

Method and Apparatus for Recognizing Illegal Behavior in Unattended Scenario

Technical Field

[001] This specification relates to the field of Internet technology, and in particular, to a method and apparatus for recognizing an unauthorized behavior in an unattended scene.

Background

[002] With the development of science and technology, more and more unattended scenes are seen in daily life, such as unmanned supermarkets, unmanned gyms, and unmanned Karaoke boxes. However, without human supervision, an unattended scene may also be subjected to some unauthorized behaviors, such as leaving without payment after eating or drinking in unmanned supermarkets, damaging fitness facilities in unmanned gyms, etc. Therefore, an effective solution for recognizing unauthorized behaviors needs to be provided in unattended scenes.

Summary

[003] In view of the foregoing, this specification discloses a method and apparatus for recognizing an unauthorized behavior in an unattended scene.

[004] For example, this specification is achieved by the following technical solutions:

[005] a method for recognizing an unauthorized behavior in an unattended scene, comprising:

[006] obtaining body data of a user in an unattended scene;

[007] obtaining feature data of an object in the unattended scene; and

[008] recognizing whether the user performs an unauthorized behavior according to the body data and the feature data of the object.

[009] An apparatus for recognizing an unauthorized behavior in an unattended scene, comprising:

[010] a first acquisition unit, configured to obtain body data of a user in an unattended scene;

[011] a second acquisition unit, configured to obtain feature data of an object in the unattended scene; and

[012] a behavior recognition unit configured to recognize whether the user performs an unauthorized behavior according to the body data and the feature data of the object.

[013] An apparatus for recognizing an unauthorized behavior in an unattended scenario,

comprising:

- [014] a processor;
- [015] a memory for storing machine-executable instructions,
- [016] wherein through reading and executing machine-executable instructions stored in the memory and correspond to a logic for recognizing an unauthorized behavior in an unattended scene, the processor is enabled to:
 - [017] obtain body data of a user in an unattended scene;
 - [018] obtain feature data of an object in the unattended scene; and
 - [019] recognize whether the user performs an unauthorized behavior according to the body data and the feature data of the object.
- [020] It can be seen from the above description that, the body data of the user and the feature data of the object in the unattended scene can be obtained, and actual conditions of the user and the object are combined to recognize an unauthorized behavior, thereby achieving effective recognition of the unauthorized behavior in the unattended scene.

Brief Description of the Drawings

- [021] FIG. 1 is a schematic flow chart of a method for recognizing an unauthorized behavior in an unattended scene according to an exemplary embodiment of this specification;
- [022] FIG. 2 is a schematic flow chart of another method for recognizing an unauthorized behavior in an unattended scene according to an exemplary embodiment of this specification;
- [023] FIG. 3 is a schematic flow chart of another method for recognizing an unauthorized behavior in an unattended scene according to an exemplary embodiment of this specification;
- [024] FIG. 4 is a schematic structural diagram of an apparatus for recognizing an unauthorized behavior in an unattended scene according to an exemplary embodiment of this specification; and
- [025] FIG. 5 is a block diagram of an apparatus for recognizing an unauthorized behavior in an unattended scene according to an exemplary embodiment of this specification.

Detailed Description

- [026] Exemplary embodiments are described in detail herein, examples of which are illustrated in the drawings. When the following description involves drawings, the same numbers in different drawings represent the same or similar elements unless otherwise indicated. The implementation manners described in the following exemplary embodiments do not represent all implementation manners consistent with this specification. Conversely,

they are merely examples of apparatuses and methods consistent with some aspects of this specification, as detailed in the attached claims.

[027] Terms used in this specification are only aimed at describing specific embodiments rather than limiting this specification. In this specification and the claims, the singular forms “a,” “an,” and “the” are intended to indicate the plural forms as well, unless the context clearly indicates otherwise. It should also be understood that the term “and/or” used herein refers to and includes any or all possible combinations of one or more associated listed items.

[028] It should be understood that although terms such as first, second, and third may be used in this specification to describe various information, the information should not be limited thereto. These terms are only used to distinguish one another for information of the same type. For example, without departing from the scope of this specification, first information may also be referred to as second information; and similarly, second information may also be referred to as first information. Depending on the context, the word “if” used herein can be interpreted as “at the time of,” “when,” or “in response to determination.”

[029] FIG. 1 is a schematic flow chart of a method for recognizing an unauthorized behavior in an unattended scene according to an exemplary embodiment of this specification.

[030] The method for recognizing an unauthorized behavior in an unattended scene can be applied to a front-end recognition device in an unattended scene, such as a recognition device with a processing function deployed in an unattended scene. The recognition method may also be applied to a back-end device for recognition in an unattended scene, such as a back-end recognition device, which is not limited by this specification.

[031] In FIG. 1, the method for recognizing an unauthorized behavior in an unattended scene may include the following steps.

