is assigned to the registered user. In the present disclosure, the state in which the portable information terminal 30 is placed in the vehicle V is a state in which

25 the portable information terminal 30 moves with movement of the vehicle V in a state in

which it is placed in the vehicle V. The portable information terminal 30 repeatedly acquires position information at intervals of a predetermined time period using the positioning function using the GNSS and periodically transmits a plurality of pieces of position information corresponding to the predetermined time period as portable

5 information terminal information D1 including time information indicating times at which the pieces of position information are acquired to the fraud detection device 20 via a base station B of a mobile communication network, a wide area network 41, or the like. Transmission of the portable information terminal information D1 to the fraud detection device 20 may be a transmission aspect including a communication means such as local
10 5G, Wi-Fi (registered trademark), Bluetooth (registered trademark) in addition to a base station B of a mobile communication network and the wide area network 41. FIG. 2 is a diagram illustrating an example of the portable information terminal information D1 according to the embodiment of the present disclosure.

[0015]

15 The portable information terminal information D1 illustrated in FIG. 2 includes an account ID (D11), an onboard device ID (D12), and a plurality of pieces of time-series information D10. Each piece of information D10 includes position information D13, a data creation time D14, and acceleration data D15. The account ID (D11) is an ID which is registered in the charging system 50. The onboard device ID (D12) is
20 identification information of the onboard device 10. When an onboard device ID is recorded in association with an account at the time of registration in the charging system 50, the portable information terminal information D1 may not include one of the account ID (D11) and the onboard device ID (D12). The onboard device ID (D12) may be manually input to an application by a user or may be automatically acquired by the
25 application through short-range wireless communication or wired communication

between the portable information terminal 30 and the onboard device 10. The position information D13 is position information of the vehicle V (exactly the portable information terminal 30) calculated on the basis of GNSS information D4 acquired using the GNSS by the portable information terminal 30 and includes information indicating
5 latitude, longitude, or the like. The GNSS information D4 is a positioning GNSS signal transmitted from a satellite S and includes time data and orbit data of the satellite S. The data creation time D14 is a time at which the position information D13 has been created (or a time at which the position information D13 has been acquired). The acceleration data D15 is data indicating acceleration which is calculated on the basis of a
10 plurality of pieces of position information D13 in a time series.

[0016]

In the present embodiment, the portable information terminal information D1 is an example of “first probe information” in the present disclosure. In the present embodiment, “probe information” is information including a time series of position
15 information acquired at predetermined intervals using the positioning function using the GNSS by the portable information terminal 30, the onboard device 10, or the like. Alternatively, in the present embodiment, “probe information” is information including position information which is created on the basis of the information received from the onboard device 10 or the like by the roadside antenna device 11. The onboard device
20 ID (D12) is an example of “first identification information” which is the identification information of the vehicle V. When the onboard device ID (D12) is omitted, the account ID (D11) is an example of “first identification information” which is the identification information of the vehicle V. The portable information terminal information D1 may include identification information displayed on a number plate of
25 the vehicle V instead of the onboard device ID (D12) or in addition to the onboard device

ID (D12). In this case, the identification information displayed on the number plate is also an example of “first identification information.” The position information D13 is an example of “first position information,” the data creation time D14 is an example of “first time information,” the acceleration data D15 is an example of “first acceleration
 5 information,” and the plurality of pieces of information D10 is an example of “a plurality of time-series sets.” The acceleration data D15 may not be included in the portable information terminal information D1.

[0017]

The onboard device 10 has a function of acquiring position information of the
 10 vehicle V (exactly an antenna for receiving the GNSS information D4 in the onboard device 10) using the GNSS and acquires the position information, for example, repeatedly at predetermined intervals. The onboard device 10 acquires the position information at intervals of a predetermined time period using the positioning function using the GNSS, thins the position information to create a time series of sets of position
 15 information and time information, for example, for each predetermined distance, and transmits the time-series sets of information as the onboard device information D2 to the roadside antenna device 11. FIG. 3 is a diagram illustrating an example of the onboard device information D2 according to the embodiment of the present disclosure.

[0018]

20 The onboard device information D2 illustrated in FIG. 3 includes an onboard device ID (D22) and a plurality of pieces of time-series information D20. Each piece of information D20 includes position information D23, a data creation time D24, and acceleration data D25. The onboard device ID (D22) is identification information of the onboard device 10 and is information which is preset for each onboard device 10. The
 25 position information D23 is position information which is calculated on the basis of the

acquired GNSS information D4 using the GNSS by the onboard device 10 and includes information indicating latitude, longitude, or the like. The data creation time D24 is a time at which the position information D23 has been created (or a time at which the position information D23 has been acquired). The acceleration data D25 is data
5 indicating acceleration which is calculated on the basis of the plurality of pieces of position information D23 in a time series. The acceleration data D25 may not be included in the onboard device information D2.

