

DATA SECURITY PROCESSING METHOD AND APPARATUS, DEVICE AND STORAGE MEDIUM

TECHNICAL FIELD

[0001] The present application relates to the field of computer communication, and relates, but is not limited, to a data security processing method and apparatus, a device and a storage medium.

BACKGROUND

[0002] Along with continuous deepening understanding of information security of people, the technical level of information security guarantee is also continuously advanced. Especially in artificial intelligence services, some specific service processing needs to store video information collected for an actual generation environment to ensure that the service execution process is analyzable. Meanwhile, an electronic device executing the service needs to collect data again according to the change of the actual environment information, and debug or improve the collected data. In order to achieve the purpose, data needs to be stored and used, which involves the problem of data protection.

SUMMARY

[0003] Embodiments of the present application provide a data security processing method and apparatus, a device and a storage medium.

[0004] The technical solutions of the embodiments of the present application are implemented as follows.

[0005] In a first aspect, the embodiments of the present application provide a data

security processing method, which includes the following operations.

- [0006] Recovered data stored in a data storage system is acquired; and the recovered data includes at least one frame of image collected in a data generation environment and an identification result of each frame of image.
- [0007] Fuzzification processing is carried out on a target object in each frame of image to obtain a corresponding candidate frame of image.
- [0008] The corresponding candidate frame of image is marked based on the identification result of each frame of image to obtain target data; and the target data is used as a training sample for training an image recognition model.
- [0009] In some possible embodiments, the operation that fuzzification processing is carried out on a target object in each frame of image to obtain a corresponding candidate frame of image includes the following operations: sensitive information of the recovered data is determined based on a service attribute of the data generation environment; the target object in each frame of image is determined based on the sensitive information; and mosaic processing is carried out on the target object in each frame of image to obtain the corresponding candidate frame of image.
- [0010] Therefore, by determining the sensitive information of the recovered data in the data generation environment and further performing mosaic processing on the target content corresponding to the sensitive information, the sensitive content in the image may be ensured not to be leaked, and the security of the recovered data is guaranteed.
- [0011] In some possible embodiments, the operation that the corresponding candidate frame of image is marked based on the identification result of each frame of image to obtain target data includes the following operations: a marking request is sent to a remote virtual machine; the marking request includes the identification result of each frame of image and the corresponding candidate frame of image; a marking response sent by the remote virtual machine is received; and the marking response includes target data obtained by marking the corresponding candidate frame of image based on the identification result of each frame of image.

[0012] Therefore, remote marking is carried out through the remote virtual machine, data may not be directly transmitted to marking personnel or marking equipment, so that the transmission risk of the recovered data is avoided, and data security is ensured.

[0013] In some possible embodiments, the data storage system is a hard disk, and the method further includes the following operations: at least one frame of image generated in the data generation environment and a recognition result of the corresponding frame of image are acquired; and the at least one frame of image and the identification result of the corresponding frame of image are written into the hard disk passing security verification as recovered data.

[0014] Therefore, the recovered data generated in the data generation environment is selectively collected and stored in the hard disk passing security verification in a persistent storage mode, so that subsequent processing may be carried out after collection.

[0015] In some possible embodiments, the hard disk includes a card slot and a processing component, the operation that the at least one frame of image and the identification result of the corresponding frame of image are written into the hard disk passing security verification as recovered data includes the following operations: an access password input by a user into the hard disk is acquired; in a case where a chip card is inserted into the card slot, the inserted chip card and the access password are respectively verified through the processing component to obtain a first verification result; and the recovered data is written into the hard disk in a case where the first verification result indicates that the inserted card and the access password pass verification.

[0016] Therefore, the hard disk may be read and written only by verifying the chip card and the access password at the same time, so that a data protection mode combining software and hardware is realized, and the persistent data may be better protected.

[0017] In some possible embodiments, the method further includes the following operations: attribute information of the hard disk is acquired, and the attribute information includes an identifier and a manufacturer of the hard disk; the identifier and the manufacturer of the hard disk are verified to obtain a second verification result; and the recovered data is written into the hard disk in a case where the second verification

result indicates that the hard disk passes verification.

[0018] Therefore, by verifying whether the manufacturer is the manufacturer designated by the service party and whether the identifier of the hard disk is matched with that of the manufacturer, it is ensured that the hard disk in which the recovered data is written passes security verification.

[0019] In some possible embodiments, the attribute information of the hard disk further includes a hidden file in the hard disk. The method further includes the following operations: encrypted characters in the hidden file in the hard disk are determined; the encrypted characters are verified to obtain a third verification result; and the recovered data is written into the hard disk in a case where the third verification result indicates that the hard disk passes verification.

[0020] Therefore, by verifying whether the appointed hidden file exists in the hard disk or not and the encrypted characters in the hidden file, it is ensured that the hard disk in which the recovered data is written passes security verification.

[0021] In a second aspect, the embodiments of the present application provide a data security processing apparatus, which includes a first acquisition module, a processing module, and a marking module.

[0022] The first acquisition module is configured to acquire recovered data stored in a data storage system; and the recovered data includes at least one frame of image collected in a data generation environment and an identification result of each frame of image.

[0023] The processing module is configured to carry out fuzzification processing on a target object in each frame of image to obtain a corresponding candidate frame of image.

[0024] The marking module is configured to mark the corresponding candidate frame of image based on the identification result of each frame of image to obtain target data; and the target data is used as a training sample for training an image recognition model.

[0025] In a third aspect, the embodiments of the present application provide an

electronic device, which includes a memory and a processor. The memory stores a computer program executable on the processor. When the processor implements the program, the steps in the data security processing method may be implemented.

