

METHODS AND APPARATUSES FOR EVALUATING IMAGE ANONYMIZATION PERFORMANCE

TECHNICAL FIELD

[0001] Embodiments of this specification generally relate to the field of image data
5 privacy protection, and in particular, to methods and apparatuses for evaluating image
anonymization performance.

BACKGROUND

[0002] Service processing solutions based on image data have been widely applied
to a large number of applications, for example, a facial recognition-based payment
10 service. In these service processing solutions, original image data needs to be
provided as input to a third-party device for processing. Due to unpredictable security
of a running environment of the third-party device, there is a possibility that the
original image data or feature vector data obtained after feature extraction is
performed on the original image data is maliciously stolen. This poses a great threat to
15 data security or service security (for example, secure payment). As such, many image
anonymization processing solutions are provided. Before the original image data is
provided to the third-party device, image anonymization processing is performed on
the original image data by using the provided image anonymization processing
solution, to protect data privacy. For various image anonymization solutions, a
20 solution for evaluating image anonymization performance needs to be provided to
efficiently and accurately evaluate image anonymization performance.

SUMMARY

[0003] In view of the above problem, embodiments of this specification provide

method and apparatuses for evaluating image anonymization performance. According to the method and the apparatus, image anonymization performance is evaluated by comprehensively considering three factors: distinctiveness (anonymization indicator) of original image data relative to anonymized image data, distinctiveness (reverse reconstruction indicator) of the original image data relative to reconstructed image data, and image recognition distinctiveness (image recognition indicator) of the original image data relative to the anonymized image data. This can efficiently and accurately evaluate image anonymization performance.

[0004] According to an aspect of an embodiment of this specification, a method for evaluating image anonymization performance is provided, including: determining a first privacy protection evaluation value by using anonymized image data, where the first privacy protection evaluation value is used to measure distinctiveness of original image data relative to the anonymized image data; determining a second privacy protection evaluation value by using reconstructed image data, where the second privacy protection evaluation value is used to measure distinctiveness of the original image data relative to the reconstructed image data, and the reconstructed image data is obtained through reverse reconstruction by using the anonymized image data; separately providing the anonymized image data and the original image data to an image data application model to determine respective image application processing results; determining an image application evaluation value based on respective image application processing results of the anonymized image data and the original image data, where the image application evaluation value is used to measure distinctiveness of the original image data relative to the anonymized image data in terms of image application processing result; and determining an evaluation value of image anonymization performance of the anonymized image data based on the first privacy protection evaluation value, the second privacy protection evaluation value, and the image application evaluation value.

[0005] Optionally, in an example of the above aspect, the determining an evaluation value of image anonymization performance of the anonymized image data based on the first privacy protection evaluation value, the second privacy protection evaluation

value, and the image application evaluation value can include: determining a total privacy protection evaluation value based on the first privacy protection evaluation value and the second privacy protection evaluation value; and determining the evaluation value of image anonymization performance of the anonymized image data based on the total privacy protection evaluation value and the image application evaluation value.

[0006] Optionally, in an example of the above aspect, the determining the evaluation value of image anonymization performance of the anonymized image data based on the total privacy protection evaluation value and the image application evaluation value can include: calculating a product of the total privacy protection evaluation value and the image application evaluation value as the evaluation value of image anonymization performance of the anonymized image data.

[0007] Optionally, in an example of the above aspect, the first privacy protection evaluation value and the second privacy protection evaluation value respectively have weights; and the determining a total privacy protection evaluation value based on the first privacy protection evaluation value and the second privacy protection evaluation value can include: performing weighted summation on the first privacy protection evaluation value and the second privacy protection evaluation value to obtain the total privacy protection evaluation value.

[0008] Optionally, in an example of the above aspect, the weights of the first privacy protection evaluation value and the second privacy protection evaluation value are set based on a privacy protection demand of an application scenario of the anonymized image data.

[0009] Optionally, in an example of the above aspect, the determining a first privacy protection evaluation value by using anonymized image data can include: determining a first visual difference measurement value between the anonymized image data and the original image data; separately providing the anonymized image data and the original image data to a feature extraction model to extract corresponding feature vectors; determining a first feature vector difference measurement value between the anonymized image data and the original image data based on the extracted feature

vectors; and determining the first privacy protection evaluation value based on the first visual difference measurement value and the first feature vector difference measurement value.

[0010] Optionally, in an example of the above aspect, the determining a first privacy protection evaluation value by using anonymized image data further includes: determining a task exclusivity measurement value of the anonymized image data; and correspondingly, the determining the first privacy protection evaluation value based on the first visual difference measurement value and the first feature vector difference measurement value can include: determining the first privacy protection evaluation value based on the first visual difference measurement value, the first feature vector difference measurement value, and the task exclusivity measurement value.

[0011] Optionally, in an example of the above aspect, the determining a second privacy protection evaluation value by using reconstructed image data can include: determining a second visual difference measurement value between the reconstructed image data and the original image data; separately providing the reconstructed image data and the original image data to a feature extraction model to extract corresponding feature vectors; determining a second feature vector difference measurement value between the reconstructed image data and the original image data based on the extracted feature vectors; and determining the second privacy protection evaluation value based on the second visual difference measurement value and the second feature vector difference measurement value.

[0012] Optionally, in an example of the above aspect, the first visual difference measurement value and the second visual difference measurement value each include a visual difference measurement value based on a Learned Perceptual Image Patch Similarity (LPIPS), a Peak Signal-to-Noise Ratio (PSNR), or a Structural Similarity (SSIM).

[0013] According to another aspect of an embodiment of this specification, an apparatus for evaluating image anonymization performance is provided, including: a first privacy protection evaluation unit, configured to determine a first privacy protection evaluation value by using anonymized image data, where the first privacy

protection evaluation value is used to measure privacy protection of original image data relative to the anonymized image data; a second privacy protection evaluation unit, configured to determine a second privacy protection evaluation value by using reconstructed image data, where the second privacy protection evaluation value is used to measure privacy protection of the original image data relative to the reconstructed image data, and the reconstructed image data is obtained through reverse reconstruction by using the anonymized image data; an image application processing unit, configured to separately provide the anonymized image data and the original image data to an image data application model to determine respective image application processing results; an image application result evaluation unit, configured to determine an image application evaluation value based on respective image application processing results of the anonymized image data and the original image data, where the image application evaluation value is used to measure distinctiveness of the original image data relative to the anonymized image data in terms of image application processing result; and an anonymization performance evaluation value determining unit, configured to determine an evaluation value of image anonymization performance of the anonymized image data based on the first privacy protection evaluation value, the second privacy protection evaluation value, and the image application evaluation value.

[0014] Optionally, in an example of the above aspect, the evaluation value determining unit can include: a total privacy protection evaluation value determining module, configured to determine a total privacy protection evaluation value based on the first privacy protection evaluation value and the second privacy protection evaluation value; and an anonymization performance evaluation value determining module, configured to determine the evaluation value of image anonymization performance of the anonymized image data based on the total privacy protection evaluation value and the image application evaluation value.

[0015] Optionally, in an example of the above aspect, the anonymization performance evaluation value determining module is configured to calculate a product of the total privacy protection evaluation value and the image application evaluation

value as the evaluation value of image anonymization performance of the anonymized image data.

[0016] Optionally, in an example of the above aspect, the first privacy protection evaluation value and the second privacy protection evaluation value respectively have weights; and the total privacy protection evaluation value determining module is configured to perform weighted summation on the first privacy protection evaluation value and the second privacy protection evaluation value to obtain the total privacy protection evaluation value.