[032] Step 102: Obtain body data of a user in an unattended scene.

[033] In some embodiments, the acquisition of the body data may be started after the user enters the unattended scene.

[034] The body data may include body behavior data and body position data of the user; and the body of the user may include: limbs, mouth, and other parts.

[035] In some embodiments, the body data of the user in the unattended scene may be obtained by using a machine vision technology. The body data may also be obtained by using other technologies, which is not limited by this specification.

[036] Step 104: Obtain feature data of an object in the unattended scene.

[037] In this embodiment, the acquisition of the feature data may also be started after the user enters the unattended scene.

[038] Here, the object may be an object in an unattended scene, such as goods in an unmanned supermarket, a cabinet in which the goods are placed in the unmanned supermarket, or fitness equipment in an unmanned gym.

[039] The feature data may include: position data of the object, external surface image data of the object, vibration data obtained by a sensor disposed in the object, and the like.

[040] In some embodiments, the feature data of the object in the unattended scene may also be obtained by using a machine vision technology. The feature data may also be obtained by other means such as a sensor, which is not limited by this specification.

[041] Step 106: Recognize whether the user performs an unauthorized behavior according to the body data and the feature data of the object.

[042] In some embodiments, the obtained body data and the feature data may be analyzed to determine whether the user in the unattended scene performs an unauthorized behavior, such as damaging goods.

[043] It can be seen from the above description that the body data of the user and the feature data of the object in the unattended scene can be obtained, and actual conditions of the user and the object are combined to recognize an unauthorized behavior, thereby achieving effective recognition of the unauthorized behavior in the unattended scene.

[044] The implementation process of this description is described below in detail using an example in which the unattended scene is an unmanned supermarket and the unauthorized behavior is unauthorized eating or drinking or damaging a cabinet.

[045] In the unmanned supermarket scene, after a user enters the unmanned supermarket, the acquisition of body data of the user and feature data of an object may be started to determine whether the user performs an unauthorized behavior, and can be ended after the user leaves the unmanned supermarket.

[046] There may be several methods for determining whether the user enters or leaves the unmanned supermarket.

[047] For example, when a user triggers opening of a door of the unmanned supermarket from the outside, it can be determined that the user enters the unmanned supermarket; when the user triggers opening of a door of the unmanned supermarket from the inside, it can be determined that the user leaves the unmanned supermarket.

[048] In another embodiment, when a recognition apparatus in the unmanned supermarket recognizes a living person, it can be determined that the user enters the unmanned supermarket; when the recognition apparatus in the unmanned supermarket cannot recognize a living person, it can determine that the user leaves the unmanned supermarket.

[049] With respect to solutions for triggering opening of the door of the unmanned supermarket and recognizing a living person by the recognition apparatus as described above, references may be made to related technologies, which are not elaborated in detail in this embodiment.

[050] In addition to the above-described solutions, other methods may further be used to determine whether the user enters or leaves the unmanned supermarket, which is not limited by this embodiment.

[051] I. Unauthorized eating or drinking as the unauthorized behavior.

[052] In the unmanned supermarket scene, a user may eat or drink in the supermarket after entering thereinto, and leaves without payment, causing economic losses to the unmanned supermarket.

[053] As shown in FIG. 2, the method for recognizing an unauthorized eating or drinking behavior in this embodiment may include the following steps.

[054] Step 202: Obtain mouth position data of the user in the unmanned supermarket.

[055] In this embodiment, face features of the user may be obtained first, and the user's mouth is then recognized, and mouth position data of the user is further obtained. For example, after the mouth of the user is recognized, the mouth position data of the user can be calculated according to the relative position relationship between the user's mouth and an acquisition apparatus. Certainly, in actual application, the mouth position data of the user may alternatively be obtained by other means, which is not limited by this embodiment.

[056] The mouth position data may be longitudinal and latitudinal data of the mouth.

[057] The mouth position data may be relative position data of the mouth in the unmanned supermarket. For example, a spatial point in the unmanned supermarket (for example, the foot of a wall of the unmanned supermarket) can be used as an origin to establish a spatial orthogonal coordinate system, and then coordinates of the user's mouth in the spatial orthogonal coordinate system can be used as the mouth position data, which is not limited by this specification.

[058] Step 204: Obtain position data of an object in the unmanned supermarket.

[059] In this embodiment, during the recognition of unauthorized eating or drinking, the

object may refer to goods to be sold in the unmanned supermarket.

[060] In some embodiments, if a Radio Frequency Identification (RFID) tag is disposed on the goods, the position data of the goods can be determined by the RFID positioning technology. If no RFID tag is disposed on the goods, the position data of the goods can be determined by using other positioning technologies, which is not limited by this embodiment.