[0026] In a fourth aspect, the embodiments of the present application provide a computer readable storage medium, having a computer program stored thereon. When executed by a processor, the computer program implements the steps in the data security processing method.

[0027] The technical solutions provided by the embodiments of the present application at least include the following beneficial effects.

[0028] In the embodiments of the present application, the recovered data stored in the data storage system is acquired first, the recovered data including at least one frame of image collected in the data generation environment and an identification result of each frame of image; then fuzzification processing is carried out on the target object in each frame of image to obtain the corresponding candidate frame of image; and finally, the corresponding candidate frame of image is marked based on the identification result of each frame of image to obtain the target data, the target data being used as the training sample for training the image recognition model. Therefore, the target object in the stored image collected in the data generation environment is subjected to fuzzification processing and then the image is marked, so that the security of the recovered data may be guaranteed to a great extent, and the sensitive information in the image is prevented from being leaked.

BRIEF DESCRIPTION OF THE DRAWINGS

[0029] In order to describe the technical solutions in the embodiments of the present application more clearly, the drawings required to be used in descriptions about the embodiments will be simply introduced below. Apparently, the drawings described below are only some embodiments of the present application, and other drawings may further be obtained by those skilled in the art according to the drawings without creative work.

[0030] FIG. 1 is a schematic flow diagram of a data security processing method according to an embodiment of the present application.

[0031] FIG. 2 is a schematic flow diagram of a data security processing method according to an embodiment of the present application.

[0032] FIG. 3 is a schematic flow diagram of a data security processing method according to an embodiment of the present application.

[0033] FIG. 4 is a schematic flow diagram of a data security processing method according to an embodiment of the present application.

[0034] FIG. 5 is a schematic flow diagram of a data security processing method according to an embodiment of the present application.

[0035] FIG. 6 is a schematic diagram of a composition structure of a data security processing apparatus according to an embodiment of the present application.

[0036] FIG. 7 is a schematic diagram of a hardware entity of an electronic device according to an embodiment of the present application.

DETAILED DESCRIPTION

[0037] In order to make the purpose, the technical solutions and the advantages of the embodiments of the present application clearer, the technical solutions in the embodiments of the present application will be clearly and completely described below in combination with the drawings in the embodiments of the present application, and it is apparent that the described embodiments are only part rather all of embodiments of the present application. The following embodiments are used to illustrate the present application, but are not intended to limit the scope of the present application. All other embodiments obtained by those of ordinary skill in the art based on the embodiments of the present application without creative efforts shall fall within the protection scope of the present application.

[0038] "Some embodiments" involved in the following descriptions describes a subset of all possible embodiments. However, it can be understood that "some embodiments" may be the same subset or different subsets of all the possible embodiments, and may be combined without conflicts.

[0039] It is to be pointed out that term "first/second/third" involved in the embodiments of the application is only for distinguishing similar objects and does not represent a specific sequence of the objects. It can be understood that "first/second/third" may be interchanged to specific sequences or orders if allowed to implement the embodiments of the application described herein in sequences except the illustrated or described ones.

[0040] Those skilled in the art can understand that, unless otherwise defined, all the terms (including technical terms and scientific terms) used herein have the same meanings usually understood by those of ordinary skill in the art of the embodiments of the application. It should also be understood that terms defined in, for example, a general dictionary, should be understood to have the same meanings as those in the context of the conventional art, and may not be explained as idealized or too formal meanings, unless otherwise specifically defined like those here.

[0041] The embodiment of the present application provides a data security processing method, applied to an electronic device. The electronic device includes, but is not limited to, a mobile phone, a notebook computer, a tablet computer, a handheld Internet device, a multimedia device, a streaming media device, a mobile Internet device, a wearable device or other types of electronic facilities. The functions realized by the method may be realized by calling program codes through a processor in the electronic device, the program codes may be stored in a computer storage medium, and it can be seen that the electronic device at least includes the processor and the storage medium. The processor may be configured to process the data security management process, and the memory may be configured to store data needed in the data security management process and generated data.

[0042] FIG. 1 is a schematic flow diagram of a data security processing method according to an embodiment of the present application. As shown in FIG. 1, the method

at least includes the following steps.

[0043] In S110, recovered data stored in a data storage system is acquired.

[0044] Here, the recovered data includes at least one frame of image collected in a data generation environment and an identification result of each frame of image. The at least one frame of image may be an image acquired in real time by an image acquisition device arranged in the data generation environment, such as a camera module, and also may be an image transmitted to a side-end device in the data generation environment by other devices in an instant messaging mode, and the side-end device is an edge computing node or an artificial intelligence (AI) server. The embodiment of the present application does not limit the form of generating the image data.

[0045] In some possible implementation modes, the camera module arranged in the data generation environment captures real-scene images in a visual field range in real time, and transmits a plurality of continuous frames of real-scene images as a video stream to a processor of the side-end device. Image processing modules for detection algorithm, recognition algorithm, association algorithm and other algorithms are arranged in the side-end device, and each image in the video stream is sequentially processed through image processing module.

[0046] It is to be noted that because data distribution in the data generation environment is inconsistent with that of a test environment, abnormal data may occur in the data generation environment, and the like, the problem that the recognition accuracy of image recognition is reduced in a real production environment generally occurs. For example, a face recognition model has difficulty in recognizing a human face wearing a mask due to the fact that the proportion of the human face wearing the mask in a test set is not high, and the service recognition rate is reduced. Therefore, data and processing result produced in the data generation environment need to be collected into a storage device so as to be used for reproducing problems, model training, or as test data sets of other new services after collecting.

[0047] In S120, fuzzification processing is carried out on a target object in each frame of image to obtain a corresponding candidate frame of image.