[0017] Optionally, in an example of the above aspect, the first privacy protection evaluation unit can include: a first visual difference measurement value determining module, configured to determine a first visual difference measurement value between the anonymized image data and the original image data; a first feature vector extraction module, configured to separately provide the anonymized image data and the original image data to a feature extraction model to extract corresponding feature vectors; a first feature vector difference measurement value determining module, configured to determine a first feature vector difference measurement value between the anonymized image data and the original image data based on the extracted feature vectors; and a first privacy protection evaluation value determining module, configured to determine the first privacy protection evaluation value based on the first visual difference measurement value and the first feature vector difference measurement value.

[0018] Optionally, in an example of the above aspect, the first privacy protection evaluation unit can further include: a task exclusivity measurement value determining module, configured to determine a task exclusivity measurement value of the anonymized image data; and the first privacy protection evaluation value determining module is configured to determine the first privacy protection evaluation value based on the first visual difference measurement value, the first feature vector difference measurement value, and the task exclusivity measurement value.

[0019] Optionally, in an example of the above aspect, the second privacy protection evaluation unit can include: a second visual difference measurement value

determining module, configured to determine a second visual difference measurement value between the reconstructed image data and the original image data; a second feature vector extraction module, configured to separately provide the reconstructed image data and the original image data to a feature extraction model to extract
5 corresponding feature vectors; a second feature vector difference measurement value determining module, configured to determine a second feature vector difference measurement value between the reconstructed image data and the original image data based on the extracted feature vectors; and a second privacy protection evaluation value determining module, configured to determine the second privacy protection
10 evaluation value based on the second visual difference measurement value and the second feature vector difference measurement value.

[0020] According to another aspect of an embodiment of this specification, an apparatus for evaluating image anonymization performance is provided, including: at least one processor, a memory coupled to the at least one processor, and a computer
15 program stored in the memory, where the at least one processor executes the computer program to implement the above method for evaluating image anonymization performance.

[0021] According to another aspect of an embodiment of this specification, a computer-readable storage medium that stores executable instructions is provided,
20 where when the instructions are executed, a processor is enabled to perform the above method for evaluating image anonymization performance.

[0022] According to another aspect of an embodiment of this specification, a computer program product is provided, including a computer program, where the computer program is executed by a processor to implement the above method for
25 evaluating image anonymization performance.

BRIEF DESCRIPTION OF DRAWINGS

[0023] The essence and advantages of this specification can be further understood with reference to the following accompanying drawings. In the accompanying

drawings, similar components or features can have the same reference numerals.

[0024] FIG. 1 is a schematic diagram illustrating an example of an application scenario of an apparatus for evaluating image anonymization performance, according to an embodiment of this specification;

5 [0025] FIG. 2 is flowchart illustrating an example of a method for evaluating image anonymization performance, according to an embodiment of this specification;

[0026] FIG. 3 is a flowchart illustrating an example of a first privacy protection evaluation process, according to an embodiment of this specification;

10 [0027] FIG. 4 is a flowchart illustrating an example of a second privacy protection evaluation process, according to an embodiment of this specification;

[0028] FIG. 5 is flowchart illustrating an example of a process of determining an evaluation value of image anonymization performance, according to an embodiment of this specification;

15 [0029] FIG. 6 is a block diagram illustrating an example of an apparatus for evaluating image anonymization performance, according to an embodiment of this specification;

[0030] FIG. 7 is a block diagram illustrating an example of a first privacy protection evaluation unit, according to an embodiment of this specification;

20 [0031] FIG. 8 is a block diagram illustrating an example of a second privacy protection evaluation unit, according to an embodiment of this specification;

[0032] FIG. 9 is a block diagram illustrating an example of an evaluation value determining unit, according to an embodiment of this specification; and

25 [0033] FIG. 10 is a schematic diagram illustrating an example of an apparatus for evaluating image anonymization performance implemented based on a computer system, according to an embodiment of this specification.

DESCRIPTION OF EMBODIMENTS

[0034] The subject matter described in this specification will be discussed with reference to example implementations. It should be understood that these

implementations are merely discussed to enable a person skilled in the art to better understand and implement the subject matter described in this specification, and are not intended to limit the protection scope, applicability, or examples described in the claims. The functions and arrangements of the discussed elements can be changed
5 without departing from the protection scope of the content of this specification. Various processes or components can be omitted, replaced, or added in the examples as needed. For example, the described method can be performed in a different order from the described order, and various steps can be added, omitted, or combined. In addition, features described for some examples can also be combined in other
10 examples.

[0035] As used in this specification, the term "include" and its variant represent open terms, and mean "including but not limited to". The term "based on" means "at least partially based on". The terms "one embodiment" and "an embodiment" represent "at least one embodiment". The term "another embodiment" represents "at least one
15 another embodiment". The terms "first", "second", etc. can represent different or same objects. The following can include other definitions, whether explicit or implicit. Unless the context clearly indicates otherwise, the definition of a term is consistent throughout the specification.

[0036] In a service processing solution based on image data, original image data
20 needs to be provided as input to a third-party device for processing. Due to unpredictable security of a running environment of the third-party device, there is a possibility that the original image data or feature vector data obtained after feature extraction is performed on the original image data is maliciously stolen. To protect data privacy of collected image data, before the original image data is provided to the
25 third-party device, image anonymization processing needs to be performed on the original image data by using an image anonymization processing solution. How to effectively evaluate image anonymization performance of the image anonymization processing solution becomes a problem urgently to be alleviated.

[0037] In view of this, embodiments of this specification provide a method and an
30 apparatus for evaluating image anonymization performance. According to the method

and the apparatus, image anonymization performance is evaluated by comprehensively considering three factors: distinctiveness (anonymization indicator) of original image data relative to anonymized image data, distinctiveness (reverse reconstruction indicator) of the original image data relative to reconstructed image data, and image recognition distinctiveness (image recognition indicator) of the original image data relative to the anonymized image data. This can efficiently and accurately evaluate image anonymization performance of an image anonymization processing solution.

[0038] The following describes the method and the apparatus for evaluating image anonymization performance according to the embodiments of this specification with reference to the accompanying drawings.

[0039] FIG. 1 is a schematic diagram illustrating an example of an application scenario 100 of an apparatus for evaluating image anonymization performance, according to an embodiment of this specification. As shown in FIG. 1, the application scenario 100 can include an image data collection apparatus 110, an image data anonymization processing apparatus 120, an apparatus 130 for evaluating image anonymization performance, an image data application apparatus 140, and a network 150.

[0040] The application scenario 100 can be widely applied to various image data processing scenarios such as a facial recognition-based payment scenario, a facial identity recognition scenario, and an image recognition scenario.

[0041] In a typical application scenario, some or all of the image data collection apparatus 110, the image data anonymization processing apparatus 120, and the apparatus 130 for evaluating image anonymization performance can be deployed on a first local device, and the first local device can include, for example, a local terminal device or a local server device. The image data collection apparatus 110 collects image data to be processed. In some embodiments, the collected image data can include, for example, face data. Examples of the image data collection apparatus 110 can include various types of image collection apparatuses such as a camera lens, a video camera, a camera, an image collector, and another device with a photographing

function. The image data collected by the image data collection apparatus 110 is provided to the image data anonymization processing apparatus 120. The image data anonymization processing apparatus 120 performs image anonymization processing on the image data by using a configured image data anonymization processing solution, and provides anonymized image data to the apparatus 130 for evaluating image anonymization performance. The apparatus 130 for evaluating image anonymization performance evaluates image anonymization performance of the anonymized image data by using the solution for evaluating image anonymization performance according to the embodiments of this specification. In some embodiments, the image data anonymization processing apparatus 120 can directly provide the anonymized image data to the image data application apparatus 140 for subsequent processing, such as image recognition. In some embodiments, only after image anonymization performance evaluated by the apparatus 130 for evaluating image anonymization performance satisfies a predetermined demand, the image data anonymization processing apparatus 120 provides the anonymized image data to the image data application apparatus 140 for subsequent processing.