[061] In this embodiment, since there are usually plenty of goods for sale in the unmanned supermarket, initial positions of each piece of goods can be stored in advance. For example, the positions of the goods on a shelf can be used as the initial positions. When the position of a certain piece of goods is determined not to be the initial position, the subsequent steps of this embodiment can be performed.

[062] In this embodiment, similar to the mouth position data of the user, the object position data may be longitudinal and latitudinal data, or relative position data of the object in the unmanned supermarket, which is not limited by this embodiment.

[063] Step 206: Calculate a distance between the user's mouth and the object according to the mouth position data and the object position data.

[064] In this embodiment, when the distance between the user's mouth and the object is calculated, the mouth position data and the object position data obtained at the same time point are usually used to ensure the accuracy of the above-described distance.

[065] Step 208: When a length of time that the distance between the mouth and the object is within a distance threshold reaches a preset length of time, determine that the user performs an unauthorized eating or drinking behavior.

[066] In some embodiments, the distance threshold may be preset, such as 20 cm or 30 cm.

[067] When the distance between the user's mouth and the goods is within the above-described distance threshold, it usually indicates that the distance between the user's mouth and the goods may be short, and the user may be smelling the goods or unauthorizedly eating or drinking the goods.

[068] If the user wants to smell the goods, the length of time that the distance between the user's mouth and the goods is within the distance threshold may be shorter; and if the user is eating or drinking the goods unauthorizedly, the length of time that the distance between the user's mouth and the goods is within the distance threshold may be longer. Therefore, when the length of time that the distance between the user's mouth and the goods is within the distance threshold reaches a preset length, it can be determined that the user is eating or

drinking unauthorizedly. In other words, the user performs an unauthorized eating or drinking behavior.

[069] Here, the above-described preset duration may also be set in advance, such as 5 s or 10 s.

[070] It can be seen from the above description that in this embodiment, when the length of time that the distance between the user's mouth and the goods is within the preset distance threshold in an unattended scene reaches the preset length, it can be determined that the user performs an unauthorized eating or drinking behavior, thereby achieving the recognition of the unauthorized eating or drinking behavior in the unattended scene.

[071] Alternatively, in order to avoid misrecognition and to improve accuracy in recognizing an unauthorized eating or drinking behavior, mouth behavior data of the user may also be obtained as the body data of the user; and whether the mouth behavior data matches a preset mouth movement pattern (such as a chewing pattern or a swallowing pattern) can be determined.

[072] If the obtained mouth behavior data matches the preset mouth movement pattern, and the length of time that the distance between the user's mouth and the goods is within a distance threshold reaches a preset length, it can be determined that the user is eating or drinking unauthorizedly, i.e., the user performs an unauthorized eating or drinking behavior.

[073] If the obtained mouth behavior data does not match the preset mouth movement pattern, it can be determined that the user does not perform an unauthorized eating or drinking behavior.

[074] Whether the mouth behavior data of the user matches the preset mouth movement pattern may be determined before or after step 206 shown in FIG. 2, or may be determined while step 206 is performed, which is not limited by this embodiment.

[075] Optionally, in order to avoid misrecognition and to improve the accuracy in recognizing an unauthorized eating or drinking behavior, attribute category data may further be obtained as the feature data of the goods. The attribute category data may refer to classification of the goods, such as edible and inedible.

[076] If the user eats or drinks unauthorizedly in the unmanned supermarket, the goods selected by the user must be in the edible category. Therefore, when the length of time that the distance between the user's mouth and the goods is within a distance threshold reaches a preset length and an attribute category of the goods falls in the edible category, it can be

determined that the user is eating or drinking unauthorizedly. For example, if the attribute category of the goods is bottled drinking water, and the length of time that the distance between the user and the bottled drinking water is within a distance threshold reaches a preset length, it can be determined that the user drinks the bottled drinking water unauthorizedly.

[077] If the length of time that the distance between the user's mouth and the goods is within a distance threshold reaches a preset length but the attribute category of the goods does not fall in the edible category, it can be determined that the user is not eating or drinking unauthorizedly. For example, when the attribute category of the goods is a household commodity and the length of time that the distance between the user and the household commodity is within a distance threshold reaches a preset length, it can also be determined that the user does not perform an unauthorized eating or drinking behavior.

[078] The attribute category of the goods can be determined before or after step 206 shown in FIG. 2, or may be determined while step 206 is performed, which is not limited by this embodiment.

[079] Optionally, in order to avoid misrecognition and to improve the accuracy in recognizing an unauthorized eating or drinking behavior, external surface image data of the goods may further be obtained as the feature data of the goods. The external surface image data can usually be understood as an external package image of the goods.

[080] Some edible goods in the unmanned supermarket can only be eaten after unpacking; thus, whether the external surface image data of the goods matches a default external surface image may further be determined. Here, the default external surface image can be stored in advance. If the external surface image data of the goods matches the default external surface image, it may indicate that the external package of the goods is not damaged; and if the external surface image data of the goods does not match the default external surface image, it may indicate that the external package of the goods is damaged.

