DATA PROCESSING METHOD AND RELATED DEVICE

TECHNICAL FIELD

[0001] This disclosure relates to the field of terminals and media applications, and in particular, to a data processing method and a related device.

BACKGROUND

[0002] The popularization of more convenient image shooting devices such as mobile phones, coupled with the development of various types of simple, efficient, and powerful content editing software (for example, AIGC software), has lowered barriers to media creation and modification for people, enabling publication across various social media platforms. However, modification of media content exacerbates the spread of some misinformation and disinformation, undermining the trustworthiness of media content as a carrier of information. Particularly in light of AI advancements, distinguishing between fabricated fake content and authentic content has become increasingly challenging to naked eyes, making "seeing" no longer necessarily "believing". Therefore, technologies that can enhance our ability to assess a trustworthiness level of content are crucial.

[0003] For example, media content is an image. In existing implementations, to detect whether the media content includes fake content, an AI detection model may be trained on a large quantity of real image sets and fake image sets. The detection model detects whether an input image has a feature similar to that of a fake image, to determine whether the image is trustworthy. However, this type of AI detection model can verify trustworthiness levels of only some specific fake content.

[0004] Therefore, there is an urgent need for a method that can verify a trustworthiness level of media content.

SUMMARY

[0005] According to a first aspect, this application provides a data processing method, where the method includes: determining whether one or more trust indicators of a media asset meet a corresponding metric requirement, to obtain trustworthiness information of the media asset. A user may determine a trustworthiness level of the media asset based on the trustworthiness information. The media asset includes media content. The media asset further includes at least one of metadata

of the media content and a trust record of the media content. The trust indicator is a parameter indicating the trustworthiness level of the media asset.

[0006] In a possible implementation, the method further includes: generating the trustworthiness information of the media asset.

[0007] In a possible implementation, the trustworthiness information may be encapsulated into a trust report.

[0008] In a possible implementation, the one or more trust indicators are determined based on at least one of the media content, the metadata corresponding to the media content, and the trust record corresponding to the media content. For example, the trust indicator may be a feature extracted from the media content, the metadata corresponding to the media content, and the trust record corresponding to the media content, or may be data obtained by performing specific processing on the media content, the metadata corresponding to the media content, and the trust record corresponding to the media content.

[0009] In a possible implementation, the trustworthiness information indicates whether the one or more trust indicators satisfy a metric, and the trust indicator includes a parameter indicating the trustworthiness level of the media asset. For example, the media content is an image, and features such as shooting time, a shooting location, a photographer, a camera lens parameter, and a shooting parameter in the metadata may be selected as trust indicators of the metadata.

[0010] For example, the media content is an image, and an image generation manner, an image editing manner, and the like in the trust record may be selected as trust indicators of the trust record. The image generation manner may include but is not limited to whether the media content is generated through AIGC software, whether the media content is generated through a camera, whether the media content is generated with software assistance, whether the media content is generated through synthetic media, and whether the media content can be used to train a model. The image editing manner may include but is not limited to rotation, resizing, cropping, content editing, and the like.

[0011] For example, the media content is an image, and features such as a person, a scene, an object type, a position relationship between objects, or an image style (for example, color, lighting, or brightness) in the media content may be selected as trust indicators of the media content.

[0012] In a possible implementation, a metric corresponding to the trust indicator is specified in a profile, and first trust configuration information may be obtained, where the first trust configuration information includes a metric that the media asset needs to satisfy.

[0013] In a possible implementation, the one or more trust indicators of the media asset may be determined based on at least one of the media content, the metadata corresponding to the media content, and the trust record corresponding to the media content.

[0014] In a possible implementation, the one or more trust indicators may be encapsulated in a trust credential.

[0015] In a possible implementation, the method further includes: adding, to the trust record, the trustworthiness information obtained by determining whether each trust indicator satisfies the metric.

[0016] Adding the newly generated trustworthiness information to the trust record of the media asset can further enhance trustworthiness of the media asset.

[0017] In a possible implementation, determining whether the one or more trust indicators satisfy the metric includes: determining whether a trust indicator in the metric is included in the one or more trust indicators, or determining whether the one or more trust indicators include a trust indicator in the metric.