[0042] The image data application apparatus 140 can be deployed in a second server device. In some embodiments, the second server device can be a local server device or a remote server device. For example, the second server device can be deployed in a same place as the first local device to obtain information and/or data sent by the first local device. For another example, the second server device can remotely receive, by using the network 150, information and/or data sent by the first local device. In some embodiments, the second server device can be implemented on a cloud platform. By way of example only, the cloud platform can include a private cloud, a public cloud, a hybrid cloud, a community cloud, a distributed cloud, an internal cloud, a multi-layer cloud, or any combination thereof.

[0043] The network 150 can facilitate exchange of information and/or data. In some embodiments, one or more components of the application scenario 100 can transmit information to other components of the application scenario 100 by using the network 150. For example, the image data anonymization processing apparatus 120 can send

the anonymized image data to be evaluated to the apparatus 130 for evaluating image anonymization performance by using the network 150, so that the apparatus 130 for evaluating image anonymization performance evaluates image anonymization performance. For another example, the image data anonymization processing apparatus 120 can send the anonymized image data to be recognized to the image data application apparatus 140 by using the network 150, so that the image data application apparatus 140 performs image recognition. For another example, the image data application apparatus 140 can return an image data application processing result (for example, an image application effect) to the first local device.

[0044] In some implementations, the network 150 can be any form of wired or wireless network, or any combination thereof. By way of example only, the network 150 can be one or a combination of a wired network, a fiber optic network, a telecommunication network, an intranet, the Internet, a local area network (LAN), a wide area network (WAN), a wireless local area network (WLAN), a metropolitan area network (MAN), a wide area network (WAN), a public switched telephone network (PSTN), a Bluetooth network, etc.

[0045] The first local device can be configured to process information and/or data associated with image data anonymization to perform one or more functions disclosed in the embodiments of this specification. In some embodiments, the first local device can be any type of device configured to provide image data anonymization services. In some embodiments, the first local device can be configured to obtain image data to be processed that is collected because the image data collection apparatus is triggered. In some embodiments, the first local device can perform anonymization processing on the image data to be processed, to obtain anonymized image data used to represent the image data to be processed. In some embodiments, a trusted execution environment can be deployed on the first local device, and image data collection and image data anonymization processing are performed in the trusted execution environment. In some embodiments, the first local device can include one or more processing engines (for example, a single-core processing engine or a multi-core processor). By way of example only, the processing engine can include one or a combination of a central

processing unit, an application-specific integrated circuit (ASIC), an application-specific instruction set processor (ASIP), a graphics processing unit (GPU), a physics processing unit (PPU), a digital signal processor (DSP), a field programmable gate array (FPGA), a programmable logic device (PLD), a controller, a
5 micro control unit, a reduced instruction set computer (RISC), a microprocessor, etc.

[0046] In some embodiments, the first local device can further be a portable device with a data acquisition, storage, and/or sending function, such as a tablet computer, a notebook computer, a smartphone, a camera lens, or any combination thereof. In some embodiments, the first local device can exchange data with the second server device
10 by using a network. For example, the first local device can transmit, to the second server device for subsequent processing, the anonymized image data obtained after anonymization processing is performed the image data to be processed.

[0047] The application scenario 100 can further include a storage device (not shown). The storage device can store data and/or instructions related to image data processing.

15 In some embodiments, the storage device can store data obtained/acquired by the first local device and/or the second server device. In some embodiments, the storage device can store data and/or instructions used by the first local device to perform or implement the example method described in the embodiments of this specification. In some embodiments, the storage device can include a mass memory, a removable
20 memory, a volatile read-write memory, a read-only memory (ROM), or any combination thereof. For example, the mass memory can include a disk, an optical disc, a solid-state disk, etc. For example, the removable memory can include a flash drive, a floppy disk, an optical disc, a memory card, a compact disc, a magnetic tape, etc. For example, the volatile read-only memory can include a random access memory
25 (RAM). For example, the RAM can include a dynamic RAM (DRAM), a double rate synchronous dynamic RAM (DDRSDRAM), a static RAM (SRAM), a thyristor RAM (T-RAM), a zero-capacitor RAM (Z-RAM), etc. For example, the ROM can include a mask ROM (MROM), a programmable ROM (PROM), an erasable programmable ROM (EPROM), an electrically erasable programmable ROM (EEPROM), a compact
30 disc ROM (CD-ROM), a digital versatile disc ROM, etc. In some embodiments, the

storage device can be implemented on a cloud platform. By way of example only, the cloud platform can include a private cloud, a public cloud, a hybrid cloud, a community cloud, a distributed cloud, an internal cloud, a multi-layer cloud, or any combination thereof.

5 [0048] In some embodiments, the storage device can be connected to the network 150 to communicate with one or more components in the application scenario 100. One or more components in the application scenario 100 can access, by using the network 150, data or instructions stored in the storage device. In some embodiments, the storage device can be directly connected to or communicate with one or more
10 components in the application scenario 100. In some embodiments, the storage device can be a part of the first local device.

[0049] FIG. 2 is flowchart illustrating an example of a method 200 for evaluating image anonymization performance, according to an embodiment of this specification. In some embodiments, the method 200 can be performed by the apparatus 130 for
15 evaluating image anonymization performance. For example, the method 200 can be stored in a storage device (such as a built-in storage unit or an external storage device of the apparatus 130 for evaluating image anonymization performance (or the first local device)) in a form of a program or instructions. When being executed, the program or the instructions can implement the method 200.

20 [0050] As shown in FIG. 2, after receiving anonymized image data from the image data anonymization processing apparatus 120, at step 210, a first privacy protection evaluation value is determined by using the anonymized image data. The first privacy protection evaluation value is used to measure distinctiveness of original image data relative to the anonymized image data. In other words, the first privacy protection
25 evaluation value is used to measure privacy protection of the original image data relative to the anonymized image data.

[0051] In some embodiments, the anonymized image data can be provided to a privacy protection evaluation model to determine the first privacy protection evaluation value. In some embodiments, both the anonymized image data and the
30 original image data can be provided to a privacy protection evaluation model to

determine the first privacy protection evaluation value.

[0052] FIG. 3 is a flowchart illustrating an example of a first privacy protection evaluation process 300, according to an embodiment of this specification.

[0053] As shown in FIG. 3, at step 310, a first visual difference measurement value S1 between the anonymized image data and the original image data is determined. The first visual difference measurement value S1 is configured to measure a visual difference between the anonymized image data and the original image data. If the first visual difference measurement value S1 is larger, it indicates an anonymization effect is better. In some embodiments, the first visual difference measurement value S1 can include a visual difference measurement value based on a Learned Perceptual Image Patch Similarity (LPIPS), a Peak Signal-to-Noise Ratio (PSNR), or a Structural Similarity (SSIM).