[081] In this example, when the length of time that the distance between the user's mouth and the goods is within a distance threshold reaches a preset length and the external package of the goods is damaged, it can be determined that the user performs an unauthorized behavior.

[082] The external surface image data of the goods can be matched before or after step 206 shown in FIG. 2, or may be matched while step 206 is performed, which is not limited by this embodiment.

[083] In actual application, the above-described various solutions may be combined, or

other recognition solutions may be adopted to recognize an unauthorized eating or drinking behavior, which is not limited by this specification.

[084] II. Damaging a cabinet as the unauthorized behavior.

[085] In the unmanned supermarket scene, after entering the unmanned supermarket, the user may damage the goods or other objects in the unmanned supermarket. For example, the user may kick a cabinet, causing losses to the unmanned supermarket.

[086] For the unauthorized behavior of damaging a cabinet, refer to FIG. 3. The recognition method provided in this embodiment may include the following steps:

[087] Step 302: Obtain limb behavior data of the user in the unmanned supermarket.

[088] In this embodiment, the limb behavior data may include arm behavior data, leg behavior data, and the like.

[089] In this embodiment, the limb behavior data of the user over a period of time may be obtained for analyzing the user's limb movement.

[090] Step 304: Obtain vibration data of the cabinet in the unmanned supermarket.

[091] In some embodiments, a sensor such as a gyroscope sensor or an acceleration sensor may be disposed on the cabinet in the unmanned supermarket to obtain the vibration data of the cabinet.

[092] Certainly, if no sensors are disposed on the cabinet, and the vibration data of the cabinet may be obtained alternatively by using other technologies such as a machine vision technology.

[093] Whether the cabinet vibrates can be determined based on the obtained vibration data.

[094] Step 306: When the limb behavior data of the user matches a preset limb movement pattern and the cabinet vibrates, determine that the user performs an unauthorized behavior.

[095] Based on the above-described step 302, after the limb behavior data of the user is obtained, whether the limb behavior data matches the preset limb movement pattern, such as a "smashing" pattern, a "kicking" pattern, or a "stepping on" pattern, can be determined.

[096] If the limb behavior data matches the preset limb movement pattern, it indicates that the user may be damaging goods in the unmanned supermarket, and the determination can be continued.

[097] If the limb behavior data does not match the preset limb movement pattern, it may indicate that the user is not performing an unauthorized behavior of damaging goods in the unmanned supermarket.

[098] Based on the above-described step 304, after the vibration data of the cabinet is obtained, whether the cabinet vibrates can be determined according to the vibration data.

[099] If the cabinet vibrates and the limb behavior data of the user matches the above-described preset limb movement pattern, it can be determined that the user performs an unauthorized behavior of damaging the cabinet.

[100] If the cabinet does not vibrate, it can be determined that the user does not perform an unauthorized behavior of damaging the cabinet.

[101] It can be seen from the above description that when the limb behavior data of the user in the unattended scene matches the preset disruptive limb movement pattern and the object vibrates, it can be determined that the user performs an unauthorized behavior of damaging an object, thereby achieving the recognition of the unauthorized disruptive behavior in the unattended scene.

[102] Optionally, in another example, during the recognition of an unauthorized damaging behavior, the distance between the above-described object and the user's limb that matches the above-described limb movement pattern may further be calculated. If the distance is within a preset range, i.e., the distance is short, it can be determined that the user performs an unauthorized behavior of damaging the object.

[103] Optionally, in another example, the user may also damage goods to be sold in the unmanned supermarket other than the cabinet. For example, the user may tear the external package of the goods. Therefore, during the recognition of an unauthorized disruptive behavior, external surface image data of the object may further be obtained; and whether the obtained external surface image data matches a default external surface image of the object may be determined to determine whether the external package of the object is damaged.

[104] External surface image data of cabinets in the unmanned supermarket, fitness equipment in the unmanned gym and other objects may also be obtained and matched with default external surface images, which is not limited by this embodiment. However, as objects such as cabinets and fitness equipment are usually sturdy, external surface images of the objects may not change even if the objects are damaged by the user. In order to improve the accuracy of recognition, other data further can be obtained for recognition.

[105] In actual application, the above-described recognition solutions can be combined to recognize whether the user performs an unauthorized disruptive behavior or other recognition solutions can be adopted, which is not limited by this specification.

[106] In addition, during the implementation of the above-described recognition solutions, developers may establish a corresponding behavior recognition model first, and then improve the behavior recognition model through continuous training. Before the behavior recognition model is improved, if the user's unauthorized behavior cannot be determined according to the body data of the user and the feature data of the object, a determination request may be output to relevant personnel. The personnel can make a determination manually and return a result of determination to improve the above-described behavior recognition model. Certainly, when the user's unauthorized behavior cannot be determined according to the body data of the user and the feature data of the object, the acquisition and recognition of the above-described body data and feature data may be continued. If the unauthorized behavior still cannot be recognized after a certain period of time, a determination request may also be output to the relevant personnel to request a manual intervention.