[0018] In other words, the metric may also include a trust indicator, and whether the trust indicator of the media asset is included in the metric (that is, whether the metric includes the trust indicator of the media asset) may be determined to determine whether the trust indicator of the media asset satisfies the metric.

[0019] In a possible implementation, the trust record includes a trust manifest; and adding the trustworthiness information to the trust record includes: adding the trustworthiness information to the trust manifest.

[0020] In a possible implementation, the method further includes: adding a hash value and a signature of the trustworthiness information to the trust manifest.

[0021] In a possible implementation, the method further includes: obtaining indication information of the media asset; and adding to the trust record includes: adding, based on the indication information, the trustworthiness information to the trust record corresponding to the media asset indicated by the indication information. When there is a need to process trustworthiness information of a plurality of media assets in batches, indication information of the media assets may be transmitted in the process.

[0022] In a possible implementation, the method further includes: generating, based on the trustworthiness information, a file associated with the media asset.

[0023] In a possible implementation, the first trust configuration information includes one of a plurality of pieces of trust configuration information, and different pieces of trust configuration information indicate metric requirements, of different regions or users, that the media asset needs to satisfy. Different scenarios (for example, regions or users) may correspond to different requirements, and different pieces of trustworthiness information may be generated, so that trustworthiness evaluation requirements of the different scenarios can be met.

[0024] In a possible implementation, the action of obtaining the one or more trust indicators

of the media asset is triggered by capturing the media content through a hardware sensor or generating the media content through generation software.

[0025] For example, an image may be captured through a camera built in a terminal device, or new media content may be generated through media content editing software (for example, AIGC). When obtaining media content, a terminal device further needs to generate a corresponding media asset through a media asset management module, where the media asset may include metadata, a trust record, and the like. In this embodiment of this application, the media asset management module may capture the media content through a hardware sensor or generate the media content through generation software, generate trustworthiness information based on the content in the media asset, and add the trustworthiness information to the media asset.

[0026] In a possible implementation, before obtaining the one or more trust indicators of the media asset, the method further includes: receiving a trustworthiness evaluation request for the media content.

[0027] For example, the user may input the trustworthiness evaluation request for the media content through a trustworthiness evaluation application.

[0028] For example, a client side may input the trustworthiness evaluation request for the media content through an interface of a cloud service for providing a trustworthiness evaluation service.

[0029] In a possible implementation, the media content is at least one of an image, a video, or an audio.

[0030] According to a second aspect, this application provides a data processing method, where the method includes: obtaining a media asset, where the media asset includes media content, and the media asset further includes at least one of metadata of the media content and a trust record of the media content; and determining one or more trust indicators of the media asset, where the one or more trust indicators are used to evaluate a trustworthiness level of the media asset.

[0031] This method enables evaluation of the trustworthiness level of the media asset through extraction of the trust indicator, thereby eliminating the need to directly read the media asset during subsequent evaluation of the trustworthiness level, instead, relying only on information read from the trust indicator to evaluate the trustworthiness level of the media asset.

[0032] In a possible implementation, the one or more trust indicators are encapsulated in a trust credential.

[0033] In a possible implementation, the one or more trust indicators are determined based on at least one of the media content, the metadata corresponding to the media content, and the trust record corresponding to the media content.

[0034] In a possible implementation, one or more trust indicators TM related to the

trustworthiness level of the media asset may be determined based on the metadata of the media content. For example, TM may be generation time of the media content, an author name of the media content, a digital content identifier of the media content, a generation location of the media content, information about a generation device of the media content, a media type (Media Type) of the media content, or a generation manner of the media content. For example, the information about the generation device of the media content may include a model of the device, a parameter of a camera, and the like; and the parameter of the camera may include a focal length, photosensitivity, exposure, and the like of the camera during picture-taking. It should be understood that TM may further include other information, for example, information used to describe the media content such as copyright information. This is not limited in this application.