[0048] Here, the fuzzification processing may be mosaic processing, fuzzification blurring, covering or other processes. Fuzzification processing is carried out on a target object in each frame of image, so that the details of the area where the target object is located may not be displayed, that is, the target object in the obtained candidate frame of image may not be recognized.

[0049] Mosaic processing is to degrade color gradation details of the area where the target object in each frame of image is located and to disorder color blocks. This fuzzification appears to be composed of small grids one by one. Fuzzification blurring generally adopts a Gaussian blur algorithm and is usually used for reducing image noise and reducing the detail level of an image area where the target object is located, essentially, each pixel of the target object takes the average value of peripheral pixels, in numerical value, smoothing is achieved, and in graph, the fuzzification effect is generated.

[0050] In one possible implementation mode, the image detection module may determine all objects in each frame of image by detecting and identifying each frame of image. It can be understood that the target object may be set according to actual needs, for example, the target object may include, but is not limited to, specific objects in a real-scene image are set to be target objects based on service scenes, for example, for entertainment venues, personal privacy of customers is regarded as sensitive information, and therefore, the target object in a game image collected in the entertainment venues may be the human face; or the object in the middle area in the real-scene image is set as the target object; or after the object in the real-scene image is recognized, the user may select the target object independently, and the embodiment of the present application is not limited.

[0051] In S130, the corresponding candidate frame of image is marked based on the identification result of each frame of image to obtain target data.

[0052] Here, the candidate frame of image is marked, that is, the object except the target object in the image is marked, so that the information of the target object may be prevented from being leaked to other marking personnel during manual marking.

[0053] The target data is at least one frame of image marked with other objects except the target object, and may be directly used as a training sample for training an image recognition model.

[0054] In some implementations, the manner of marking may be manual marking or automatic marking by a local data center; in some implementations, the manner of marking may also be provided to marking personnel for marking in a manner of a remote virtual machine; in some implementations, the manner of marking may also be automatic marking by an access device on which the remote virtual machine is located.

[0055] It is to be noted that, in order to avoid data leakage in the transmission process, a remote marking mode may be adopted for marking, so that data security is guaranteed to a great extent, and leakage of sensitive information is avoided.

[0056] In the embodiments of the present application, the recovered data stored in the data storage system is acquired first, and the recovered data includes at least one frame of image collected in the data generation environment and the identification result of each frame of image; then fuzzification processing is carried out on the target object in each frame of image to obtain the corresponding candidate frame of image; and finally, the corresponding candidate frame of image is marked based on the identification result of each frame of image to obtain the target data, and the target data is used as the training sample for training the image recognition model. Therefore, the target object in the stored image collected in the data generation environment is subjected to fuzzification processing and then the image is marked, so that the security of the recovered data may be guaranteed to a great extent, and the sensitive information in the image is prevented from being leaked.

[0057] FIG. 2 is a schematic flow diagram of a data security processing method according to an embodiment of the present application. As shown in FIG. 2, the method at least includes the following steps.

[0058] In S210, recovered data stored in a data storage system is acquired.

[0059] Here, the recovered data includes at least one frame of image collected in a data generation environment and an identification result of each frame of image. That is,

the recovered data is uniformly stored in the data storage system, and the corresponding recovered data is read from the data storage system when the data needs to be processed.

[0060] In S220, sensitive information of the recovered data is determined based on a service attribute of the data generation environment.

[0061] Here, the service attribute of the data generation environment may be an actual scene where a side-end device is located, namely a data source, and also may be a specific requirement of customers, a provision of related service, namely a data requirement, and the like.

[0062] Exemplarily, the data generation environment is an entertainment venue, at least one frame of game image collected from the entertainment venue is taken as the recovered data, and human face information in each frame of game image may be taken as the sensitive information according to regulations of related game services in the entertainment venue.

[0063] In S230, a target object in each frame of image is determined based on the sensitive information.

[0064] Here, after the sensitive information in each frame of image is determined, a target object corresponding to the sensitive information may be determined by adopting related image processing algorithms such as key point detection and semantic segmentation.

[0065] In S240, mosaic processing is carried out on the target object in each frame of image to obtain a corresponding candidate frame of image.

[0066] Here, the process of mosaic processing may be that the image area where the target object is located is determined first, and then the image area where the target object is located is filled with small color blocks (rectangular or square) with different colors, so that the candidate frame of image corresponding to each frame of image is obtained.

[0067] Exemplarily, mosaic processing is carried out on the human face in the game image to obtain an image with the fuzzy human face as the candidate frame of image, so

that the image may be subsequently marked and used as a test data set of other new services.

[0068] In S250, the corresponding candidate frame of image is marked based on the identification result of each frame of image to obtain target data.

[0069] Here, the target data is used as a training sample for training an image recognition model.

[0070] It is to be noted that, the candidate frame of image is marked, that is, the object except the target object in the image is marked, so that the information of the target object may be prevented from being leaked to other marking personnel during manual marking.

[0071] The common data marking includes classification marking, marking frame marking, area marking and drawing point marking, the classification marking is that an object of a determined type is marked, and the marked object is of a specific type; marking frame marking is to select the object to be detected. When the human face is recognized, the position of the human face is determined first, and then the face recognition is carried out on the area where the detection frame is located; compared with marking frame marking, the requirement of area marking is more accurate, and the edge may be flexible, such as road recognition in automatic driving; and the drawing point marking is applicable to some applications with detailed feature requirements, such as bone recognition. Generally, the sample data sets used for model training or testing have been marked.

[0072] In practical product applications, marker data is usually required to be used as prior experience to carry out supervised learning, so that the model identifies whether the type of each object is the same as the marked type or not, and the identification accuracy of the trained model meets the requirement.