[107] After the unauthorized behavior of the user is recognized, the user may be warned or penalized for the unauthorized behavior in different ways.

[108] In one example, when the user performs an unauthorized behavior, the user can be subjected to a credit penalty.

[109] For example, before entering the unattended scene, the user can undergo identity authentication, such as scanning a QR code before entering the unmanned supermarket to allow the unmanned supermarket to obtain the user's account information.

[110] If the user performs an unauthorized behavior, the credit information of his account can be updated in a negative direction. For example, a credit rating of the user is lowered.

[111] In another example, if the user performs an unauthorized behavior, the unauthorized behavior may be reported in the unattended scene. For example, the unauthorized behavior of the user may be broadcast in audio form or may be played back in video form as a warning.

[112] In another example, if the user performs an unauthorized behavior, an amount of resources corresponding to the object targeted by the unauthorized behavior may be added to the user's bill. The amount of resources may refer to the value of the object.

[113] For example, if the user unauthorizedly eats potato chips in the unmanned supermarket, the cost of the potato chips can be added to the user's bill. The user will still be charged for the corresponding fees even if the user discards the package in the unmanned supermarket after eating the potato chips.

[114] If the user damages a cabinet in the unmanned supermarket, a fine corresponding to the behavior of damaging the cabinet can be added to the user's bill to achieve the purpose of

penalizing the user.

[115] Certainly, in actual application, when the user performs an unauthorized behavior, the user may be penalized in other ways (for example, the unauthorized behavior of the user is made public in the industry), which is not limited by this specification.

[116] Corresponding to the above-described embodiments of the method for recognizing an unauthorized behavior in an unattended scene, this specification further provides an embodiment of an apparatus for recognizing an unauthorized behavior in an unattended scene.

[117] The embodiments of the apparatus for recognizing an unauthorized behavior in an unattended scene in this specification can be applied to a recognition device. The apparatus embodiment may be achieved by software, hardware, or a combination thereof. Using software to achieve the apparatus embodiment as an example, the apparatus in a logical sense is formed by reading, by a processor in the recognition device in which the apparatus is located, a corresponding computer program instruction in a non-volatile memory into an internal storage thereof and running the same. In terms of hardware, FIG. 4 is a hardware structural diagram of a recognition device in which the apparatus for recognizing an unauthorized behavior in an unattended scene is located. In addition to a processor, an internal storage, a network interface, and a non-volatile memory shown in FIG. 4, usually the recognition device in which the apparatus of this embodiment is located may further include other hardware according to actual functions of the recognition device. Details are not described herein.

[118] FIG. 5 is a block diagram of an apparatus for recognizing an unauthorized behavior in an unattended scene according to an exemplary embodiment of this specification.

[119] Referring to FIG. 5, the apparatus 400 for recognizing an unauthorized behavior in an unattended scene can be applied to the above-described recognition device shown in FIG. 4, and includes a first acquisition unit 401, a second acquisition unit 402, a behavior recognition unit 403, a credit penalty unit 404, a broadcast penalty unit 405, and a resource penalty unit 406.

[120] The first acquisition unit 401 is configured to obtain body data of a user in an unattended scene.

[121] The second acquisition unit 402 is configured to obtain feature data of an object in the unattended scene.

- [122] The behavior recognition unit 403 recognizes, according to the body data and the feature data of the object, whether the user performs an unauthorized behavior.
- [123] Optionally, the body data includes mouth position data of the user.
- [124] The feature data includes object position data of the object.
- [125] The behavior recognition unit 403 may be configured to calculate the distance between the user's mouth and the object according to the mouth position data and the object position data. When the length of time that the distance between the mouth and the object is within a distance threshold reaches a preset length, determines that the user performs an unauthorized behavior.
- [126] In some embodiments, the body data may further include mouth behavior data of the user.
- [127] When the length of time that the distance between the mouth and the object is within a distance threshold reaches a preset length and the mouth behavior data of the user matches a preset mouth movement pattern, the behavior recognition unit 403 recognizes that the user performs an unauthorized behavior.
- [128] In some embodiments, the feature data further includes attribute category data of the object.
- [129] When the length of time that the distance between the mouth and the object is within a distance threshold reaches a preset length and the attribute category of the object falls in the edible category, the behavior recognition unit 403 is configured to determine that the user performs an unauthorized behavior.
- [130] Optionally, the feature data further includes external surface image data of the object.
- [131] When the length of time that the distance between the mouth and the object is within a distance threshold reaches a preset length and the external surface image of the object does not match a default external surface image, the behavior recognition unit 403 is configured to determine that the user performs an unauthorized behavior.
- [132] Optionally, the body data may include limb data of the user.
- [133] The feature data may include vibration data of the object.
- [134] When the limb behavior data of the user matches a preset limb movement pattern and the object vibrates, the behavior recognition unit 403 is configured to determine that the user performs an unauthorized behavior.