[0035] In a possible implementation, one or more trust indicators TR related to the trustworthiness level of the media asset may be determined based on the trust record of the media content. For example, generation time of the media content, an author name of the media content, a digital content identifier of the media content, a generation location of the media content, information about a generation device of the media content, a media editing manner, a media type (Media Type) of the media content, or a generation manner of the media content in the trust record may be selected as TR. For example, the information about the generation device of the media content may include a model of the device, a parameter of a camera, and the like; and the parameter of the camera may include a focal length, photosensitivity, exposure, and the like of the camera during picture-taking. It should be understood that TR may further include other information, for example, information used to describe the media content such as copyright information. This is not limited in this application. The media generation manner may include but is not limited to whether the media content is generated through AIGC, whether the media content is generated through a camera, whether the media content is generated with software assistance, whether the media content is generated through synthetic media, and whether the media content can be used to train a model. The media editing manner may include but is not limited to rotation, resizing, cropping, content editing, and the like. TR may further include a media assertion, and the media assertion may include a thumbnail, whether modification is allowed, an operation permission, a use permission, provenance of second media content, and the like.

[0036] In a possible implementation, one or more trust indicators TC related to the trustworthiness level of the media asset may be determined based on the media content. For example, features such as a person, a scene, an object type, a position relationship between objects, and a media style (for example, color, lighting, or brightness) in the media content may be selected as trust indicators of the media content.

[0037] In a possible implementation, the one or more trust indicators are used to determine

trustworthiness information of the media asset, and the trustworthiness information indicates whether the one or more trust indicators satisfy a metric.

[0038] In a possible implementation, the metric includes data indicating a trust indicator that the media asset needs to satisfy. For example, the metric indicates a creator, and the metric may be the creator or a name of the creator. For example, the metric indicates a media generation location, and the metric may be the location or a name of the location. Examples are not enumerated herein.

[0039] In a possible implementation, the trust indicator includes a parameter indicating the trustworthiness level of the media asset.

[0040] In a possible implementation, the media content is at least one of an image, a video, or an audio.

[0041] According to a third aspect, this application provides a data processing method, where the method includes: obtaining first media content; and generating a modification record of the first media content, where a trust record of the first media content includes initial information of the first media content, a hard binding of the first media content, and a first digital signature; the first digital signature is a digital signature of first data; and the first data is data determined based on at least the initial information and the hard binding of the first media content. The trust record may be used for tracing provenance of the media content, and can help a user determine authenticity of the media content to some extent.

[0042] In a possible implementation, the first data is data obtained by combining at least the hard binding of the first media content and the initial information of the first media content, or the first data is data obtained by combining at least a hard binding of the initial information (for example, a hash value AIGC.Hash of AIGC, or a hash value Media Type.Hash of a media generation manner) and a hard binding of a first media hard binding (for example, a hash value Media Hash 0.Hash of a first media hash value).

[0043] In a possible implementation, the first data may alternatively be a first combined hash value (Hash(TD)), and the first combined hash value includes a hash value obtained by combining the initial information of the first media content and a first media hash value. For example, the first combined hash value includes a hash value obtained by combining the initial information of the first media content, the first media hash value, and other descriptive information; and the other descriptive information may not be other descriptive information in the initial information, for example, information about a tool for generating a trust profile or other information describing the initial information of the first media content.

[0044] In a possible implementation, the first data may alternatively be a first combined hash value, and the first combined hash value may include a hash value obtained by combining a hash value of the initial information of the first media content and a hash value (Media Hash 0. Hash)

of a first media hash value. For example, the first combined hash value is a hash value obtained by combining the hash value of the initial information of the first media content, the hash value of the first media hash value, and a hash value of other metadata information. Herein, when there are at least two pieces of initial information of the first media content, the hash value of the initial information of the first media content may include a hash value of each piece of initial information of the first media content, or the hash value of the initial information of the first media content may include a hash value obtained by combining all the pieces of initial information of the first media content.

[0045] In a possible implementation, the initial information of the media content may be information generated when the media content is generated. For example, the initial information of the media content includes at least one of the following: generation time of the media content, an author name of the media content, a digital content identifier of the media content, a generation location of the media content, information about a generation device of the media content, a resolution of the media content, a size of the media content, a media type (Media Type) of the media content, or a generation manner of the media content. For example, the information about the generation device of the media content may include a model of the device, a parameter of a camera, and the like; and the parameter of the camera may include a focal length, photosensitivity, exposure, and the like of the camera during picture-taking. It should be understood that the initial information of the media content may further include other information, for example, information used to describe the media content such as copyright information.