[0019]

In the present embodiment, the onboard device information D2 is an example of
10 “second probe information” in the present disclosure. The onboard device ID (D22) is an example of “second identification information” which is the identification information of the vehicle V. The onboard device information D2 may include identification information included in the number plate of the vehicle V in addition to the onboard device ID (D22). In this case, the identification information included in the number
15 plate is also an example of “second identification information.” The onboard device ID (D12) included in the portable information terminal information D1 and the onboard device ID (D22) included in the onboard device information D2 are the same. In this case, the “first identification information” and the “second identification information” are the same. Here, when the portable information terminal information D1 includes the
20 identification information displayed on the number plate as the identification information of the vehicle V instead of the onboard device ID (D12) as described above, the “first identification information” and the “second identification information” in the present disclosure are different from each other. In this case, the fraud detection device 20 may correlate the “first identification information” and the “second identification information”
25 using information for correlating the “first identification information” and the “second

identification information.” The position information D23 is an example of “second position information,” the data creation time D24 is an example of “second time information,” the acceleration data D25 is an example of “second acceleration information,” and the plurality of pieces of information D20 is an example of “a plurality of time-series sets.”

[0020]

The roadside antenna device 11 transmits and receives predetermined information with respect to the onboard device 10 using dedicated short range communications (DSRC) technology. The roadside antenna device 11 receives the onboard device information D2 from the onboard device 10. The roadside antenna device 11 transmits the onboard device information D2 received from the onboard device 10 to the fraud detection device 20 via a wide area network 42. The roadside antenna device 11 creates the roadside antenna information D3 on the basis of the onboard device information D2 received from the onboard device 10 and transmits the created roadside antenna information D3 to the fraud detection device 20 via the wide area network 42. When the charging system 50 is used instead of using the portable information terminal 30, the roadside antenna device 11 transmits and receives predetermined information used for charging with respect to the onboard device 10 and transmits and receives predetermined information based on the transmitted and received information with respect to the charging system 50.

[0021]

FIG. 4 is a diagram illustrating an example of the roadside antenna information D3 according to the embodiment of the present disclosure. The roadside antenna information D3 illustrated in FIG. 4 includes identification ID (D31), installation place position information D32, onboard device ID (D33), communication result D34 and data

creation time D35. The identification ID (D31) is identification information of the roadside antenna device 11. The installation place position information D32 is position information of an installation place of the roadside antenna device 11. The onboard device ID (D22) is identification information of the onboard device 10 which is a transmission source of the onboard device information D2. The communication result D34 is information indicating whether communication with the onboard device 10 is normal or abnormal. The data creation time D35 is a time at which the roadside antenna information D3 has been created (or a time at which the onboard device information D2 has been received).

10 [0022]

In the present embodiment, the roadside antenna information D3 is an example of “third probe information” in the present disclosure. The identification ID (D31) is an example of “identification information of a roadside antenna device.” The onboard device ID (D33) is an example of “second identification information” which is the identification information of the vehicle V. The installation place position information D32 is an example of “position information of the roadside antenna device.” The roadside antenna information D3 may not include any one of the identification ID (D31) and the installation place position information D32. In this case, the fraud detection device 20 may correlate the “identification information of the roadside antenna device” and the “position information of the roadside antenna device” using information for correlating the “identification information of the roadside antenna device” and the “position information of the roadside antenna device.”

[0023]

The fraud detection device 20 is a so-called a center server (computer). The fraud detection device 20 compares the portable information terminal information D1

received from the portable information terminal 30 placed in the vehicle V with the onboard device information D2 received from the onboard device 10 installed in the vehicle V via the roadside antenna device 11 and determines whether there is a suspicion of impersonation in the portable information terminal information D1. Alternatively, the fraud detection device 20 compares the received portable information terminal information D1 with the roadside antenna information D3 received from the roadside antenna device 11 and determines whether there is a suspicion of impersonation in the portable information terminal information D1.

Here, the onboard device information D2 and the portable information terminal information D1 are different in easiness in information falsification. Specifically, the onboard device 10 is mounted on or set up in a vehicle by a qualified operator, and a user has difficulty intervening in processes until necessary processes such as charging are completed on data of the received position information or the like. The onboard device 10 is designed as a device for only the purpose of reception and utilization of traffic information such as the position information, and position information optimal for reception and utilization of traffic information is acquired. On the other hand, the portable information terminal 30 (a smartphone) is designed as a device to which various applications can be arbitrarily added by a user and which can be used for the purpose other than reception of utilization of traffic information. Accordingly, since the portable information terminal 30 can cope with flexible payment methods in comparison with the onboard device 10 and can more easily introduce a malicious application (for example, a position information impersonation application) or the like thereinto, it is difficult to secure accuracy of the acquired position information.