[135] Optionally, the vibration data can be obtained by a sensor disposed on the object.

[136] The credit penalty unit 404 is configured to inflict a credit penalty on the user when the user performs an unauthorized behavior.

[137] The broadcast penalty unit 405 broadcasts, when the user performs an unauthorized behavior, the unauthorized behavior in the unattended scene.

[138] The resource penalty unit 406 is configured to add an amount of resources corresponding to the object to the user's bill when the user performs an unauthorized behavior.

[139] For details about the implementation process of functions and effects of each unit in the above-described apparatus, see the implementation process of the corresponding steps in the above-described method. Details are not described herein again.

[140] Since the apparatus embodiments correspond to the method embodiments, for relevant portions, reference may be made to the specifications in the method embodiments. The above-described apparatus embodiments are only examples. Units described as separate components may or may not be physically separated, and components displayed as units may or may not be physical units, i.e., may be located at one place or be distributed on multiple network units. Some or all of the modules may be selected according to actual needs to achieve the objectives of the solutions in this specification. A person of ordinary skill in the art can understand and implement the solutions without creative efforts.

[141] Systems, apparatuses, modules, or units described in the above embodiments may be implemented by computer chips or physical objects, or by products with certain functions. A typical type of implementation device is a computer, and a specific form of the computer may be a personal computer, a laptop computer, a mobile phone, a camera phone, a smart phone, a personal digital assistant, a media player, a navigation device, an email sending and receiving device, a game console, a tablet computer, a wearable device, or a combination of any of these devices.

[142] Corresponding to the above-described embodiments of the method for recognizing an unauthorized behavior in an unattended scene, this specification further provides a device for recognizing an unauthorized behavior in an unattended scene. The device for recognizing an unauthorized behavior in an unattended scene includes a processor and a memory for storing a machine-executable instruction. Here, the processor and the memory are usually connected to each other through an internal bus. In other possible implementations, the

device may further include an external interface to enable communications with other equipment or components.

[143] In this embodiment, through reading and executing a machine-executable instruction that is stored in the memory and that corresponds to a logic for recognizing an unauthorized behavior in an unattended scenario, the processor is enabled to:

[144] obtain body data of a user in an unattended scene;

[145] obtain feature data of an object in the unattended scene; and

[146] recognize whether the user performs an unauthorized behavior according to the body data and the feature data of the object.

[147] Optionally, the body data includes mouth position data of the user.

[148] The feature data includes object position data of the object.

[149] When the user performs an unauthorized behavior according to the body data and the feature data of the object is recognized, the processor is enabled to:

[150] calculate the distance between the user's mouth and the object according to the mouth position data and the object position data.

[151] When the length of time that the distance between the mouth and the object is within a distance threshold reaches a preset length, determine that the user performs an unauthorized behavior.

[152] Optionally, the body data further includes mouth behavior data of the user.

[153] When the user performs an unauthorized behavior according to the body data and the feature data of the object, the processor is enabled to:

[154] when the length of time that the distance between the mouth and the object is within a distance threshold reaches a preset length and the mouth behavior data of the user matches a preset mouth movement pattern, determine that the user performs an unauthorized behavior.

[155] Optionally, the feature data further includes attribute category data of the object.

[156] When the user performs an unauthorized behavior according to the body data and the feature data of the object is recognized, the processor is enabled to:

[157] when the length of time that the distance between the mouth and the object is within a distance threshold reaches a preset length and the attribute category of the object falls in an edible category, determine that the user performs an unauthorized behavior.

[158] Optionally, the feature data further includes external surface image data of the object.

[159] When the user performs an unauthorized behavior according to the body data and the feature data of the object is recognized, the processor is enabled to:

[160] when the length of time that the distance between the mouth and the object is within a distance threshold reaches a preset length, and the external surface image of the object does not match a default external surface image, determine that the user performs an unauthorized behavior.

[161] Optionally, the body data includes limb behavior data of the user.

[162] The feature data includes vibration data of the object.

[163] To determine whether the user performs an unauthorized behavior according to the body data and the feature data of the, the processor is enabled to:

[164] when the limb behavior data of the user matches a preset limb movement pattern and the object vibrates, determine that the user performs an unauthorized behavior.

[165] Alternatively, the vibration data is obtained by a sensor disposed on the object.

[166] Alternatively, through reading and executing the machine-executable instruction stored in the memory and that corresponds to a logic for recognizing an unauthorized behavior in an unattended scene, the processor is further enabled to:

[167] when the user performs an unauthorized behavior, inflict a credit penalty on the user.