[0073] In the embodiments of the present application, by determining the sensitive information of the recovered data in the data generation environment and further performing mosaic processing on the target object corresponding to the sensitive information, then marking the object except the target object, the sensitive content in the

image may be ensured not to be leaked, and therefore, the security of the recovered data is guaranteed.

[0074] FIG. 3 is a schematic flow diagram of a data security processing method according to an embodiment of the present application. As shown in FIG. 3, the method may be implemented by the following steps.

[0075] In S310, recovered data stored in a data storage system is acquired.

[0076] Here, the recovered data includes at least one frame of image collected in a data generation environment and an identification result of each frame of image.

[0077] In S320, fuzzification processing is carried out on a target object in each frame of image to obtain a corresponding candidate frame of image.

[0078] In S330, a marking request is sent to a remote virtual machine.

[0079] Here, the remote virtual machine may be a server, a virtual machine, or the like; and the marking request includes the identification result of each frame of image and the corresponding candidate frame of image.

[0080] In S340, a marking response sent by the remote virtual machine is received.

[0081] Here, the marking response includes target data obtained by marking the corresponding candidate frame of image based on the identification result of each frame of image. The target data is used as a training sample for training an image recognition model.

[0082] It is to be noted that, in implementation, marking personnel may remotely access the recovered data in the local data center by logging in the virtual machine, and mark the corresponding candidate frame of image based on the identification result of each frame of image to obtain the target data. That is, for the requirement of data marking, the data is provided for the marking personnel through the remote virtual machine, and the recovered data is not directly transmitted to the marking personnel, so that sensitive content in the recovered data is prevented from being leaked.

[0083] In the embodiment of the present application, after data recovery, each frame of image in the data storage system and the identification result of the corresponding frame of image are acquired; the target object in each frame of image is first subjected to fuzzification processing, then remote marking is carried out through the remote virtual machine, data is not directly transmitted to marking personnel or marking equipment, so that the transmission risk of the recovered data is avoided, and data security is ensured.

[0084] FIG. 4 is a schematic flow diagram of a data security processing method according to an embodiment of the present application. As shown in FIG. 4, the method may be implemented by the following steps.

[0085] In S410, at least one frame of image generated in a data generation environment and an identification result of the corresponding frame of image are acquired.

[0086] Here, the image generated in the data generation environment, the recognition result, a processing result generated in a program execution process, and the like may be selectively collected in a certain storage system in an automatic collection manner.

[0087] In S420, the at least one frame of image and the identification result of the corresponding frame of image are written into a hard disk passing security verification as recovered data.

[0088] Here, the hard disk is used as a storage mode of persistent data, and the hard disk needs to be verified to be a specific secure hard disk before the recovered data is written. Meanwhile, when part of the recovered data is read from the hard disk for processing, the identity or authority of a user needs to be verified, and the hard disk is read only after the verification passes.

[0089] It is to be noted that persistent data in the hard disk is stored on Flash granules. Due to the fact that the number of abrasion times of Flash granules is limited, when the number of abrasion times of Flash blocks exceeds the rated number of erasing and writing times, programming failure or data reading errors such as uncorrectable read errors (UNC) are likely to occur, and security problems of data storage are caused.

[0090] Therefore, the recovered data generated in the data generation environment is selectively collected and stored in the hard disk passing security verification in a persistent storage mode, so that subsequent processing may be carried out after collection.

[0091] In some implementation modes, the hard disk includes a card slot and a processing component, and S420 may be implemented by the following operations.

[0092] In S4201, an access password input by the user into the hard disk is acquired.

[0093] Here, when the user needs to read the recovered data in the hard disk, the user needs to input the access password first, and the access password is usually determined by a service party and the user in a negotiation mode.

[0094] In S4202, in a case where a chip card is inserted into the card slot, the inserted chip card and the access password are respectively verified through the processing component to obtain a first verification result.

[0095] Here, the processing component is a small box wrapped with a processing chip, and whether a card inserted into the card slot is the chip card corresponding to the hard disk or not may be verified. Meanwhile, after the corresponding chip card is inserted into the hard disk, whether the access password input by the user is consistent with the stored password of the data storage hard disk or not is verified, and the first verification result is obtained.

[0096] In S4203, the recovered data is written into the hard disk in a case where the first verification result indicates that the inserted card and the access password both pass verification.

[0097] Here, in a case where the card inserted into the card slot is the chip card corresponding to the hard disk and the access password input by the user is consistent with the stored password, the hard disk may be read and written by the user. Therefore, the recovered data may be written into the hard disk which passes the security verification.

[0098] It is to be noted that, the service party (such as a management person of an

entertainment venue) manages the chip card and the stored password at the same time, and the stored password of the hard disk is updated regularly, so that privacy protection of the persistently recovered data stored in the hard disk is ensured, and data information security in the data generation environment is guaranteed.

[0099] In S4201 to S4203, the hard disk may be read and written only by verifying the chip card and the access password at the same time, that is, a data protection mode combining software and hardware is provided by the embodiment of the present application, so that the persistent data may be better protected.

[00100] In S430, the recovered data stored in a data storage system is acquired.

[00101] Here, the recovered data includes at least one frame of image collected in a data generation environment and an identification result of each frame of image.

[00102] In S440, fuzzification processing is carried out on a target object in each frame of image to obtain a corresponding candidate frame of image.

[00103] In S450, the corresponding candidate frame of image is marked based on the identification result of each frame of image to obtain target data.

[00104] Here, the target data is used as a training sample for training an image recognition model.