[0024]

(Functional configuration of fraud detection device)

The functional configuration of the fraud detection device 20 will be described with reference to FIG. 5.

FIG. 5 is a diagram illustrating the entire configuration of the fraud detection system 1 and the functional configuration of the fraud detection device 20 according to
5 the embodiment of the present disclosure.

As illustrated in FIG. 2, the fraud detection device 20 includes a processor 21, a main memory 22, a storage 23, and a communication interface 24.

[0025]

The processor 21 is, for example, a central processing unit (CPU) and performs
10 processes of the fraud detection device 20. The functions of the processor 21 will be described later.

[0026]

The main memory 22 includes a memory area which is required for operation of the processor 21.

15 [0027]

The storage 23 is a so-called auxiliary storage device.

Examples of the storage 23 include a magnetic disk, a magneto-optical disc, and a semiconductor memory. The storage 23 may be an internal medium connected directly to a bus of a computer or may be an external medium connected to the fraud
20 detection device 20 (computer) via the communication interface 24 or a communication line.

[0028]

The communication interface 24 is an interface for transmitting and receiving information with respect to an external device (the portable information terminal 30 and
25 the roadside antenna device 11).

[0029]

The functions of the processor 21 will be described below. The processor 21 serves as a recording unit 210, a comparison unit 214, and a determination unit 215 by operating in accordance with a predetermined program. The recording unit 210
5 includes a first recording unit 211, a second recording unit 212, and a third recording unit 213.

[0030]

The first recording unit 211 receives the portable information terminal information D1 including a plurality of time-series sets D10 of the position information
10 D13 of the vehicle V and the data creation time D14 indicating a time at which the position information D13 has been acquired and the onboard device ID (D12) which is the identification information of the vehicle V from the portable information terminal 30 placed in the vehicle V and records the received portable information terminal information D1 on the storage 23.

15 [0031]

The second recording unit 212 receives the onboard device information D2 including a plurality of time-series sets D20 of the position information D23 of the vehicle V and the data creation time D24 indicating a time at which the position information D23 has been acquired and the onboard device ID (D22) which is the
20 identification information of the vehicle V from the onboard device 10 installed in the vehicle V and records the received portable information terminal information D1 on the storage 23. At that time, the second recording unit 212 receives the onboard device information D2 from the onboard device 10 via the roadside antenna device 11 and records the received onboard device information D2.

25 [0032]

The third recording unit 213 receives the roadside antenna information D3 including the installation place position information D32 or/and the identification ID (D31) of the roadside antenna device 11 having received the onboard device information D2, the onboard device ID (D33) corresponding to the onboard device 10 which is a transmission source of the onboard device information D2, and the data creation time D35 corresponding to the time at which the onboard device information D2 has been received from the roadside antenna device 11 and records the received roadside antenna information D3 on the storage 23.

[0033]

10 The comparison unit 214 compares the portable information terminal information D1 and the onboard device information D2 in which the onboard device ID (D12) and the onboard device ID (D22) match. At that time, for example, the comparison unit 214 compares the position information D13 and the position information D23 in which a time difference between the data creation time D14 and the data creation time D24 is less than a predetermined time difference or/and compares the data creation time D14 and the data creation time D24 in which a distance between the position information D13 and the position information D23 is less than a predetermined distance. For example, the comparison unit 214 compares the acceleration data D15 and the acceleration data D25 in which a time difference between the data creation time D14 and the data creation time D24 is less than a predetermined time difference or/and compares the acceleration data D15 and the acceleration data D25 in which a distance between the position information D13 and the position information D23 is less than a predetermined distance. For example, the comparison unit 214 compares the portable information terminal information D1 and the roadside antenna information D3 in which the onboard device ID (D12) and the onboard device ID (D33) included in the roadside antenna

15

20

25

information D3 match.

[0034]

The determination unit 215 determines whether there is a suspicion of impersonation in the portable information terminal information D1 on the basis of the comparison results from the comparison unit 214. At that time, for example, when the distance between the position information D13 and the position information D23 which have been compared is greater than a predetermined position threshold value (which is also referred to as a first threshold value) or the time difference between the data creation time D14 and the data creation time D24 which have been compared is greater than a predetermined time threshold value (which is also referred to as a second threshold value), the determination unit 215 determines that there is a suspicion of impersonation in the portable information terminal information D1. Alternatively, when the difference between the acceleration data D15 and the acceleration data D25 which have been compared is greater than a predetermined acceleration threshold value (which is also referred to as a third threshold value), the determination unit 215 determines that there is a suspicion of impersonation in the portable information terminal information D1. Alternatively, when the distance between the position information D13 and the installation place position information D32 is greater than a predetermined threshold value (which is also referred to as a fourth threshold value) or the time difference between the data creation time D14 and the data creation time D35 is greater than a predetermined threshold value (which is also referred to as a fifth threshold value), the determination unit 215 determines that there is a suspicion of impersonation in the portable information terminal information D1.