[0046] In a possible implementation, the media type may include but is not limited to an image type, a video type, an audio type, a graphics type, and the like. The generation manner may include an AI generation manner, a non-AI generation manner, and the like. In a possible manner, the generation manner in the initial information may be replaced with an AI generation (AIGC) identifier. For example, when the media content is generated by AI, a value of the AIGC identifier is 1; or when the media content is not generated by AI, a value of the AIGC identifier is 0. The author name of the media content may be a name of a creator of the media content or a name of a shooting device of the media content.

[0047] According to a fourth aspect, this application provides a data processing apparatus, where the apparatus includes:

an obtaining module, configured to obtain one or more trust indicators of a media asset, where the media asset includes media content, and at least one of metadata corresponding to the media content and a trust record corresponding to the media content; and

a processing module, configured to determine whether the one or more trust indicators satisfy a metric.

[0048] In a possible implementation, the obtaining module is further configured to:

obtain first trust configuration information, where the first trust configuration information includes a metric that the media asset needs to satisfy.

[0049] In a possible implementation, the one or more trust indicators are determined based on at least one of the media content, the metadata corresponding to the media content, and the trust record corresponding to the media content.

[0050] In a possible implementation, the one or more trust indicators are encapsulated in a trust credential.

[0051] In a possible implementation, the metric includes data indicating a trust indicator that the media asset needs to satisfy.

[0052] In a possible implementation, the processing module is specifically configured to:

determine whether a corresponding trust indicator in the metric is included in the one or more trust indicators, or determining whether the one or more trust indicators include a corresponding trust indicator in the metric.

[0053] In a possible implementation, the processing module is further configured to:

generate trustworthiness information of the media asset, where the trustworthiness information indicates whether the one or more trust indicators satisfy the metric, and the trust indicator includes a parameter indicating a trustworthiness level of the media asset. In a possible implementation, the processing module is further configured to:

add the trustworthiness information to the trust record.

[0054] In a possible implementation, the trust record includes a trust manifest; and

the processing module is specifically configured to:

add the trustworthiness information to the trust manifest.

[0055] In a possible implementation, the obtaining module is further configured to:

obtain indication information of the media asset; and

the processing module is specifically configured to:

add, based on the indication information, the trustworthiness information to the trust record corresponding to the media asset indicated by the indication information.

[0056] In a possible implementation, the trustworthiness information is encapsulated in a trust report.

[0057] In a possible implementation, the processing module is further configured to:

generate, based on the trustworthiness information, a file associated with the media asset.

[0058] In a possible implementation, the first trust configuration information includes one of a plurality of pieces of trust configuration information, and different pieces of trust configuration

information indicate metric requirements, of different regions or users, that the media asset needs to satisfy.

[0059] In a possible implementation, the action of obtaining the one or more trust indicators of the media asset is triggered by capturing the media content through a hardware sensor or generating the media content through generation software.

[0060] In a possible implementation, before obtaining a plurality of metrics and a profile of the media asset, the obtaining module is further configured to:

receive a trustworthiness evaluation request for the media content.

[0061] In a possible implementation, the media content is at least one of an image, a video, or an audio.

[0062] According to a fifth aspect, this application provides a data processing apparatus, where the apparatus includes:

an obtaining module, configured to obtain a media asset, where the media asset includes media content, and at least one of metadata corresponding to the media content and a trust record corresponding to the media content; and

a processing module, configured to determine one or more trust indicators of the media asset, where the one or more trust indicators are used to evaluate a trustworthiness level of the media asset.

[0063] In a possible implementation, the one or more trust indicators are encapsulated in a trust credential.

[0064] In a possible implementation, the one or more trust indicators are determined based on at least one of the media content, the metadata corresponding to the media content, and the trust record corresponding to the media content.

[0065] In a possible implementation, the one or more trust indicators are used to determine trustworthiness information of the media asset, and the trustworthiness information indicates whether the one or more trust indicators satisfy a metric.