[0054] In some embodiments, for a plurality of sample images, each anonymized image data can be provided to a model used to calculate an LPIPS to calculate an LPIPS value between each anonymized image data and the original image data, and then the calculated LPIPS values are averaged to obtain an image quality measurement value m1 of the anonymized image data. The image quality measurement value m1 can reflect a degree of difference between the anonymized image data and the original image data. If the image quality measurement value m1 is small, it indicates that image quality of the anonymized image data is better, and therefore the degree of difference between the anonymized image data and the original image data is low, and an anonymization effect is poor. If the image quality measurement value m1 is large, it indicates that image quality of the anonymized image data is poorer, and therefore the degree of difference between the anonymized image data and the original image data is high, and an anonymization effect is good. Because a range of the LPIPS value is not [0, 1], normalization processing needs to be performed on the obtained image quality measurement value m1 to determine the first visual difference measurement value S1. That is, the first visual difference measurement value S1 is an image quality measurement value that undergoes normalization processing.

[0055] In some embodiments, for a plurality of sample images, each anonymized image data can be provided to a model used to calculate a PSNR or an SSIM to calculate a PSNR value or an SSIM value between each anonymized image data and the original image data, and then the calculated PSNR values or SSIM values are averaged to obtain a similarity measurement value $m2$ between the anonymized image data and the original image data. For the PSNR-based similarity measurement value $m2$, because a range of the PSNR value is not $[0, 1]$, normalization processing further needs to be performed on the similarity measurement value $m2$. For the SSIM-based similarity measurement value $m2$, because a range of the SSIM value is $[0, 1]$, normalization processing does not need to be performed. Finally, the first visual difference measurement value $S1$ is determined based on the similarity measurement value (or the similarity measurement value that undergoes normalization processing) $m2$. For example, the first visual difference measurement value $S1$ is calculated by using the equation $S1 = 1 - m2$. If the similarity measurement value $m2$ is large, it indicates that a similarity between the anonymized image data and the original image data is high, and therefore an anonymization effect is poor. If the similarity measurement value $m2$ is small, it indicates that a similarity between the anonymized image data and the original image data is low, and therefore an anonymization effect is good.

[0056] At step 320, the anonymized image data and the original image data are separately provided to a feature extraction model to extract corresponding feature vectors. The feature extraction model can be, for example, a feature extraction model pre-trained by using the original image data.

[0057] At step 330, a first feature vector difference measurement value $S2$ between the anonymized image data and the original image data is determined based on the extracted feature vectors. The first feature vector difference measurement value $S2$ is used to measure a feature vector difference between the anonymized image data and the original image data. If the first feature vector difference measurement value $S2$ is larger, it indicates that a feature vector similarity between the anonymized image data and the original image data is lower, and therefore an anonymization effect is better.

[0058] For example, for a plurality of sample images, a feature vector similarity between each anonymized image data and the original image data can be determined based on the extracted feature vectors, and the feature vector similarities are averaged to obtain a first feature vector similarity m_3 . Then, the first feature vector difference measurement value S_2 is determined based on the first feature vector similarity m_3 . For example, the first feature vector difference measurement value is calculated by using the equation $S_2 = 1 - m_3$. Examples of a representation of the first feature vector similarity m_3 , for example, can include but are not limited to a Euclidean distance, a cosine similarity, a Manhattan distance, a Hamming distance, a Chebyshev distance, and information entropy.

[0059] At step 340, the first privacy protection evaluation value is determined based on the first visual difference measurement value and the first feature vector difference measurement value. In some embodiments, the first privacy protection evaluation value can be determined by averaging the first visual difference measurement value and the first feature vector difference measurement value, that is, the first privacy protection evaluation value $\text{ScorePP1} = (S_1 + S_2)/2$. In some embodiments, the first privacy protection evaluation value can also be determined based on other equations and the first visual difference measurement value and the first feature vector difference measurement value. For example, weighted averaging is performed on the first visual difference measurement value and the first feature vector difference measurement value to determine the first privacy protection evaluation value.

[0060] In some embodiments, when the first privacy protection evaluation value is determined, task exclusivity of the anonymized image data is also considered, that is, a task exclusivity measurement value of the anonymized image data is determined.

The task exclusivity measurement value is used to indicate that the anonymized image data is applicable only to a current image data application task and is not applicable to some specified image data application tasks. For example, assume that the current image data application task is an expression recognition task, and the specified image data application tasks are, for example, a race recognition task and a gender recognition task. In this case, the task exclusivity measurement value is used to

indicate that the anonymized image data can be applied to expression recognition, and recognition performance for the application task such as race recognition and gender recognition decreases significantly. For example, assume that a current task of the anonymized image data is task A. For task A, precision before anonymization is a_A , and precision after anonymization is a_{mA} . Tasks that require privacy protection (that is, tasks that require exclusivity) are task B and task C. For task B and task C, precision before anonymization is a_B and a_C respectively, and precision after anonymization is a_{mB} and a_{mC} respectively. In this case, a task exclusivity measurement value $S5$ can be determined by using the equation $S5 = a_{mA}/a_A * (a_B - a_{mB})/a_B * (a_C - a_{mC})/a_C$. It should be noted that the determined task exclusivity measurement value $S5$ is a value that undergoes normalization processing. In this case, the first privacy protection evaluation value can be determined based on the first visual difference measurement value, the first feature vector difference measurement value, and the task exclusivity measurement value, that is, $\text{ScorePP1} = (S1 + S2 + S5)/3$.

[0061] At step 220, a second privacy protection evaluation value is reconstructed by using reconstructed image data, where the determined second privacy protection evaluation value is used to measure distinctiveness of the original image data relative to the reconstructed image data. In other words, the second privacy protection evaluation value is used to measure privacy protection of the original image data relative to the reconstructed image data. In some embodiments, the reconstructed image data is obtained through reverse reconstruction by using the anonymized image data. For example, reverse reconstruction tools such as pix2pix and styleGAN can be used to obtain the reconstructed image data through reverse reconstruction based on the anonymized image data.

[0062] The image data reconstruction solution generally includes an image data reconstruction solution based on a white-box attack and an image data reconstruction solution based on a black-box attack. In the image data reconstruction solution based on the white-box attack, all details of the privacy protection method can be known in advance. Therefore, an implementation solution of the image data reconstruction

solution based on the white-box attack can be customized, that is, different privacy protection methods may correspond to different image data reconstruction solutions. To emphasize commonality of evaluation criteria, a generative adversarial network (GAN network) can be used as a basis for image data reconstruction. The anonymized image data is obtained by using a secondary data set and an anonymization algorithm, thereby forming a data pair of the original image data and the anonymized image data. The anonymized image data is used as input, the original image data is used as output, and a strong fitting capability of the GAN network is used to fit a correspondence between these data pairs. In more cases, this image data reconstruction solution is the image data reconstruction solution based on the black-box attack. However, if details of the privacy protection method can be known in advance, the details can also be incorporated as prior information into the image data reconstruction process. When a plurality of different image anonymization processing solutions are measured, the image data reconstruction network GAN needs to be trained based on a unified image data reconstruction network and training set, and then image data reconstruction is performed based on the anonymized image data and the image data reconstruction network GAN.

[0063] In some embodiments, the reconstructed image data can be provided to a privacy protection evaluation model to determine the second privacy protection evaluation value. In some embodiments, both the reconstructed image data and the original image data can be provided to a privacy protection evaluation model to determine the second privacy protection evaluation value.

[0064] FIG. 4 is a flowchart illustrating an example of a second privacy protection evaluation process 400, according to an embodiment of this specification.