[0035]

The determination unit 215 records information indicating that the determination

process on each piece of data has been completed in the storage 23 in correlation with, for example, the portable information terminal information D1 and records information indicating that it is determined that there is a suspicion of impersonation in the storage 23 in correlation with the data (for example, the onboard device ID) when it is determined
5 that there is a suspicion of impersonation.

[0036]

The comparison unit 214 and the determination unit 215 may perform the comparison and determination processes, for example, repeatedly at intervals of a predetermined period or may perform the comparison and determination processes, for
10 example, only when the vehicle V has entered a specific determination area or the vehicle V has passed through the specific determination area. The specific determination area is, for example, an entrance or an exit of a toll road or a charging area or an area corresponding to a transit point such as a junction to a plurality of roads. When the portable information terminal information D1 including the position information in such
15 an area is received or the onboard device 10 communicates with the roadside antenna device 11 in such an area and receives the roadside antenna information D3, the comparison and determination processes can be performed.

[0037]

(Threshold values)

20 The threshold values depend on position information acquisition cycles in the onboard device 10 and the portable information terminal 30. For example, when the onboard device 10 acquires the position information at intervals of 200 m and the vehicle V travels at 180 km/h, a transit time is 4 seconds. When at least two positioning points with an interval of 200 m are secured by the portable information terminal 30,
25 positioning is required every 2 seconds. When it is assumed that any of two points is

included in the interval of 200 m even when a positioning error, missing, or the like occurs and it is assumed that a positioning point is necessarily included in three sections including previous and subsequent sections, the threshold values can be set, for example, as follows.

5 [0038]

The position threshold value (the first threshold value) and the fourth threshold value can be set to, for example, 200 m. The time threshold value (the second threshold value) and the fifth threshold value can be set to, for example, 4 seconds.

[0039]

10 The acceleration depends on a time difference, a road structure, or a traffic jam. In an expressway, for example, the acceleration threshold value (the third threshold value) can be set to, for example, 40 km/(h*h).

[0040]

In the present embodiment, since falsification of data from the onboard device
15 10 is more difficult than falsification of data from the portable information terminal 30, whether there is a suspicion of impersonation is determined on the basis of the assumption that data (position information and time information) from the onboard device 10 is basically correct.

[0041]

20 The operations of the recording unit 210 (the first recording unit 211, the second recording unit 212, and the third recording unit 213), the comparison unit 214, and the determination unit 215 are stored in the storage 23 in the form of a program. The processor 21 reads the program from the storage 23, loads the read program to the main memory 22, and performs the aforementioned processes in accordance with the program.

25 The processor 21 secures storage areas corresponding to the recording unit 210 (the first

recording unit 211, the second recording unit 212, and the third recording unit 213), the comparison unit 214, and the determination unit 215 in the main memory 22 in accordance with the program.

[0042]

- 5 The program may be a program for realizing some of the functions which is to be performed by a computer. For example, the program may be a program for realizing the functions in combination with another program stored in advance in the storage 23 or in combination with another program installed in another device.

[0043]

- 10 The program may be a program for realizing some of the aforementioned functions. The program may be a so-called differential file (a differential program) for realizing the aforementioned functions in combination with another program stored in advance in the storage 23

[0044]

- 15 When the program is transmitted to a computer via a communication line, the computer having received the program may load the program to the main memory 22 and perform the aforementioned processes.

[0045]

- The fraud detection device 20 may include a customized large scale integrated
20 circuit (LSI) such as a programmable logic device (PLD) in addition to the aforementioned constituents or instead of the aforementioned constituents. Examples of the PLD include a programmable array logic (PAL) a generic array logic (GAL), a complex programmable logic device (CPLD), and a field-programmable gate array (FPGA). In this case, some or all of the functions which are realized by the processor
25 21 may be realized by the integrated circuits.

[0046]

(Process flow of fraud detection device)

A process flow of the fraud detection device 20 will be described below with reference to FIGS. 6 to 9. A process flow (FIG. 6) in which the roadside antenna

5 information D3 is not used and a process flow (FIGS. 7 to 9) in which a roadside antenna is used will be described as the process flow of the fraud detection device 20.

[0047]

FIG. 6 is a first flowchart illustrating an example of the process flow of the fraud detection device according to the embodiment of the present disclosure. FIG. 6

10 illustrates a process flow when the roadside antenna information D3 is not used. The process flow illustrated in FIG. 6 is performed, for example, repeatedly at intervals of a predetermined period or performed when position information in a specific determination area is received.