[00105] In the embodiment of the present application, first, the recovered data generated in the data generation environment is selectively collected and stored in the hard disk passing security verification in a persistent storage mode, so that subsequent processing may be carried out after collection. Meanwhile, whether the hard disk is secure or not needs to be verified before the recovered data is written into the hard disk, the embodiment of the present application provides a hard disk data read-write protection solution combining software and hardware, and the persistent recovered data may be better protected.

[00106] FIG. 5 is a schematic flow diagram of a data security processing method according to an embodiment of the present application. As shown in FIG. 5, the method

may be implemented by the following steps.

- [00107] In S510, attribute information of a hard disk is acquired.
- [00108] Here, the attribute information includes an identifier and a manufacturer of the hard disk.
- [00109] It is to be noted that in a case where both a card inserted into a card slot of the hard disk and an access password input by a user pass verification, the local equipment, such as a local data center, for processing the recovered data may automatically read the attribute information of the connected hard disk.
- [00110] In S520, the identifier and the manufacturer of the hard disk are verified to obtain a second verification result.
- [00111] Here, the manufacturer is a manufacturing company of the hard disk, and the Identity Document (ID) is a unique identity under the manufacturing company.
- [00112] By verifying whether the manufacturer is the manufacturer designated by the service party and whether the identifier of the hard disk is matched with that of the manufacturer, the second verification result is obtained.
- [00113] In S530, the recovered data is written into the hard disk in a case where the second verification result indicates that the hard disk passes verification.
- [00114] Here, in a case where the manufacturer is the designated manufacturer and the identifier of the hard disk is the unique identifier under the manufacturer, it is indicated that the hard disk is correct and secure, and the recovered data may be written into the hard disk.
- [00115] In S540, encrypted characters in a hidden file in the hard disk are determined.
- [00116] Here, the hidden file is an encrypted file agreed by the service party and the manufacturer, and the file name of the hidden file is a string of encrypted characters composed of numbers and letters, which is equivalent to an agreed password.
- [00117] In S550, the encrypted characters are verified to obtain a third verification

result.

[00118] In implementation, whether the appointed hidden file exists in the hard disk or not is verified first, and if the hidden file does not exist, it is indicated that the hard disk is insecure; and in a case where the hidden file exists, the file name of the hidden file is read to obtain the encrypted characters, and whether the encrypted characters are consistent with the appointed password or not is verified to obtain the third verification result.

[00119] In S560, the recovered data is written into the hard disk in a case where the third verification result indicates that the hard disk passes verification.

[00120] Here, when the hidden file exists in the hard disk and the encrypted characters in the hidden file are correct, it is indicated that the hard disk is secure, and the recovered data may be written into the hard disk.

[00121] In the embodiment of the present application, first, whether the manufacturer is the manufacturer designated by the service party or not is verified, whether the identifier of the hard disk is matched with that of the manufacturer or not is verified, and then whether the appointed hidden file exists in the hard disk or not and the encrypted characters in the hidden file are verified. That is, the identifier of the hard disk, the manufacturer, and the hidden files contained in the hard disk are verified before the recovered data is written into the hard disk to ensure that the written hard disk is correct, and thus the persistent recovered data is better protected.

[00122] The embodiment of the present application at least may be applied to the following use scenes: video information collected in a game process needs to be saved in an entertainment venue to ensure that the game process on a game table in the entertainment venue is traceable, and at the same time, an algorithm and a service layer need to be debugged or improved according to actual scene information. In order to achieve the purpose, the recovered data needs to be stored and used, which involves the problem of data protection. By adopting the data security management scheme provided by the embodiment of the present application, the data security may be guaranteed to a great extent, and the leakage of the sensitive information is avoided.

[00123] It should be noted that the various embodiments in this specification are described in a progressive manner, each embodiment is focused on differing from the other embodiments, and the same and similar parts of the various embodiments are referred to with respect to each other.

[00124] Based on the above embodiment, the embodiment of the present application further provides a data security processing apparatus. Each module of the device and each submodule and unit of each module may be implemented through a processor in an electronic device, and of course, may also be implemented through a specific logic circuit. In an implementation process, the processor may be a Central Processing Unit (CPU), a Micro Processing Unit (MPU), a Digital Signal Processor (DSP), a Field Programmable Gate Array (FPGA), etc.

[00125] FIG. 6 is a schematic diagram of a composition structure of a data security processing apparatus according to an embodiment of the present application. As shown in FIG. 6, the apparatus 600 includes a first acquisition module 610, a processing module 620, and a marking module 630.

[00126] The first acquisition module 610 is configured to acquire recovered data stored in a data storage system; and the recovered data includes at least one frame of image collected in a data generation environment and an identification result of each frame of image.

[00127] The processing module 620 is configured to carry out fuzzification processing on a target object in each frame of image to obtain a corresponding candidate frame of image.

[00128] The marking module 630 is configured to mark the corresponding candidate frame of image based on the identification result of each frame of image to obtain target data; and the target data is used as a training sample for training an image recognition model.

[00129] In some possible embodiments, the processing module 620 includes a first determination sub-module, a second determination sub-module and a processing sub-module. The first determination sub-module is configured to determine sensitive

information of the recovered data based on a service attribute of the data generation environment; the second determination sub-module is configured to determine the target object in each frame of image based on the sensitive information; the processing sub-module is configured to carry out mosaic processing on the target object in each frame of image to obtain the corresponding candidate frame of image.

[00130] In some possible embodiments, the marking module 630 includes a sending sub-module and a receiving sub-module. The sending sub-module is configured to send a marking request to a remote virtual machine; the marking request includes the identification result of each frame of image and the corresponding candidate frame of image; the receiving sub-module is configured to receive a marking response sent by the remote virtual machine; the marking response includes target data obtained by marking the corresponding candidate frame of image based on the identification result of each frame of image.