[0065] As shown in FIG. 4, at step 410, a second visual difference measurement value S3 between the reconstructed image data and the original image data is determined. The second visual difference measurement value S3 is configured to measure a visual difference between the reconstructed image data and the original image data. If the second visual difference measurement value S3 is larger, it indicates an anonymization effect is better. In some embodiments, the second visual difference

measurement value S3 can include a visual difference measurement value based on an LPIPS, a PSNR, or an SSIM.

[0066] In some embodiments, for a plurality of sample images, each reconstructed image data can be provided to a model used to calculate an LPIPS to calculate an LPIPS value between each reconstructed image data and the original image data, and then the calculated LPIPS values are averaged to obtain an image quality measurement value m4 of the reconstructed image data. The image quality measurement value m4 can reflect a degree of difference between the reconstructed image data and the original image data. If the image quality measurement value m4 is small, it indicates that image quality of the reconstructed image data is better, and therefore the degree of difference between the reconstructed image data and the original image data is low, and an anonymization effect is poor. If the image quality measurement value m4 is large, it indicates that image quality of the reconstructed image data is poorer, and therefore the degree of difference between the reconstructed image data and the original image data is high, and an anonymization effect is good. Because a range of the LPIPS value is not [0, 1], normalization processing needs to be performed on the obtained image quality measurement value m4 to determine the second visual difference measurement value S3. That is, the second visual difference measurement value S3 is an image quality measurement value that undergoes normalization processing.

[0067] In some embodiments, for a plurality of sample images, each reconstructed image data can be provided to a model used to calculate a PSNR or an SSIM to calculate a PSNR value or an SSIM value between each reconstructed image data and the original image data, and then the calculated PSNR values or SSIM values are averaged to obtain a similarity measurement value m5 between the reconstructed image data and the original image data. For the PSNR-based similarity measurement value m5, because a range of the PSNR value is not [0, 1], normalization processing further needs to be performed. For the SSIM-based similarity measurement value m5, because a range of the SSIM value is [0, 1], normalization processing does not need to be performed. Finally, the second visual difference measurement value S3 is

determined based on the similarity measurement value (or the similarity measurement value that undergoes normalization) m_5 . For example, the second visual difference measurement value S_3 is calculated by using the equation $S_3 = 1 - m_5$. If the similarity measurement value m_5 is large, it indicates that a similarity between the reconstructed image data and the original image data is high, and therefore an anonymization effect is poor. If the similarity measurement value m_5 is small, it indicates that a similarity between the reconstructed image data and the original image data is low, and therefore an anonymization effect is good.

[0068] At step 420, the reconstructed image data and the original image data are separately provided to a feature extraction model to extract corresponding feature vectors. The feature extraction model can be, for example, a feature extraction model pre-trained by using the original image data.

[0069] At step 430, a second feature vector difference measurement value S_4 between the reconstructed image data and the original image data is determined based on the extracted feature vectors. The second feature vector difference measurement value S_4 is used to measure a feature vector difference between the reconstructed image data and the original image data. If the second feature vector difference measurement value S_4 is larger, it indicates that a feature vector similarity between the reconstructed image data and the original image data is lower, and therefore an anonymization effect is better.

[0070] For example, for a plurality of sample images, a feature vector similarity between each anonymized image data and the original image data can be determined based on the extracted feature vectors, and the feature vector similarities are averaged to obtain a second feature vector similarity m_6 . Then, the second feature vector difference measurement value S_4 is determined based on the second feature vector similarity m_6 . For example, the second feature vector difference measurement value S_4 is calculated by using the equation $S_4 = 1 - m_6$. Examples of a representation of the second feature vector similarity m_6 , for example, can include but are not limited to a Euclidean distance, a cosine similarity, a Manhattan distance, a Hamming distance, a Chebyshev distance, and information entropy.

[0071] At step 440, the second privacy protection evaluation value is determined based on the second visual difference measurement value and the second feature vector difference measurement value. In some embodiments, the second privacy protection evaluation value can be determined by averaging the second visual difference measurement value and the second feature vector difference measurement value, that is, the second privacy protection evaluation value $\text{ScorePP2} = (\text{S3} + \text{S4})/2$. In some embodiments, the second privacy protection evaluation value can also be determined based on other equations and the second visual difference measurement value and the second feature vector difference measurement value. For example, weighted averaging is performed on the second visual difference measurement value and the second feature vector difference measurement value to determine the second privacy protection evaluation value.

[0072] Back to FIG. 2, at step 230, the anonymized image data and the original image data are separately provided to an image data application model to determine respective image application results. For example, when the image data application model is an image recognition model, the anonymized image data can be provided to the image recognition model to determine an image recognition rate Acc_mask , and the original image data can be provided to the image recognition model to determine an image recognition rate Acc_baseline .

[0073] At step 240, an image application evaluation value ScoreCIs is determined based on respective image application results of the anonymized image data and the original image data, where the determined image application evaluation value is used to measure distinctiveness of the original image data relative to the anonymized image data in terms of image application effect. For example, when the image data application model is an image recognition model, the image application evaluation value ScoreCIs can be determined by using the equation $\text{ScoreCIs} = \text{Acc_mask} / \text{Acc_baseline}$. If the ScoreCIs is larger, it indicates that the anonymized image data still has good image recognition performance, and therefore an anonymization effect is better.

[0074] At step 250, an evaluation value of image anonymization performance of the

anonymized image data is determined based on the first privacy protection evaluation value, the second privacy protection evaluation value, and the image application evaluation value.

[0075] FIG. 5 is flowchart illustrating an example of a process 500 of determining an evaluation value of image anonymization performance, according to an embodiment of this specification.

[0076] As shown in FIG. 5, at step 510, a total privacy protection evaluation value is determined based on the first privacy protection evaluation value and the second privacy protection evaluation value.

[0077] In some embodiments, the first privacy protection evaluation value and the second privacy protection evaluation value can be added to obtain the total privacy protection evaluation value. In some embodiments, the first privacy protection evaluation value and the second privacy protection evaluation value respectively have weights α and β , and weighted summation is performed on the first privacy protection evaluation value and the second privacy protection evaluation value to obtain the total privacy protection evaluation value. Here, a sum of the weights α and β is 1.

[0078] For example, assume that the weight of the first privacy protection evaluation value is α , and the weight of the second privacy protection evaluation value is β . In this case, the total privacy protection evaluation value ScorePP can be calculated based on the following equation:

$$\text{ScorePP} = \alpha * \text{ScoreP1} + \beta * \text{ScoreP2} = (\alpha * (S1 + S2) + \beta * (S3 + S4))/2.$$

[0079] In some embodiments, the weights of the first privacy protection evaluation value and the second privacy protection evaluation value can be set based on a privacy protection demand of an application scenario of the anonymized image data. For example, if the application scenario has a higher demand on an anonymization effect (e.g. the first privacy protection evaluation value) of image anonymization processing, α can be set to be greater than β , for example, α is set to 0.6 and β is set to 0.4.

[0080] At step 520, the evaluation value of image anonymization performance of the anonymized image data is determined based on the total privacy protection evaluation value and the image application evaluation value.

[0081] In some embodiments, a product of the total privacy protection evaluation value and the image application evaluation value can be calculated as the evaluation value of image anonymization performance of the anonymized image data, that is, $\text{Score} = \text{ScorePP} * \text{ScoreCIs}$.

[0082] According to the method for evaluating image anonymization performance, image anonymization performance is evaluated by comprehensively considering three factors: distinctiveness (anonymization indicator) of original image data relative to anonymized image data, distinctiveness (reverse reconstruction indicator) of the original image data relative to reconstructed image data, and image recognition distinctiveness (image recognition indicator) of the original image data relative to the anonymized image data. This can efficiently and accurately evaluate image anonymization performance of an image anonymization processing solution.