[0066] In a possible implementation, the metric includes data indicating a trust indicator that the media asset needs to satisfy.

[0067] In a possible implementation, the trust indicator includes a parameter indicating the trustworthiness level of the media asset.

[0068] In a possible implementation, the media content is at least one of an image, a video, or an audio.

[0069] According to a sixth aspect, an embodiment of this application provides a data processing apparatus, where the apparatus includes:

an obtaining module, configured to obtain first media content; and

a processing module, configured to generate a modification record of the first media content, where a trust record of the first media content includes initial information of the first media content, a hard binding of the first media content, and a first digital signature; the first digital signature is a digital signature of first data; and the first data is data determined based on at least the initial information and the hard binding of the first media content.

[0070] According to a seventh aspect, an embodiment of this application provides a data processing system, including:

a first device, configured to obtain a media asset;

a second device, configured to obtain one or more trust indicators of the media asset based on the media asset, where the first device and the second device may be same or different devices; and

a third device, configured to generate a trust report based on the one or more trust indicators of the media asset that are obtained and trust configuration information. In a possible implementation, the one or more trust indicators of the media asset are recorded in a trust credential. In a possible implementation, the second device sends the one or more trust indicators of the media asset to the third device in response to a request from the third device. The trust configuration information may be recorded in a trust profile. In a possible implementation, the third device may obtain the trust profile from a trust profile repository. In a possible implementation, the third device may directly read the trust profile in a local memory.

[0071] According to an eighth aspect, an embodiment of this application provides a data processing apparatus, where the apparatus may include a memory, a processor, and a bus system, the memory is configured to store a program, and the processor is configured to execute the program in the memory, to perform the method according to the first aspect and any one of the optional implementations of the first aspect, the method according to the second aspect and any one of the optional implementations of the second aspect, and the method according to the third aspect and any one of the optional implementations of the third aspect.

[0072] According to a ninth aspect, an embodiment of this application provides a computer-readable storage medium, where the computer-readable storage medium stores a computer program, and when the computer program is run on a computer, the computer is enabled to perform the method according to the first aspect and any one of the optional implementations of the first aspect, the method according to the second aspect and any one of the optional implementations of the second aspect, and the method according to the third aspect and any one of the optional implementations of the third aspect.

[0073] According to a tenth aspect, an embodiment of this application provides a computer program product including instructions, where when the instructions are run on a computer, the

computer is enabled to perform the method according to the first aspect and any one of the optional implementations of the first aspect, the method according to the second aspect and any one of the optional implementations of the second aspect, and the method according to the third aspect and any one of the optional implementations of the third aspect.

[0074] According to an eleventh aspect, this application provides a chip system, where the chip system includes a processor, configured to support a data processing apparatus to implement a part or all of functions in the foregoing aspects, for example, sending or processing data or information in the foregoing methods. In a possible design, the chip system further includes a memory, configured to store program instructions and data that are necessary for a data processing apparatus. The chip system may include a chip, or may include a chip and another discrete component.

BRIEF DESCRIPTION OF DRAWINGS

[0075] FIG. 1(1) and FIG. 1(2) show an application scenario;

[0076] FIG. 2 shows a structure of a terminal device;

[0077] FIG. 3 shows a structure of a server;

[0078] FIG. 4 shows a cloud service;

[0079] FIG. 5 shows an application architecture;

[0080] FIG. 6A shows a framework of a trust record;

[0081] FIG. 6B shows a procedure of a data processing method;

[0082] FIG. 7 shows generation of trustworthiness information;

[0083] FIG. 8 shows generation of trustworthiness information;

[0084] FIG. 9 shows a procedure of a data processing method;

[0085] FIG. 10 shows a procedure of a data processing method;

[0086] FIG. 11A and FIG. 11B show a procedure of a data processing method;

[0087] FIG. 12A and FIG. 12B show a procedure of a data processing method;

[0088] FIG. 13 shows a procedure of a data processing method;

[0089] FIG. 14 shows a procedure of a data processing method;

[0090] FIG. 15 shows a procedure of a data processing method;

[0091] FIG. 16A-1 and FIG. 16A-2 show a procedure of a data processing method;

[0092] FIG. 16B shows a procedure of a data processing method;

[0093] FIG. 16C shows a procedure of a data processing method;

[0094] FIG. 17 shows a structure of a data processing apparatus;

[0095] FIG. 18 shows a structure of a data processing apparatus; and

[0096] FIG. 19 shows a structure of a server.