[168] Alternatively, through reading and executing the machine-executable instruction stored in the memory and that corresponds to a logic for recognizing an unauthorized behavior in an unattended scene, the processor is further enabled to:

[169] if the user performs an unauthorized behavior, broadcast the unauthorized behavior in the unattended scene.

[170] Alternatively, through reading and executing the machine-executable instruction stored in the memory and that corresponds to a logic for recognizing an unauthorized behavior in an unattended scene, the processor is further enabled to:

[171] if the user performs an unauthorized behavior, add an amount of resources corresponding to the object to the user's bill.

[172] Corresponding to the above-described embodiments of the method for recognizing an unauthorized behavior in an unattended scene, this specification further provides a computer-readable storage medium. The computer-readable storage medium stores a computer program, which is executed by a processor to perform the following steps:

[173] obtain body data of a user in an unattended scene;

[174] obtain feature data of an object in the unattended scene; and

[175] recognize whether the user performs an unauthorized behavior according to the body data and the feature data of the object.

[176] Alternatively, the body data includes mouth position data of the user.

[177] The feature data includes object position data of the object.

[178] Recognizing whether the user performs an unauthorized behavior according to the body data and the feature data of the object includes:

[179] calculating the distance between the user's mouth and the object according to the mouth position data and the object position data; and

[180] when the length of time that the distance between the mouth and the object is within a distance threshold reaches a preset length, determining that the user performs an unauthorized behavior.

[181] Alternatively, the body data further includes mouth behavior data of the user.

[182] Recognizing whether the user performs an unauthorized behavior according to the body data and the feature data of the object includes:

[183] when the length of time that the distance between the mouth and the object is within a distance threshold reaches a preset length and the mouth behavior data of the user matches a preset mouth movement pattern, determining that the user performs an unauthorized behavior.

[184] Alternatively, the feature data further includes attribute category data of the object.

[185] Recognizing whether the user performs an unauthorized behavior according to the body data and the feature data of the object includes:

[186] when the length of time that the distance between the mouth and the object is within a distance threshold reaches a preset length and the attribute category of the object falls in an edible category, determining that the user performs an unauthorized behavior.

[187] Alternatively, the feature data further includes external surface image data of the object.

[188] Recognizing whether the user performs an unauthorized behavior according to the body data and the feature data of the object includes:

[189] when the length of time that the distance between the mouth and the object is within a distance threshold reaches a preset length, and the external surface image of the object does not match a default external surface image, determining that the user performs an unauthorized behavior.

[190] Alternatively, the body data includes limb data of the user.

- [191] The feature data includes vibration data of the object.
- [192] Recognizing whether the user performs an unauthorized behavior according to the body data and the feature data of the object includes:
- [193] when the limb behavior data of the user matches a preset limb movement pattern and the object vibrates, determining that the user performs an unauthorized behavior.
- [194] Alternatively, the vibration data is obtained by a sensor disposed on the object.
- [195] Alternatively, the following is further included:
- [196] when the user performs an unauthorized behavior, inflicting a credit penalty on the user.
- [197] Alternatively, the following is further included:
- [198] if the user performs an unauthorized behavior, broadcast the unauthorized behavior in the unattended scene.
- [199] Alternatively, the following is further included:
- [200] if the user performs an unauthorized behavior, add an amount of resources corresponding to the object to the user's bill.
- [201] The embodiments of this specification are described above. Other embodiments are within the scope of the attached claims. In some cases, actions or steps in the claims may be performed in a sequence different from that in the embodiments and the desired result can still be achieved. In addition, the desired result can still be achieved if the processes described in the drawings are not necessarily performed in the illustrated particular or continuous sequence. In some implementations, multitasking and parallel processing are also feasible or may be advantageous.
- [202] The above embodiments are only preferred embodiments of this specification and are not intended to limit this specification. Any modification, equivalent replacement, or improvement made within the spirit and principles of this specification shall fall within the scope of this specification.

CLAIMS

1. A method for recognizing an unauthorized eating or drinking behavior, comprising:
obtaining, through machine vision, body movement pattern data of a user;
obtaining mouth position data of the user;
obtaining feature data of an object, the feature data comprising:
 position data of the object based on a radio frequency identification tag on the object,
 attribute category data of the object, and
 external surface image data of the object;
comparing the body movement pattern data with a preset body movement pattern; and
determining that the user's behavior is unauthorized eating or drinking in response to the body movement pattern data matching the preset body movement pattern and that:
 a distance between the user's mouth and the object is within a distance threshold over a preset length of time,
 the attribute category of the object is an edible category, and
 the external surface image data does not match a default external surface image of the object.
2. The method according to claim 1, wherein
the body movement pattern data comprises mouth behavior data of the user; and
the preset body movement pattern comprises a preset mouth movement pattern.
3. The method according to claim 1, wherein the determining that the user's behavior is unauthorized comprises:
 when the preset category is an edible category, determining that the user performs the unauthorized behavior.
4. The method according to claim 1, wherein
the body movement pattern data comprises limb behavior data of the user;
the preset body movement pattern comprises a preset limb movement pattern;
the feature data further comprises vibration data of the object, wherein the vibration data is obtained with a sensor on the object; and
the determining that the user's behavior is unauthorized in response to the body movement pattern data matching the preset body movement pattern comprises:

determining a vibration state of the object based on the vibration data; and when the limb behavior data matches the preset limb movement pattern and the object vibrates, determining that the user performs the unauthorized behavior.

5. The method according to claim 1, wherein the obtaining feature data of an object includes obtaining the feature data through machine vision.

6. A method for recognizing an unauthorized eating or drinking behavior, comprising:
obtaining, through machine vision, body data of a user, wherein the body movement pattern data includes mouth position data of the user;

obtaining feature data of an object, wherein the feature data comprises object position data of the object and attribute category data of the object;

comparing the body data with a preset body movement pattern; and

in response to the body data matching the preset body movement pattern and the feature data meeting preset conditions, determining the unauthorized eating or drinking behavior of the user based on the body data and the feature data by:

determining the attribute category of the object is an edible category,

calculating a distance between the user's mouth and the object according to the mouth position data and the object position data, and

determining a length of time that the distance between the mouth and the object is within a distance threshold.

7. The method according to claim 6, wherein
the object position data is obtained with a radio frequency identification tag.

8. The method according to claim 7, wherein the determining the unauthorized behavior of the user comprises:

when the length of time reaches a preset length of time, determining that the user performs the unauthorized behavior.

9. The method according to claim 7, wherein
the body data further comprises mouth behavior data of the user;
the preset body movement pattern comprises a preset mouth movement pattern; and
the determining the unauthorized behavior of the user comprises:

when the length of time reaches a preset length of time and the mouth behavior data matches the preset mouth movement pattern, determining that the user performs the unauthorized behavior.

10. The method according to claim 7, wherein:

the determining the unauthorized behavior of the user comprises:

when the length of time reaches a preset length of time, determining that the user performs the unauthorized behavior.

11. The method according to claim 7, wherein

the feature data further comprises external surface image data of the object;

the preset conditions include the external surface image data does not match a default external surface image; and

the determining the unauthorized behavior of the user comprises:

when the length of time reaches a preset length of time, determining that the user performs the unauthorized behavior.

12. The method according to claim 6, wherein

the body data comprises limb behavior data of the user;

the preset body movement pattern comprises a preset limb movement pattern;

the feature data comprises vibration data of the object, wherein the vibration data is obtained with a sensor on the object; and

the preset conditions include that the object vibrates.

13. A method for recognizing an unauthorized behavior, comprising:

obtaining body data of a user, wherein the body data comprises mouth position data of the user;

obtaining feature data of an object, wherein the feature data comprises object position data of the object and attribute category data of the object; and

determining, according to a behavior recognition model trained with results of recognizing unauthorized behaviors, the unauthorized eating or drinking behavior of the user based on the body data, the feature data, and preset body movement patterns, by:

determining the attribute category of the object is an edible category,

calculating a distance between the user's mouth and the object according to the

mouth position data and the object position data, and

determining a length of time that the distance between the mouth and the object is within a distance threshold.

14. The method according to claim 13, wherein

the object position data is obtained with a radio frequency identification tag.

15. The method according to claim 14, wherein the determining the unauthorized behavior of the user comprises:

when the length of time reaches a preset length of time, determining that the user performs the unauthorized behavior.

16. The method according to claim 14, wherein

the determining the unauthorized behavior of the user comprises:

when the length of time reaches a preset length of time and the mouth behavior data matches the preset mouth movement pattern, determining that the user performs the unauthorized behavior.

17. The method according to claim 14, wherein

the feature data further comprises external surface image data of the object; and

the determining the unauthorized behavior of the user comprises:

when the length of time reaches a preset length of time and the external surface image data does not match a default external surface image, determining that the user performs the unauthorized behavior.

18. The method according to claim 14, wherein

the determining the unauthorized behavior of the user comprises:

when the length of time reaches a predetermined length of time, determining that the user performs the unauthorized behavior.

19. The method according to claim 14, wherein

the body data comprises limb behavior data of the user;

the preset body movement pattern comprises a preset limb movement pattern;

the feature data comprises vibration data of the object, wherein the vibration data is

obtained with a sensor on the object; and

the determining the unauthorized behavior of the user comprises:

determining a vibration state of the object based on the vibration data; and

when the limb behavior data matches the preset limb movement pattern and the object vibrates, determining that the user performs the unauthorized behavior.