[0083] According to the method for evaluating image anonymization performance, quantifiable measurement is performed on the anonymization indicator, the reverse reconstruction indicator, and the image recognition indicator, so that judgement does not merely depend on the human eye, thereby improving accuracy of evaluating image anonymization performance. In addition, when anonymization performance is evaluated, a privacy protection capability and an image application effect indicator of the anonymized image data are integrated together, so that it is convenient to measure performance trade-offs of the image anonymization solution in the two aspects.

[0084] It should be noted that descriptions of the above process are merely used for illustration and description, and constitute no limitation on the application scope of the embodiments of this specification. A person skilled in the art can make various modifications and changes to the processes under the guidance of this specification. However, these modifications and changes still fall within the scope of the embodiments of this specification, for example, changes of steps of a related process in the embodiments of this specification, such as adding a preprocessing step and a

storage step.

[0085] FIG. 6 is a block diagram illustrating an example of an apparatus 600 for evaluating image anonymization performance, according to an embodiment of this specification. As shown in FIG. 6, the apparatus 600 for evaluating image anonymization performance includes a first privacy protection evaluation unit 610, a second privacy protection evaluation unit 620, an image application processing unit 630, an image application effect evaluation unit 640, and an anonymization performance evaluation value determining unit 650.

[0086] The first privacy protection evaluation unit 610 is configured to determine a first privacy protection evaluation value by using anonymized image data, where the determined first privacy protection evaluation value is used to measure distinctiveness of original image data relative to the anonymized image data. For an operation of the first privacy protection evaluation unit 610, references can be made to the operation described above with reference to step 210 in FIG. 2.

[0087] In some embodiments, the first privacy protection evaluation unit 610 can provide the anonymized image data to a privacy protection evaluation model to determine the first privacy protection evaluation value. In some embodiments, the first privacy protection evaluation unit 610 can provide both the anonymized image data and the original image data to a privacy protection evaluation model to determine the first privacy protection evaluation value.

[0088] FIG. 7 is a block diagram illustrating an example of a first privacy protection evaluation unit 700, according to an embodiment of this specification. As shown in FIG. 7, the first privacy protection evaluation unit 700 includes a first visual difference measurement value determining module 710, a first feature vector extraction module 720, a first feature vector difference measurement value determining module 730, and a first privacy protection evaluation value determining module 740.

[0089] The first visual difference measurement value determining module 710 is configured to determine a first visual difference measurement value between the anonymized image data and the original image data. For an operation of the first

visual difference measurement value determining module 710, references can be made to the operation described above with reference to step 310 in FIG. 3.

[0090] The first feature vector extraction module 720 is configured to separately provide the anonymized image data and the original image data to a feature extraction model to extract corresponding feature vectors. For an operation of the first feature vector extraction module 720, references can be made to the operation described above with reference to step 320 in FIG. 3.

[0091] The first feature vector difference measurement value determining module 730 is configured to determine a first feature vector difference measurement value between the anonymized image data and the original image data based on the extracted feature vectors. For an operation of the first feature vector difference measurement value determining module 730, references can be made to the operation described above with reference to step 330 in FIG. 3.

[0092] The first privacy protection evaluation value determining module 740 is configured to determine the first privacy protection evaluation value based on the first visual difference measurement value and the first feature vector difference measurement value. For an operation of the first privacy protection evaluation value determining module 740, references can be made to the operation described above with reference to step 340 in FIG. 3.

[0093] In some embodiments, the first privacy protection evaluation unit 700 can further include a task exclusivity measurement value determining module (not shown). The task exclusivity measurement value determining module is configured to determine a task exclusivity measurement value of the anonymized image data. Correspondingly, the first privacy protection evaluation value determining module 740 determines the first privacy protection evaluation value based on the first visual difference measurement value, the first feature vector difference measurement value, and the task exclusivity measurement value.

[0094] The second privacy protection evaluation unit 620 is configured to determine a second privacy protection evaluation value by using reconstructed image data, where the determined second privacy protection evaluation value is used to measure

distinctiveness of the original image data relative to the reconstructed image data, and the reconstructed image data is obtained through reverse reconstruction by using the anonymized image data. For an operation of the second privacy protection evaluation unit 620, references can be made to the operation described above with reference to step 220 in FIG. 2.

[0095] In some embodiments, the second privacy protection evaluation unit 620 can provide the reconstructed image data to a privacy protection evaluation model to determine the second privacy protection evaluation value. In some embodiments, the second privacy protection evaluation unit 620 can provide both the reconstructed image data and the original image data to a privacy protection evaluation model to determine the second privacy protection evaluation value.

[0096] FIG. 8 is a block diagram illustrating an example of a second privacy protection evaluation unit 800, according to an embodiment of this specification. As shown in FIG. 8, the second privacy protection evaluation unit 800 includes a second visual difference measurement value determining module 810, a second feature vector extraction module 820, a second feature vector difference measurement value determining module 830, and a second privacy protection evaluation value determining module 840.

[0097] The second visual difference measurement value determining module 810 is configured to determine a second visual difference measurement value between the reconstructed image data and the original image data. For an operation of the second visual difference measurement value determining module 810, references can be made to the operation described above with reference to step 410 in FIG. 4.

[0098] The second feature vector extraction module 820 is configured to separately provide the reconstructed image data and the original image data to a feature extraction model to extract corresponding feature vectors. For an operation of the second feature vector extraction module 820, references can be made to the operation described above with reference to step 420 in FIG. 4.

[0099] The second feature vector difference measurement value determining module 830 is configured to determine a second feature vector difference measurement value

between the reconstructed image data and the original image data based on the extracted feature vectors. For an operation of the second feature vector difference measurement value determining module 830, references can be made to the operation described above with reference to step 430 in FIG. 4.

5 **[0100]** The second privacy protection evaluation value determining module 840 is configured to determine the second privacy protection evaluation value based on the second visual difference measurement value and the second feature vector difference measurement value. For an operation of the second privacy protection evaluation value determining module 840, references can be made to the operation described
10 above with reference to step 440 in FIG. 4.

[0101] The image application processing unit 630 is configured to separately provide the anonymized image data and the original image data to an image data application model to determine respective image application processing results. For an operation of the image application processing unit 630, references can be made to the
15 operation described above with reference to step 230 in FIG. 2.

[0102] The image application result evaluation unit 640 is configured to determine an image application evaluation value based on respective image application processing results of the anonymized image data and the original image data, where the determined image application evaluation value is used to measure distinctiveness
20 of the original image data relative to the anonymized image data in terms of image application processing result. For an operation of the image application result evaluation unit 640, references can be made to the operation described above with reference to step 240 in FIG. 2.

[0103] The anonymization performance evaluation value determining unit 650 is
25 configured to determine an evaluation value of image anonymization performance of the anonymized image data based on the first privacy protection evaluation value, the second privacy protection evaluation value, and the image application evaluation value. For an operation of the anonymization performance evaluation value determining unit 650, references can be made to the operation described above with
30 reference to step 250 in FIG. 2.

[0104] FIG. 9 is a block diagram illustrating an example of an evaluation value determining unit 900, according to an embodiment of this specification. As shown in FIG. 9, the evaluation value determining unit 900 includes a total privacy protection evaluation value determining module 910 and an anonymization performance evaluation value determining module 920.

[0105] The total privacy protection evaluation value determining module 910 is configured to determine a total privacy protection evaluation value based on the first privacy protection evaluation value and the second privacy protection evaluation value.