[0048]

15 In the process flow illustrated in FIG. 6, the comparison unit 214 retrieves target data of enforcement determination from the storage 23 (Step S101). In Step S101, for example, the comparison unit 214 retrieves data of a vehicle V on which the comparison and determination processes have not been performed yet or retrieves data of a vehicle V on which the comparison and determination processes have not been performed yet and
20 which includes position information in the specific determination area.

[0049]

Then, the comparison unit 214 determines whether data of the same onboard device ID in the portable information terminal information D1 and the onboard device information D2 is included in the retrieved data (Step S102). When there is no data

25 including the same onboard device ID in the portable information terminal information

D1 and the onboard device information D2 (Step S102: NO), the comparison unit 214 determines that there is no target data of determination (Step S103) and ends the enforcement determination process illustrated in FIG. 6.

[0050]

5 On the other hand, when there is data including the same onboard device ID in the portable information terminal information D1 and the onboard device information D2 (Step S102: YES), the comparison unit 214 compares data of the portable information terminal information D1 and data of the onboard device information D2 and determines whether there is a suspicion of impersonation in the target data (Step S104).

10 [0051]

 Then, the determination unit 215 determines whether the position information (a distance between the position information) is less than the position threshold value and the time (a time difference between the times) is less than the time threshold value (Step S105). When the position information is greater than the position threshold value or the time is greater than the time threshold value (Step S105: NO), the determination unit 215 determines that there is a suspicion of impersonation in the portable information terminal information D1 in which data is greater than the threshold value (Step S106). When the position information is less than the position threshold value or the time is less than the time threshold value (Step S105: YES), the determination unit 215 determines that there is no suspicion of impersonation of data in the portable information terminal information D1 (Step S107).

[0052]

 FIGS. 7 and 8 are second and third flowcharts illustrating an example of the process flow of the fraud detection device according to the embodiment of the present disclosure. The flowcharts illustrated in FIGS. 7 and 8 illustrate process flows when the

roadside antenna information D3 is used. The process flows illustrated in FIGS. 7 and 8 are performed, for example, repeatedly at intervals of a predetermined period. The process flow illustrated in FIG. 7 and the process flow illustrated in FIG. 8 are connected by a coupler C1. The processes of Steps S101 to S106 illustrated in FIG. 7 are the same as the processes of Steps S101 to S106 described above with reference to FIG. 6. In Step S101 illustrated in FIG. 7, for example, the comparison unit 214 retrieves data of a vehicle V on which the comparison and determination processes have not been performed yet.

[0053]

10 In FIG. 7, when the position information is less than the position threshold value or the time is less than the time threshold value (Step S105: YES), the comparison unit 214 retrieves the roadside antenna information D3 corresponding to enforcement determination from the storage 23 (Step S201).

[0054]

15 Then, the comparison unit 214 determines whether data with the same onboard device ID in the portable information terminal information D1 and the roadside antenna information D3 is included in the retrieved data (Step S202 of FIG. 8). When there is no data with the same onboard device ID in the portable information terminal information D1 and the roadside antenna information D3 (Step S202: NO), the comparison unit 214 determines that there is no target data of determination (Step S203), and the enforcement determination process illustrated in FIGS. 7 and 8 ends.

[0055]

On the other hand, when there is data with the same onboard device ID in the portable information terminal information D1 and the roadside antenna information D3 (Step S202: YES), the comparison unit 214 compares data in the portable information

25

terminal information D1 and data in the roadside antenna information D3 and determines whether there is a suspicion of impersonation in the target data (Step S204).

[0056]

Then, the determination unit 215 determines whether the position information (a
 5 distance between the position information) is less than the fourth threshold value and the
 time (a time difference between the times) is less than the fifth threshold value (Step
 S205). When the position information is greater than the fourth threshold value or the
 time is greater than the fifth threshold value (Step S205: NO), the determination unit 215
 determines that there is a suspicion of impersonation in the portable information terminal
 10 information D1 in which data is greater than the threshold values (Step S206). When
 the position information is less than the fourth threshold value or the time is less than the
 fifth threshold value (Step S205: YES), the determination unit 215 determines that there
 is no suspicion of impersonation of data in the portable information terminal information
 D1 (Step S207).