DESCRIPTION OF EMBODIMENTS

[0097] The following describes embodiments of the present invention with reference to the accompanying drawings in embodiments of the present invention. Terms used in embodiments of the present invention are merely intended to explain specific embodiments of the present invention, and are not intended to limit the present invention.

[0098] The following describes embodiments of this application with reference to the accompanying drawings. A person of ordinary skill in the art may learn that, with the development of technologies and emergence of a new scenario, the technical solutions provided in embodiments of this application are also applicable to a similar technical problem.

[0099] In the specification, claims, and the accompanying drawings of this application, the terms "first", "second", and the like are intended to differentiate similar objects but do not necessarily indicate a specific order or sequence. It should be understood that the terms used in such a way are interchangeable in proper circumstances, and this is merely a discrimination manner for describing objects having a same attribute in embodiments of this application. In addition, the terms "include", "have", and any other variants thereof are intended to cover non-exclusive inclusion, so that a process, method, system, product, or device that includes a series of units is not necessarily limited to those units, but may include other units that are not expressly listed or are inherent to such a process, method, product, or device.

[00100] The terms "substantially (substantially)", "about (about)", and similar expressions used in this specification are intended as approximate terms rather than terms of degree, and are intended to take into account inherent deviations in measured values or computed values that are known to a person of ordinary skill in the art. In addition, "may (may)" used to describe embodiments of the present invention means "one or more possible embodiments". The terms "use (use)", "using (using)", and "used (used)" used in this specification may be considered to be synonymous with the terms "utilize (utilize)", "utilizing (utilizing)", and "utilized (utilized)" respectively. In addition, the term "example (exemplary)" is intended to refer to an example or illustration.

[00101] An application scenario of this application is first described.

[00102] This application may provide, to a user, trustworthiness information (or may be referred to as a trust report) that is used as a basis for determining a trustworthiness level of a media asset.

[00103] In a scenario, embodiments of this application may be applied to an application that provides trustworthiness information of a media asset.

[00104] In a scenario, embodiments of this application may be applied to a cloud service that provides trustworthiness information of a media asset.

[00105] In a scenario, embodiments of this application may be applied to a media asset management module. The module may generate trustworthiness information of a media asset, and update a trust record in the media asset using the trustworthiness information or generate, based on the trustworthiness information, a file associated with the media asset, to help the user determine a trustworthiness level of the media asset.

[00106] This application may provide, to the user, a trust indicator (or may be referred to as a trust credential) that is used as a basis for determining a trustworthiness level of a media asset.

[00107] In a scenario, embodiments of this application may be applied to an application that provides a trust credential.

[00108] In a scenario, embodiments of this application may be applied to a cloud service that provides a trust credential.

[00109] In a scenario, embodiments of this application may be applied to a media asset management module. The module may generate a trust credential of a media asset, and update a trust record in the media asset using the trust credential or generate, based on the trust credential, a file associated with the media asset, to help the user determine a trustworthiness level of the media asset.

[00110] The following separately describes the foregoing application scenarios.

[00111] Scenario 1: Application

[00112] In a scenario, embodiments of this application are in the form of application for providing trustworthiness information or a trust credential of a media asset (which may be briefly referred to as trustworthiness determining application in embodiments of this application).

[00113] A product form of embodiments of this application may be a trustworthiness determining application. The trustworthiness determining application may be run on a terminal device or a cloud-side server.

[00114] In a possible implementation, the trustworthiness determining application may present trustworthiness information or a trust credential of a media asset to a user in response to input of media content or indication information of the media asset.

[00115] FIG. 1(1) and FIG. 1(2) are a diagram of an example of an application scenario.