[00131] In some possible embodiments, the data storage system is a hard disk, the device 600 further includes a second acquisition module and a storage module. The second acquisition module is configured to acquire at least one frame of image generated in the data generation environment and a recognition result of the corresponding frame of image; the storage module is configured to write the at least one frame of image and the identification result of the corresponding frame of image into the hard disk passing security verification as recovered data.

[00132] In some possible embodiments, the hard disk includes a card slot and a processing component, the storage module includes a first acquisition sub-module, a first verification sub-module and a first storage sub-module, the first acquisition sub-module is configured to acquire an access password input by a user into the hard disk; the first verification sub-module is configured to verify the inserted chip card and the access password respectively through the processing component to obtain a first verification result in a case where a chip card is inserted into the card slot; and first storage sub-module is configured to write the recovered data into the hard disk in a case where the first verification result indicates that the inserted card and the access password both pass verification.

[00133] In some possible embodiments, the storage module further includes a second acquisition sub-module, a second verification sub-module and a second storage sub-module. The second acquisition sub-module is configured to acquire attribute information of the hard disk, and the attribute information includes an identifier and a manufacturer of the hard disk; the second verification sub-module is configured to verify the identifier and the manufacturer of the hard disk to obtain a second verification result; the second storage sub-module is configured to write the recovered data into the hard disk in a case where the second verification result indicates that the hard disk passes verification.

[00134] In some possible embodiments, the attribute information of the hard disk further includes a hidden file in the hard disk. The storage module further includes a third determination sub-module, a third verification sub-module and a third storage sub-module. The third determination sub-module is configured to determine encrypted characters in the hidden file in the hard disk; the third verification sub-module is configured to verify the encrypted characters to obtain a third verification result; the third storage sub-module is configured to write the recovered data into the hard disk in a case where the third verification result indicates that the hard disk passes verification.

[00135] It is to be pointed out that descriptions about the above apparatus embodiment are similar to descriptions about the method embodiment, and beneficial effects similar to those of the method embodiment are achieved. Technical details undisclosed in the apparatus embodiments of the application may be understood with reference to the descriptions about the method embodiments of the application.

[00136] It is to be noted that, in the embodiments of the present application, when implemented in form of a software function module and sold or used as an independent product, the data security processing method may also be stored in a computer readable storage medium. Based on such an understanding, the technical solutions of the embodiments of the present application substantially or parts making contributions to the related art may be embodied in form of software product, the computer software product is stored in a storage medium, including a plurality of instructions configured to enable an electronic device (which may be a smart phone with a camera, a tablet computer, etc.)

to execute all or part of the method in each embodiment of the present application. The foregoing storage medium includes any medium that can store program codes, such as a U disk, a removable hard disk, a Read Only Memory (ROM), a magnetic disk, or an optical disc. Therefore, the embodiments of the present application are not limited to any specific hardware and software combination.

[00137] Correspondingly, the embodiments of the present application provide a computer readable storage medium, having a computer program stored thereon. The computer program, when executed by a processor, implements the steps in the data security processing method.

[00138] Correspondingly, the embodiments of the present application further provide a chip. The chip includes a programmable logic circuit and/or a program instruction. The chip, when running, is configured to implement the steps in the data security processing method in any abovementioned embodiment.

[00139] Correspondingly, the embodiments of the present application further provide a computer program product. The computer program product, when executed by a processor of an electronic device, is configured to implement the steps in the data security processing method in any abovementioned embodiment.

[00140] Based on the same technical concept, the embodiment of the present application provides an electronic device, which is configured to implement the data security processing method recorded in the method embodiment. FIG. 7 is a schematic diagram of a hardware entity an electronic device according to an embodiment of the present application. As shown in FIG. 7, the electronic device 700 includes a memory 710 and a processor 720. The memory 710 stores a computer program capable of running in the processor 720. The processor 720 executes the program to implement the steps in any data security processing method in the embodiments of the present application.

[00141] The memory 710 is configured to store an instruction and application executable for the processor 720, may also cache data (for example, image data, video data, voice communication data, and video communication data) to be processed or having been processed by the processor 720 and each module in the electronic device,

and may be implemented through a flash or a Random Access Memory (RAM).

[00142] The processor 720 executes the program to implement the steps of any data security processing method. The processor 720 usually controls overall operations of the electronic device 700.

[00143] The processor may be at least one of an Application Specific Integrated Circuit (ASIC), a Digital Signal Processor (DSP), a Digital Signal Processing Device (DSPD), a Programmable Logic Device (PLD), a Field Programmable Gate Array (FPGA), a Central Processing Unit (CPU), a controller, a microcontroller, or an MPU. It can be understood that other electronic devices may also be configured to realize functions of the processor, and no specific limits are made in the embodiments of the present application.

[00144] The computer storage medium/memory may be a memory such as a Read Only Memory (ROM), a Programmable Read-Only Memory (PROM), an Erasable Programmable Read-Only Memory (EPROM), an Electrically Erasable Programmable Read-Only Memory (EEPROM), a Ferromagnetic Random Access Memory (FRAM), a flash memory, a magnetic surface memory, an optical disk, or a Compact Disc Read-Only Memory (CD-ROM), or may be any electronic device including one or any combination of the abovementioned memories, such as a mobile phone, a computer, a tablet device, and a personal digital assistant.

[00145] It is to be pointed out here that the above descriptions about the storage medium and device embodiments are similar to the descriptions about the method embodiment, and beneficial effects similar to those of the method embodiment are achieved. Technical details undisclosed in the storage medium and device embodiment of the application are understood with reference to the descriptions about the method embodiment of the application.