15 [0057]

FIG. 9 is a fourth flowchart illustrating an example of the process flow of the
 fraud detection device according to the embodiment of the present disclosure. The
 coupler C1 illustrated in FIG. 9 is connected to the coupler C1 illustrated in FIG. 8. The
 flowcharts illustrated in FIGS. 9 and 8 illustrate process flows when the roadside antenna
 20 information D3 is used. The process flows illustrated in FIGS. 9 and 8 are performed,
 for example, when position information in a specific determination area is received.
 The processes of Steps S101 and S102 and Steps S104 to S106 illustrated in FIG. 9 are
 the same as the processes of Steps S101 and S102 and Steps S104 to S106 described
 above with reference to FIG. 6. In Step S101 illustrated in FIG. 9, for example, the
 25 comparison unit 214 retrieves data of a vehicle V on which the comparison and

determination processes have not been performed yet and which includes the position information in the specific determination area. In Step S102 illustrated in FIG. 9, when there is no data with the same onboard device ID in the portable information terminal information D1 and the onboard device information D2 (Step S102: NO), the comparison unit 214 retrieves the roadside antenna information D3 corresponding to the enforcement determination from the storage 23 (Step S201). The processes of Step S201 and steps subsequent thereto are the same as described above with reference to FIG. 8.

[0058]

As described above, according to the present embodiment, when the portable information terminal information D1 includes data with a suspicion of impersonation (position information or time information), it is possible to detect a suspicion of impersonation on the basis of the onboard device information D2 or the onboard device information D2 and the roadside antenna information D3.

[0059]

When it is determined that there is a suspicion of impersonation, the followings are conceivable as the subsequent processes in the fraud detection system 1. For example, a past travel history is retrieved as a suspicion of a fraud vehicle (a past suspicion of impersonation with the same onboard device ID is determined).

Alternatively, for example, when there is a strong suspicion of impersonation such as

repetition of multiple times, a process of transmitting a report to an authority concerned can be supported (for example, information for recommending a report is notified of).

Alternatively, a process of stopping a card for the electronic toll collection system or a credit card can be supported. A process of collecting fares later on the basis of personal information which can be acquired from the onboard device information can be

supported.

[0060]

According to the present embodiment, since the fraud detection device 20 can collect the position information acquired by the portable information terminal 30 via the wide area network 42, it is possible to utilize data of arbitrary areas and road lines in the country using probe information without blank information. For example, traffic jam counter measures based on earlier detection of a traffic jam, traffic safety measures based on earlier detection of traffic abnormality, dynamic price setting, area charging, fare measures such as traveling fares, physical distribution support such as traveling monitoring of large vehicles and monitoring of hazmat vehicles, and public traffic support such as periodical service information provision are conceivable as the utilization of data.

[0061]

According to the present embodiment, it is possible to easily diversify payment forms by cooperating with other application software such as electronic payment using two-dimensional codes which operates in the portable information terminal 30 or enabling fare payment using carrier payment.

[0062]

(Operations and effects)

According to the present embodiment, when the portable information terminal information D1 acquired from the portable information terminal 30 includes data with a suspicion of impersonation (position information, time information, or both thereof), it is possible to detect a suspicion of impersonation on the basis of the onboard device information D2 or the onboard device information D2 and the roadside antenna information D3.

25 [0063]

While an embodiment of the present disclosure has been described above, the embodiment has been presented as an example and is not intended to limit the scope of the invention. The embodiment can be embodied in various other forms, and various omissions, substitutions, and modifications can be added without departing from the gist of the invention. The embodiment and modifications thereof are included the inventions described in the appended claims and equivalents thereto as included in the scope or the gist of the invention.

[0064]

(Other embodiments)

For example, in the aforementioned embodiment, the onboard device information D2 and the roadside antenna information D3 are used as information to be compared with the portable information terminal information D1, but the present disclosure is not limited thereto. For example, when a vehicle V is an automated driving vehicle or the like and has a driving support function or an automated driving function using the GNSS, probe information including position information or time information may be acquired from a control device of the vehicle V. In this case, the fraud detection device 20 receives the probe information including position information or time information from the control device of the vehicle V, for example, via the wide area network 42. It is possible to detect a suspicion of impersonation by comparing the portable information terminal information D1 acquired from the portable information terminal 30 with the probe information including position information or time information acquired from the control device of the vehicle V. In this case, the control device of the vehicle V is an example of an “onboard device” in the present disclosure.

[0065]

By installing an imaging device in the vicinity of the roadside antenna device 11

or regardless of an installation position of the roadside antenna device 11, recognizing, for example, number plate information of the vehicle V or appearance information of the vehicle V, and comparing the recognized information with information registered in advance, it may be possible to detect a suspicion of impersonation.

5 [0066]

<Remarks>

For example, the fraud detection device described above in the embodiment can be understood as follows.