[0106] In some embodiments, the total privacy protection evaluation value determining module 910 can add the first privacy protection evaluation value and the second privacy protection evaluation value to obtain the total privacy protection evaluation value. In some embodiments, the first privacy protection evaluation value and the second privacy protection evaluation value respectively have weights α and β . The total privacy protection evaluation value determining module 910 performs weighted summation on the first privacy protection evaluation value and the second privacy protection evaluation value to obtain the total privacy protection evaluation value. Here, a sum of the weights α and β is 1. In some embodiments, the weights of the first privacy protection evaluation value and the second privacy protection evaluation value can be set based on a privacy protection demand of an application scenario of the anonymized image data.

[0107] The anonymization performance evaluation value determining module 920 is configured to determine the evaluation value of image anonymization performance of the anonymized image data based on the total privacy protection evaluation value and the image application evaluation value. In some embodiments, the anonymization performance evaluation value determining module 920 can calculate a product of the total privacy protection evaluation value and the image application evaluation value as the evaluation value of image anonymization performance of the anonymized image data.

[0108] The method for evaluating image anonymization performance and the

apparatus for evaluating image anonymization performance according to the embodiments of this specification are described above with reference to FIG. 1 to FIG. 9. The above apparatus for evaluating image anonymization performance can be implemented by using hardware, or can be implemented by using software or a combination of hardware and software.

[0109] FIG. 10 is a schematic diagram illustrating an example of an apparatus 1000 for evaluating image anonymization performance implemented based on a computer system, according to an embodiment of this specification. As shown in FIG. 10, the apparatus 1000 for evaluating image anonymization performance can include at least one processor 1010, a memory (for example, a non-volatile memory) 1020, an internal memory 1030, and a communication interface 1040, and the at least one processor 1010, the memory 1020, the internal memory 1030, and the communication interface 1040 are connected together by using a bus 1060. The at least one processor 1010 executes at least one computer-readable instruction (for example, the above element implemented in a form of software) stored or encoded in the memory.

[0110] In an embodiment, computer-executable instructions are stored in the memory, and the computer-executable instructions are executed to cause the at least one processor 1010 to perform the following operations: determining a first privacy protection evaluation value by using anonymized image data, where the first privacy protection evaluation value is used to measure distinctiveness of original image data relative to the anonymized image data; determining a second privacy protection evaluation value by using reconstructed image data, where the second privacy protection evaluation value is used to measure distinctiveness of the original image data relative to the reconstructed image data, and the reconstructed image data is obtained through reverse reconstruction by using the anonymized image data; separately providing the anonymized image data and the original image data to an image data application model to determine respective image application processing results; determining an image application evaluation value based on respective image application processing results of the anonymized image data and the original image data, where the image application evaluation value is used to measure distinctiveness

of the original image data relative to the anonymized image data in terms of image application processing result; and determining an evaluation value of image anonymization performance of the anonymized image data based on the first privacy protection evaluation value, the second privacy protection evaluation value, and the image application evaluation value.

[0111] It should be understood that when the computer-executable instructions stored in the memory are executed, the at least one processor 1010 is enabled to perform the various operations and functions described above with reference to FIG. 1 to FIG. 9 in the embodiments of this specification.

[0112] According to an embodiment, a program product such as a machine-readable medium (for example, a non-transitory machine-readable medium) is provided. The machine-readable medium can have instructions (that is, the elements implemented in a form of software). When the instructions are executed by a machine, the machine is enabled to perform the various operations and functions described above with reference to FIG. 1 to FIG. 9 in the embodiments of this specification. Specifically, a system or an apparatus equipped with a readable storage medium can be provided, and software program code for implementing a function of any one of the embodiments is stored in the readable storage medium, so that a computer or a processor of the system or the apparatus reads and executes the instructions stored in the readable storage medium.

[0113] In this case, the program code read from the readable medium can implement a function of any one of the embodiments. Therefore, the machine readable code and the readable storage medium that stores the machine readable code constitute a part of this application.

[0114] Embodiments of the readable storage medium include a floppy disk, a hard disk, a magnetic disk, an optical disc (such as a compact disc read-only memory (CD-ROM), a compact disc-recordable (CD-R), a compact disc-rewritable (CD-RW), a digital versatile disc-read-only memory (DVD-ROM), a digital versatile disc-random access memory (DVD-RAM), a digital versatile disc-rewritable (DVD-RW), a digital versatile disc-rewritable (DVD-RW)), a magnetic tape, a

non-volatile memory card, and a ROM. Optionally, program code can be downloaded from a server computer or cloud by a communication network.

[0115] According to an embodiment, a computer program product is provided. The computer program product includes a computer program, and when the computer program is executed by a processor, the processor is enabled to perform various operations and functions described above with reference to FIG. 1 to FIG. 9 in the embodiments of this specification.

[0116] It should be understood by a person skilled in the art that various changes and modifications can be made to the embodiments disclosed above without departing from the spirit of this application. Therefore, the protection scope of this application should be defined by the appended claims.

[0117] Not all steps and units in the above processes and system structure diagrams are mandatory, and some steps or units can be ignored as actually needed. A sequence for performing steps is not fixed, and can be determined based on needs. The apparatus structure described in the above embodiments can be a physical structure, or can be a logical structure, that is, some units can be implemented by a same physical entity, or some units can be implemented by a plurality of physical entities, or can be implemented jointly by some components in a plurality of independent devices.

[0118] In the above embodiments, the hardware units or modules can be implemented mechanically or electrically. For example, a hardware unit, module, or processor can include dedicated permanent circuitry or logic (for example, a dedicated processor, an FPGA, or an ASIC) for performing a corresponding operation. The hardware unit or processor can further include programmable logic or circuitry (for example, a general-purpose processor or another programmable processor), and can be temporarily arranged by software to perform a corresponding operation. A specific implementation (a mechanical manner, a dedicated permanent circuitry, or a temporarily arranged circuitry) can be determined based on costs and time considerations.

[0119] Exemplary embodiments are described above in the specific implementations described with reference to the accompanying drawings, but do not represent all

embodiments that can be implemented or fall within the protection scope of the claims. The term "example" used throughout this specification means "used as an example, an instance, or an illustration", and does not mean "preferred" or "advantageous" over other embodiments. For the purpose of providing an understanding of the described technologies, the specific implementations include specific details. However, these technologies can be implemented without these specific details. In some examples, well-known structures and apparatuses are shown in block diagrams to avoid difficulties in understanding the concept of the described embodiments.

[0120] The above descriptions of the content of this application are provided to cause any person of ordinary skill in the art to implement or use the content of this application. For a person of ordinary skill in the art, various modifications made to the content of this application are obvious. In addition, the general principles defined in this application can be applied to other variations without departing from the protection scope of the content of this specification. Therefore, the content of this application is not limited to the examples and designs described in this specification, but is consistent with the widest range of principles and novelty features that are disclosed in this specification.

CLAIMS

What is claimed is:

1. A method for evaluating image anonymization performance, comprising:

determining a first privacy protection evaluation value by using anonymized
5 image data, wherein the first privacy protection evaluation value is used to measure distinctiveness of original image data relative to the anonymized image data;

determining a second privacy protection evaluation value by using reconstructed
image data, wherein the second privacy protection evaluation value is used to measure distinctiveness of the original image data relative to the reconstructed image data, and

10 the reconstructed image data is obtained through reverse reconstruction by using the anonymized image data;

separately providing the anonymized image data and the original image data to
an image data application model to determine respective image application processing
results;

15 determining an image application evaluation value based on respective image application processing results of the anonymized image data and the original image data, wherein the image application evaluation value is used to measure distinctiveness of the original image data relative to the anonymized image data in terms of image application processing result; and

20 determining an evaluation value of image anonymization performance of the anonymized image data based on the first privacy protection evaluation value, the second privacy protection evaluation value, and the image application evaluation value.