[00146] It is to be understood that "one embodiment" and "an embodiment" mentioned in the whole specification mean that specific features, structures or characteristics related to the embodiment is included in at least one embodiment of the application. Therefore, "in one embodiment" or "in an embodiment" mentioned throughout the specification

does not always refer to the same embodiment. In addition, these specific features, structures or characteristics may be combined in one or more embodiments freely as appropriate. It is to be understood that, in each embodiment of the application, a magnitude of a sequence number of each process does not mean an execution sequence and the execution sequence of each process should be determined by its function and an internal logic and should not form any limit to an implementation process of the embodiments of the application. The sequence numbers of the embodiments of the application are adopted not to represent superiority-inferiority of the embodiments but only for description.

[00147] It is to be noted that terms "include" and "contain" or any other variant thereof is intended to cover nonexclusive inclusions herein, so that a process, method, object or device including a series of elements not only includes those elements but also includes other elements which are not clearly listed or further includes elements intrinsic to the process, the method, the object or the device. Under the condition of no more limitations, an element defined by the statement "including a/an....." does not exclude existence of the same other elements in a process, method, object or device including the element.

[00148] In some embodiments provided by the application, it is to be understood that the disclosed device and method may be implemented in another manner. The device embodiment described above is only schematic, and for example, division of the units is only logic function division, and other division manners may be adopted during practical implementation. For example, multiple units or components may be combined or integrated into another system, or some characteristics may be neglected or not executed. In addition, coupling or direct coupling or communication connection between each displayed or discussed component may be indirect coupling or communication connection, implemented through some interfaces, of the device or the units, and may be electrical and mechanical or adopt other forms.

[00149] The units described as separate parts may or may not be physically separated, and parts displayed as units may or may not be physical units, and namely may be located in the same place, or may also be distributed to multiple network units. Part of all of the units may be selected according to a practical requirement to achieve the purposes

of the solutions of the embodiments of the application.

[00150] In addition, each functional unit in each embodiment of the application may be integrated into a processing unit, each unit may also serve as an independent unit and two or more than two units may also be integrated into a unit. The integrated unit may be implemented in a hardware form and may also be implemented in form of hardware and software functional unit.

[00151] Or, when implemented in form of software functional module and sold or used as an independent product, the integrated unit of the application may also be stored in a computer-readable storage medium. Based on such an understanding, the technical solutions of the embodiments of the application substantially or parts making contributions to the related art may be embodied in form of a software product. The computer software product is stored in a storage medium, including a plurality of instructions configured to enable an automatic test line of a device to execute all or part of the method in each embodiment of the application. The storage medium includes: various media capable of storing program codes such as a mobile hard disk, a ROM, a magnetic disk, or an optical disc.

[00152] The methods disclosed in some method embodiments provided in the application may be freely combined without conflicts to obtain new method embodiments.

[00153] The characteristics disclosed in some method or device embodiments provided in the application may be freely combined without conflicts to obtain new method embodiments or device embodiments.

[00154] The above is only the implementation mode of the application and not intended to limit the scope of protection of the application. Any variations or replacements apparent to those skilled in the art within the technical scope disclosed by the application shall fall within the scope of protection of the application. Therefore, the scope of protection of the application shall be subject to the scope of protection of the claims.

CLAIMS

1. A data security processing method, comprising:

acquiring recovered data stored in a data storage system, wherein the recovered data comprises at least one frame of image collected in a data generation environment and an identification result of each frame of image;

carrying out fuzzification processing on a target object in the each frame of image to obtain a corresponding candidate frame of image; and

marking the corresponding candidate frame of image based on the identification result of the each frame of image to obtain target data, wherein the target data is used as a training sample for training an image recognition model.

2. The data security processing method of claim 1, wherein the carrying out fuzzification processing on a target object in the each frame of image to obtain a corresponding candidate frame of image comprises:

determining sensitive information of the recovered data based on a service attribute of the data generation environment;

determining the target object in the each frame of image based on the sensitive information; and

carrying out mosaic processing on the target object in the each frame of image to obtain a corresponding candidate frame of image.

3. The method of claim 1 or 2, the marking the corresponding candidate frame of image based on the identification result of the each frame of image to obtain target data comprises:

sending a marking request to a remote virtual machine, wherein the marking request includes the identification result of the each frame of image and the corresponding candidate frame of image; and

receiving a marking response sent by the remote virtual machine, wherein the marking response includes target data obtained by marking the corresponding candidate frame of image based on the identification result of the each frame of image.

4. The method of any of claims 1-3, wherein the data storage system is a hard disk, and the method further comprises:

acquiring at least one frame of image generated in the data generation environment and an identification result of the corresponding frame of image; and

writing the at least one frame of image and the identification result of the corresponding frame of image into the hard disk passing security verification as recovered data.

5. The method of claim 4, wherein the hard disk comprises a card slot and a processing component, wherein the writing the at least one frame of image and the identification result of the corresponding frame of image into the hard disk passing security verification as recovered data comprises:

acquiring an access password input by a user into the hard disk;

in a case where a chip card is inserted into the card slot, verifying the inserted chip card and the access password respectively through the processing component to obtain a first verification result; and

in a case where the first verification result indicates that the inserted card and the access password both pass verification, writing the recovered data into the hard disk.

6. The method of claim 4, wherein the method further comprises:

acquiring attribute information of the hard disk, wherein the attribute information comprises an identifier and a manufacturer of the hard disk;

verifying the identifier and the manufacturer of the hard disk to obtain a second verification result; and

in a case where the second verification result indicates that the hard disk passes verification, writing the recovered data into the hard disk.

7. The method of claim 6, wherein the attribute information of the hard disk further comprises a hidden file of the hard disk, and the method further comprises:

determining encrypted characters in the hidden file in the hard disk;

verifying the encrypted characters to obtain a third verification result; and

in a case where the third verification result indicates that the hard disk passes verification, writing the recovered data into the hard disk.