[0067]

10 (1) A fraud detection device 20 according to a first aspect includes a first recording unit 211 configured to receive and record first probe information (portable information terminal information D1) including a plurality of time-series sets of first position information which is position information of a vehicle V and first time information indicating a time at which the first position information is acquired and first
15 identification information which is identification information of the vehicle from a portable information terminal 30 placed in the vehicle V, a second recording unit 212 configured to receive and record second probe information (onboard device information D2) including a plurality of time-series sets of second position information which is position information of the vehicle V and second time information indicating a time at
20 which the second position information is acquired and second identification information which is identification information of the vehicle from an onboard device (onboard device 10) installed in the vehicle V, a comparison unit 214 configured to compare the first probe information and the second probe information in which the first identification information and the second identification information match, and a determination unit
25 215 configured to determine whether there is a suspicion of impersonation in the first

probe information on the basis of a comparison result from the comparison unit 214.

According to this aspect and the following aspects, when probe information (portable information terminal information D1) acquired from the portable information terminal 30 includes data (position information or time information or both thereof) with a suspicion
5 of impersonation, it is possible to detect a suspicion of impersonation on the basis of the onboard device information D2.

[0068]

(2) A fraud detection device 20 according to a second aspect is the fraud detection device 20 according to (1), wherein the comparison unit compares the first
10 position information and the second position information in which a time difference between the first time information and the second time information is less than a predetermined time difference or/and compares the first time information and the second time information in which a distance between the first position information and the second position information is less than a predetermined distance, and the determination
15 unit determines that there is a suspicion of impersonation in the first probe information when the distance between the first position information and the second position information which have been compared is greater than a first threshold value or the time difference between the first time information and the second time information which have been compared is greater than a second threshold value. According to this aspect,
20 when position information or time information is greater than a predetermined threshold value, it is possible to determine that there is a suspicion of impersonation.

[0069]

(3) A fraud detection device 20 according to a third aspect is the fraud detection device 20 according to (1) or (2), wherein the first probe information includes first
25 acceleration information indicating acceleration of the vehicle, the second probe

information includes second acceleration information indicating the acceleration of the vehicle, the comparison unit compares the first acceleration information and the second acceleration information in which a time difference between the first time information and the second time information is less than a predetermined time difference or/and
 5 compares the first acceleration information and the second acceleration information in which a distance between the first position information and the second position information is less than a predetermined distance, and the determination unit determines that there is a suspicion of impersonation in the first probe information when a difference between the first acceleration information and the second acceleration information which
 10 have been compared is greater than a third threshold value. According to this aspect, when the acceleration difference is greater than a predetermined threshold value, it is possible to determine that there is a suspicion of impersonation.

[0070]

(4) A fraud detection device 20 according to a fourth aspect is the fraud
 15 detection device 20 according to any one of (1) to (3), wherein the onboard device transmits the second probe information to a roadside antenna device which is provided on a roadside of a road on which the vehicle is traveling, the second recording unit receives and records the second probe information from the onboard device via the roadside antenna device, the fraud detection device further includes a third recording unit
 20 configured to receive and record third probe information (roadside antenna information D3) including position information or/and identification information of the roadside antenna device via which the second probe information has been received, the second identification information corresponding to the onboard device which is a transmission source of the second probe information, and third time information corresponding to a
 25 time at which the second probe information has been received from the roadside antenna

device, the comparison unit compares the first probe information and the third probe information in which the first identification information and the second identification information included in the third probe information match, and the determination unit determines that there is a suspicion of impersonation in the first probe information when

5 a distance between the first position information and the position information of the roadside antenna device is greater than a fourth threshold value or a time difference between the first time information and the third time information is greater than a fifth threshold value. According to this aspect, when probe information (portable information terminal information D1) acquired from the portable information terminal 30

10 includes data (position information or time information or both thereof) with a suspicion of impersonation, it is possible to detect a suspicion of impersonation on the basis of both of the onboard device information D2 and the roadside antenna information D3.

INDUSTRIAL APPLICABILITY

[0071]

15 With the fraud detection device, the fraud detection system, the fraud detection method, and the program according to the present disclosure, it is possible to detect impersonation when a portable information terminal is used.

REFERENCE SIGNS LIST

[0072]

20 1 Fraud detection system

10 Onboard device

11 Roadside antenna device

20 Fraud detection device

21 Processor

25 30 Portable information terminal

210 Recording unit

211 First recording unit

212 Second recording unit

213 Third recording unit

5 214 Comparison unit

215 Determination unit

22 Main memory

23 Storage

24 Communication interface

CLAIMS

[Claim 1] A fraud detection device comprising:

a first recording unit configured to receive and record first probe information including a plurality of time-series sets of first position information which is position
5 information of a vehicle and first time information indicating a time at which the first position information is acquired and first identification information which is identification information of the vehicle from a portable information terminal placed in the vehicle;

a second recording unit configured to receive and record second probe
10 information including a plurality of time-series sets of second position information which is position information of the vehicle and second time information indicating a time at which the second position information is acquired and second identification information which is identification information of the vehicle from an onboard device installed in the vehicle;

15 a comparison unit configured to compare the first probe information and the second probe information in which the first identification information and the second identification information match; and

a determination unit configured to determine whether there is a suspicion of impersonation in the first probe information on the basis of a comparison result from the
20 comparison unit.