2. The method according to claim 1, wherein the determining an evaluation value
25 of image anonymization performance of the anonymized image data based on the first privacy protection evaluation value, the second privacy protection evaluation value, and the image application evaluation value comprises:

determining a total privacy protection evaluation value based on the first privacy protection evaluation value and the second privacy protection evaluation value; and

determining the evaluation value of image anonymization performance of the anonymized image data based on the total privacy protection evaluation value and the image application evaluation value.

3. The method according to claim 2, wherein the determining the evaluation value of image anonymization performance of the anonymized image data based on the total privacy protection evaluation value and the image application evaluation value comprises:

calculating a product of the total privacy protection evaluation value and the image application evaluation value as the evaluation value of image anonymization performance of the anonymized image data.

4. The method according to claim 2, wherein the first privacy protection evaluation value and the second privacy protection evaluation value respectively have weights; and

the determining a total privacy protection evaluation value based on the first privacy protection evaluation value and the second privacy protection evaluation value comprises:

performing weighted summation on the first privacy protection evaluation value and the second privacy protection evaluation value to obtain the total privacy protection evaluation value.

5. The method according to claim 4, wherein the weights of the first privacy protection evaluation value and the second privacy protection evaluation value are set based on a privacy protection demand of an application scenario of the anonymized image data.

6. The method according to claim 1, wherein the determining a first privacy protection evaluation value by using anonymized image data comprises:

determining a first visual difference measurement value between the anonymized image data and the original image data;

separately providing the anonymized image data and the original image data to a feature extraction model to extract corresponding feature vectors;

determining a first feature vector difference measurement value between the

anonymized image data and the original image data based on the extracted feature vectors; and

determining the first privacy protection evaluation value based on the first visual difference measurement value and the first feature vector difference measurement value.

7. The method according to claim 6, wherein the determining a first privacy protection evaluation value by using anonymized image data further comprises:

determining a task exclusivity measurement value of the anonymized image data; and

the determining the first privacy protection evaluation value based on the first visual difference measurement value and the first feature vector difference measurement value comprises:

determining the first privacy protection evaluation value based on the first visual difference measurement value, the first feature vector difference measurement value, and the task exclusivity measurement value.

8. The method according to claim 1, wherein the determining a second privacy protection evaluation value by using reconstructed image data comprises:

determining a second visual difference measurement value between the reconstructed image data and the original image data;

separately providing the reconstructed image data and the original image data to a feature extraction model to extract corresponding feature vectors;

determining a second feature vector difference measurement value between the reconstructed image data and the original image data based on the extracted feature vectors; and

determining the second privacy protection evaluation value based on the second visual difference measurement value and the second feature vector difference measurement value.

9. The method according to claim 6 or 8, wherein the first visual difference measurement value and the second visual difference measurement value each comprise a visual difference measurement value based on a Learned Perceptual Image

Patch Similarity (LPIPS), a Peak Signal-to-Noise Ratio (PSNR), or a Structural Similarity (SSIM).

10. An apparatus for evaluating image anonymization performance, comprising:

a first privacy protection evaluation unit, configured to determine a first privacy protection evaluation value by using anonymized image data, wherein the first privacy protection evaluation value is used to measure distinctiveness of original image data relative to the anonymized image data;

a second privacy protection evaluation unit, configured to determine a second privacy protection evaluation value by using reconstructed image data, wherein the second privacy protection evaluation value is used to measure distinctiveness of the original image data relative to the reconstructed image data, and the reconstructed image data is obtained through reverse reconstruction by using the anonymized image data;

an image application processing unit, configured to separately provide the anonymized image data and the original image data to an image data application model to determine respective image application processing results;

an image application result evaluation unit, configured to determine an image application evaluation value based on respective image application processing results of the anonymized image data and the original image data, wherein the image application evaluation value is used to measure distinctiveness of the original image data relative to the anonymized image data in terms of image application processing result; and

an anonymization performance evaluation value determining unit, configured to determine an evaluation value of image anonymization performance of the anonymized image data based on the first privacy protection evaluation value, the second privacy protection evaluation value, and the image application evaluation value.

11. The apparatus according to claim 10, wherein the evaluation value determining unit comprises:

a total privacy protection evaluation value determining module, configured to

determine a total privacy protection evaluation value based on the first privacy protection evaluation value and the second privacy protection evaluation value; and

an anonymization performance evaluation value determining module, configured to determine the evaluation value of image anonymization performance of the anonymized image data based on the total privacy protection evaluation value and the image application evaluation value.

12. The apparatus according to claim 11, wherein the anonymization performance evaluation value determining module is configured to calculate a product of the total privacy protection evaluation value and the image application evaluation value as the evaluation value of image anonymization performance of the anonymized image data.

13. The apparatus according to claim 11, wherein the first privacy protection evaluation value and the second privacy protection evaluation value respectively have weights, and the total privacy protection evaluation value determining module is configured to perform weighted summation on the first privacy protection evaluation value and the second privacy protection evaluation value to obtain the total privacy protection evaluation value.

14. The apparatus according to claim 10, wherein the first privacy protection evaluation unit comprises:

a first visual difference measurement value determining module, configured to determine a first visual difference measurement value between the anonymized image data and the original image data;

a first feature vector extraction module, configured to separately provide the anonymized image data and the original image data to a feature extraction model to extract corresponding feature vectors;

a first feature vector difference measurement value determining module, configured to determine a first feature vector difference measurement value between the anonymized image data and the original image data based on the extracted feature vectors; and

a first privacy protection evaluation value determining module, configured to

determine the first privacy protection evaluation value based on the first visual difference measurement value and the first feature vector difference measurement value.

15 15. The apparatus according to claim 14, wherein the first privacy protection evaluation unit further comprises:

a task exclusivity measurement value determining module, configured to determine a task exclusivity measurement value of the anonymized image data; and

10 the first privacy protection evaluation value determining module is configured to determine the first privacy protection evaluation value based on the first visual difference measurement value, the first feature vector difference measurement value, and the task exclusivity measurement value.

16. The apparatus according to claim 10, wherein the second privacy protection evaluation unit comprises:

15 a second visual difference measurement value determining module, configured to determine a second visual difference measurement value between the reconstructed image data and the original image data;

a second feature vector extraction module, configured to separately provide the reconstructed image data and the original image data to a feature extraction model to extract corresponding feature vectors;

20 a second feature vector difference measurement value determining module, configured to determine a second feature vector difference measurement value between the reconstructed image data and the original image data based on the extracted feature vectors; and

25 a second privacy protection evaluation value determining module, configured to determine the second privacy protection evaluation value based on the second visual difference measurement value and the second feature vector difference measurement value.

17. An apparatus for evaluating image anonymization performance, comprising:

at least one processor;

30 a memory coupled to the at least one processor, and

a computer program stored in the memory, wherein the at least one processor executes the computer program to implement the method for evaluating image anonymization performance according to any one of claims 1 to 9.

5 18. A computer-readable storage medium that stores executable instructions, wherein when the instructions are executed, a processor is enabled to perform the method for evaluating image anonymization performance according to any one of claims 1 to 9.

10 19. A computer program product, comprising a computer program, wherein the computer program is executed by a processor to implement the method for evaluating image anonymization performance according to any one of claims 1 to 9.