8. A data security processing apparatus, comprising a first acquisition module, a processing module, and a marking module, wherein

the first acquisition module is configured to acquire recovered data stored in a data storage system, wherein the recovered data comprises at least one frame of image collected in a data generation environment and an identification result of each frame of image;

the processing module is configured to carry out fuzzification processing on a target object in the each frame of image to obtain a corresponding candidate frame of image;

the marking module is configured to mark the corresponding candidate frame of image based on the identification result of the each frame of image to obtain target data, wherein the target

data is used as a training sample for training an image recognition model.

9. An electronic device, comprising a memory and a processor, wherein the memory stores a computer program executable on the processor, wherein when executing the computer program, the processor is configured to:

acquire recovered data stored in a data storage system, wherein the recovered data comprises at least one frame of image collected in a data generation environment and an identification result of each frame of image;

carry out fuzzification processing on a target object in the each frame of image to obtain a corresponding candidate frame of image; and

mark the corresponding candidate frame of image based on the identification result of the each frame of image to obtain target data, wherein the target data is used as a training sample for training an image recognition model.

10. The electronic device of claim 9, wherein when carrying out fuzzification processing on the target object in the each frame of image to obtain the corresponding candidate frame of image, the processor is configured to:

determine sensitive information of the recovered data based on a service attribute of the data generation environment;

determine the target object in the each frame of image based on the sensitive information; and

carry out mosaic processing on the target object in the each frame of image to obtain a corresponding candidate frame of image.

11. The electronic device of claim 9 or 10, wherein when marking the corresponding

candidate frame of image based on the identification result of the each frame of image to obtain target data, the processor is configured to:

send a marking request to a remote virtual machine, wherein the marking request includes the identification result of the each frame of image and the corresponding candidate frame of image; and

receive a marking response sent by the remote virtual machine, wherein the marking response includes target data obtained by marking the corresponding candidate frame of image based on the identification result of the each frame of image.

12. The electronic device of any of claims 9-11, wherein the data storage system is a hard disk, and the processor is further configured to:

acquire at least one frame of image generated in the data generation environment and an identification result of the corresponding frame of image; and

write the at least one frame of image and the identification result of the corresponding frame of image into the hard disk passing security verification as recovered data.

13. The electronic device of claim 12, wherein the hard disk comprises a card slot and a processing component, wherein when writing the at least one frame of image and the identification result of the corresponding frame of image into the hard disk passing security verification as the recovered data, the processor is configured to:

acquire an access password input by a user into the hard disk;

in a case where a chip card is inserted into the card slot, verify the inserted chip card and the access password respectively through the processing component to obtain a first verification result; and

in a case where the first verification result indicates that the inserted card and the access password both pass verification, write the recovered data into the hard disk.

14. The electronic device of claim 12, wherein the processor is further configured to:

acquire attribute information of the hard disk, wherein the attribute information comprises an identifier and a manufacturer of the hard disk;

verify the identifier and the manufacturer of the hard disk to obtain a second verification result; and

in a case where the second verification result indicates that the hard disk passes verification, write the recovered data into the hard disk.

15. The electronic device of claim 14, wherein the attribute information of the hard disk further comprises a hidden file of the hard disk, and the processor is further configured to:

determine encrypted characters in the hidden file in the hard disk;

verify the encrypted characters to obtain a third verification result; and

in a case where the third verification result indicates that the hard disk passes verification, write the recovered data into the hard disk.

16. A computer readable storage medium, having a computer program stored thereon, wherein when executed by a processor, the computer program is configured to:

acquire recovered data stored in a data storage system, wherein the recovered data comprises at least one frame of image collected in a data generation environment and an identification result of each frame of image;

carry out fuzzification processing on a target object in the each frame of image to obtain a corresponding candidate frame of image; and

mark the corresponding candidate frame of image based on the identification result of

the each frame of image to obtain target data, wherein the target data is used as a training sample for training an image recognition model.

17. The storage medium of claim 16, wherein when carrying out fuzzification processing on the target object in the each frame of image to obtain the corresponding candidate frame of image, the computer program is configured to:

determine sensitive information of the recovered data based on a service attribute of the data generation environment;

determine the target object in the each frame of image based on the sensitive information; and

carry out mosaic processing on the target object in the each frame of image to obtain a corresponding candidate frame of image.

18. The electronic device of claim 16 or 17, wherein when marking the corresponding candidate frame of image based on the identification result of the each frame of image to obtain target data, the computer program is configured to:

send a marking request to a remote virtual machine, wherein the marking request includes the identification result of the each frame of image and the corresponding candidate frame of image; and

receive a marking response sent by the remote virtual machine, wherein the marking response includes target data obtained by marking the corresponding candidate frame of image based on the identification result of the each frame of image.

19. The electronic device of any of claims 16-18, wherein the data storage system is a hard disk, and the coputer program is further configured to:

acquire at least one frame of image generated in the data generation environment and an identification result of the corresponding frame of image; and

write the at least one frame of image and the identification result of the corresponding frame of image into the hard disk passing security verification as recovered data.

20. A computer program, comprising computer instructions executable by an electronic device, wherein when executed by a processor in the electronic device, the computer instructions are configured to:

acquire recovered data stored in a data storage system, wherein the recovered data comprises at least one frame of image collected in a data generation environment and an identification result of each frame of image;

carry out fuzzification processing on a target object in the each frame of image to obtain a corresponding candidate frame of image; and

mark the corresponding candidate frame of image based on the identification result of the each frame of image to obtain target data, wherein the target data is used as a training sample for training an image recognition model.