[Claim 2] The fraud detection device according to claim 1, wherein the comparison unit compares the first position information and the second position information in which a time difference between the first time information and the second time information is less than a predetermined time difference or/and compares the first time information and the
25 second time information in which a distance between the first position information and

the second position information is less than a predetermined distance, and

wherein the determination unit determines that there is a suspicion of impersonation in the first probe information when the distance between the first position information and the second position information which have been compared is greater than a first threshold value or the time difference between the first time information and the second time information which have been compared is greater than a second threshold value.

[Claim 3] The fraud detection device according to claim 2, wherein the first probe information includes first acceleration information indicating acceleration of the vehicle,

wherein the second probe information includes second acceleration information indicating acceleration of the vehicle,

wherein the comparison unit compares the first acceleration information and the second acceleration information in which a time difference between the first time information and the second time information is less than a predetermined time difference

or/and compares the first acceleration information and the second acceleration information in which a distance between the first position information and the second position information is less than a predetermined distance, and

wherein the determination unit determines that there is a suspicion of impersonation in the first probe information when a difference between the first acceleration information and the second acceleration information which have been compared is greater than a third threshold value.

[Claim 4] The fraud detection device according to any one of claims 1 to 3, wherein the onboard device transmits the second probe information to a roadside antenna device which is provided on a roadside of a road on which the vehicle is traveling,

wherein the second recording unit receives and records the second probe

information from the onboard device via the roadside antenna device,

wherein the fraud detection device further comprises a third recording unit configured to receive and record third probe information including position information or/and identification information of the roadside antenna device via which the second
5 probe information has been received, the second identification information corresponding to the onboard device which is a transmission source of the second probe information, and third time information corresponding to a time at which the second probe information has been received from the roadside antenna device,

wherein the comparison unit compares the first probe information and the third
10 probe information in which the first identification information and the second identification information included in the third probe information match, and

wherein the determination unit determines that there is a suspicion of impersonation in the first probe information when a distance between the first position information and the position information of the roadside antenna device is greater than a
15 fourth threshold value or a time difference between the first time information and the third time information is greater than a fifth threshold value.

[Claim 5] A fraud detection system comprising: a fraud detection device including

a first recording unit configured to receive and record first probe information including a plurality of time-series sets of first position information which is
20 position information of a vehicle and first time information indicating a time at which the first position information is acquired and first identification information which is identification information of the vehicle from a portable information terminal placed in the vehicle,

a second recording unit configured to receive and record second probe
25 information including a plurality of time-series sets of second position information which

is position information of the vehicle and second time information indicating a time at which the second position information is acquired and second identification information which is identification information of the vehicle from an onboard device installed in the vehicle,

5 a comparison unit configured to compare the first probe information and the second probe information in which the first identification information and the second identification information match, and

 a determination unit configured to determine whether there is a suspicion of impersonation in the first probe information on the basis of a comparison
10 result from the comparison unit; and
 the onboard device.

[Claim 6] A fraud detection method comprising:

 a step of receiving and recording first probe information including a plurality of time-series sets of first position information which is position information of a vehicle
15 and first time information indicating a time at which the first position information is acquired and first identification information which is identification information of the vehicle from a portable information terminal placed in the vehicle;

 a step of receiving and recording second probe information including a plurality of time-series sets of second position information which is position information of the
20 vehicle and second time information indicating a time at which the second position information is acquired and second identification information which is identification information of the vehicle from an onboard device installed in the vehicle;

 a step of comparing the first probe information and the second probe information in which the first identification information and the second identification
25 information match; and

a step of determining whether there is a suspicion of impersonation in the first probe information on the basis of a comparison result.

[Claim 7] A program causing a computer to perform:

5 a step of receiving and recording first probe information including a plurality of time-series sets of first position information which is position information of a vehicle and first time information indicating a time at which the first position information is acquired and first identification information which is identification information of the vehicle from a portable information terminal placed in the vehicle;

10 a step of receiving and recording second probe information including a plurality of time-series sets of second position information which is position information of the vehicle and second time information indicating a time at which the second position information is acquired and second identification information which is identification information of the vehicle from an onboard device installed in the vehicle;

15 a step of comparing the first probe information and the second probe information in which the first identification information and the second identification information match; and

a step of determining whether there is a suspicion of impersonation in the first probe information on the basis of a comparison result.