[00116] When a user needs to determine a trustworthiness level of media content, the user may start a client (for example, an application, an applet, or a web page) of a media trustworthiness platform on a terminal device to perform query.

[00117] For example, after a mobile phone A of a user A receives media content sent by a mobile phone B of a user B, if the user A needs to use (for example, forward) the media content, the user

A may first determine a trustworthiness level of the media content. After determining the trustworthiness level of the media content, the user A determines whether to use the media content.

[00118] It should be understood that the mobile phone A may alternatively be another electronic device with a strong computing capability, for example, a personal computer, a computer workstation, or a tablet computer. This is not limited in this application.

[00119] For example, when the user needs to determine a trustworthiness level of media content on a smartwatch, the user may send the media content on the smartwatch to a mobile phone, and the mobile phone determines the trustworthiness level of the media content and then sends trustworthiness information to the smartwatch.

[00120] It should be understood that the smartwatch may alternatively be another electronic device with a weak computing capability, for example, a media consumption device, a wearable device, a set-top box, or a game console. This is not limited in this application. The mobile phone may alternatively be another electronic device with a strong computing capability, for example, a personal computer, a computer workstation, or a tablet computer. This is not limited in this application.

[00121] With reference to FIG. 1(1), a main interface 101 of the media trustworthiness platform may include one or more controls, including but not limited to an input box, a trustworthiness level determining button, and the like. This is not limited in this application.

[00122] For example, the user may tap the input box, and the media trustworthiness platform may display a file selection interface in response to the operation behavior of the user. Then, after selecting corresponding media content on the file selection interface, the user may tap a trustworthiness information generation button on the main interface 101. Correspondingly, the media trustworthiness platform may obtain trustworthiness information of a media asset in response to the operation behavior of the user.

[00123] For example, the media trustworthiness platform may display the trustworthiness information. For example, in this embodiment of this application, the trustworthiness information may include whether at least one trust indicator that is of the media asset and that is for the media content satisfies a metric requirement in a predefined profile.

[00124] With reference to FIG. 1(2), a displayed verification result in FIG. 1(2) includes satisfaction of trust indicators T1, T3, T4, and Tn of the media content against metric requirements specified in the predefined profile, for example, the trust indicator T1 satisfies the metric requirement, the trust indicator T2 satisfies the metric requirement, the trust indicator T3 does not satisfy the metric requirement, and the trust indicator T4 satisfies the metric requirement.

[00125] In a possible manner, the client of the media trustworthiness platform may identify the trustworthiness information of the media asset. For example, when there is one to-be-identified

media asset, the client of the media trustworthiness platform may locally perform identification.

[00126] In a possible manner, a server of the media trustworthiness platform may identify the trustworthiness information of the media asset. For example, when there are a plurality of to-be-identified media assets, the client of the media trustworthiness platform may send the plurality of to-be-identified media assets to the server of the media trustworthiness platform, and the server of the media trustworthiness platform identifies trustworthiness information of the media assets, and returns the identified trustworthiness information to the client of the media trustworthiness platform.

[00127] It should be noted that, in this application, whether the client of the media trustworthiness platform identifies the trustworthiness information of the media asset or the server of the media trustworthiness platform identifies the trustworthiness information of the media asset is not limited by a quantity of pieces of to-be-identified media content.

[00128] It should be understood that the description of the scenario corresponding to FIG. 1(1) and FIG. 1(2) is also applicable to generation of a trust credential, and similarities are not described herein again.

[00129] The following describes a product form that a terminal 100 takes when the media trustworthiness platform is on a terminal side.

[00130] The terminal 100 in embodiments of this application may be a mobile phone, a tablet computer, a wearable device, a vehicle-mounted device, an augmented reality (augmented reality, AR)/virtual reality (virtual reality, VR) device, a notebook computer, an ultra-mobile personal computer (ultra-mobile personal computer, UMPC), a netbook, a personal digital assistant (personal digital assistant, PDA), or the like. This is not limited in embodiments of this application.

[00131] FIG. 2 is a diagram of an optional hardware structure of the terminal 100.

[00132] As shown in FIG. 2, the terminal 100 may include components such as a radio frequency unit 110, a memory 120, an input unit 130, a display unit 140, a camera 150 (optional), an audio circuit 160 (optional), a speaker 161 (optional), a microphone 162 (optional), a processor 170, an external interface 180, and a power supply 190. A person skilled in the art may understand that FIG. 2 is merely an example of the terminal or a multi-functional device and does not constitute a limitation on the terminal or the multi-functional device. The terminal or the multi-functional device may include more or fewer components than those shown in the figure, or combine some components, or include different components.

[00133] The input unit 130 may be configured to: receive input digital or character information, and generate a button signal input related to a user setting and function control of the terminal 100. Specifically, the input unit 130 may include a touchscreen 131 (optional) and/or another input device 132. The touchscreen 131 may collect a touch operation performed by a user on or near the

touchscreen 131 (for example, an operation performed by the user on or near the touchscreen by using any proper object such as a finger, a joint, or a stylus), and drive a corresponding connection apparatus based on a preset program. The touchscreen may detect a touch operation performed by the user on the touchscreen, convert the touch operation into a touch signal, and send the touch signal to the processor 170, and can receive and execute a command sent by the processor 170. The touch signal includes at least touch point coordinate information. The touchscreen 131 may provide an input interface and an output interface between the terminal 100 and the user. In addition, the touchscreen may be implemented in a plurality of types, such as a resistive type, a capacitive type, an infrared ray type, and a surface acoustic wave type. In addition to the touchscreen 131, the input unit 130 may include another input device. Specifically, the another input device 132 may include but is not limited to one or more of the following: a physical keyboard, a functional button (such as a volume control button or an on/off button), a trackball, a mouse, a joystick, and the like.

[00134] The input device 132 may receive a media asset designated for trustworthiness level determining.

[00135] The display unit 140 may be configured to display information input by the user or information provided to the user, various menus of the terminal 100, an interaction interface, a file, and/or play any multimedia file. In embodiments of this application, the display unit 140 may be configured to display trustworthiness information (for example, a trust report), and the like.

[00136] The memory 120 may be configured to store instructions and data. The memory 120 may mainly include an instruction storage area and a data storage area. The data storage area may store various types of data such as a multimedia file and a text. The instruction storage area may store software units such as an operating system, an application, and instructions required for at least one function, a subset thereof, or an extended set thereof. The memory 120 may further include a non-volatile random access memory, and provide support to the processor 170 in managing hardware, software, and data resources in a computing processing device, to support control on software and an application. The memory 120 is further configured to: store a multimedia file, and run a program and store an application.

[00137] The processor 170 is a control center of the terminal 100, connects parts of the entire terminal 100 through various interfaces and lines, and executes various functions of the terminal 100 and processes data by running or executing the instructions stored in the memory 120 and invoking the data stored in the memory 120, to perform overall control on the terminal device. Optionally, the processor 170 may include one or more processing units. For example, an application processor and a modem processor may be integrated into the processor 170. The application processor mainly processes an operating system, a user interface, an application, and

the like. The modem processor mainly processes wireless communication. It may be understood that the modem processor may not be integrated into the processor 170. In some embodiments, the processor and the memory may be implemented on a single chip. In some embodiments, the processor and the memory may alternatively be implemented on independent chips. The processor 170 may be further configured to: generate a corresponding operation control signal, send the operation control signal to a corresponding component in the computing processing device, and read and process data in software, especially the data and the program in the memory 120, to cause functional modules in the processor 170 to perform corresponding functions and therefore control corresponding components to perform operations as required by instructions.

[00138] The memory 120 may be configured to store software code related to the data processing method. The processor 170 may perform steps of the data processing method of a chip, or may schedule another unit (for example, the input unit 130 and the display unit 140) to implement a corresponding function.

[00139] The radio frequency unit 110 (optional) may be configured to receive and send signals during information receiving and sending or during a call. For example, after receiving downlink information of a base station, the radio frequency unit 110 sends the downlink information to the processor 170 for processing. In addition, the radio frequency unit 110 sends related uplink data to the base station. Usually, an RF circuit includes but is not limited to an antenna, at least one amplifier, a transceiver, a coupler, a low noise amplifier (Low Noise Amplifier, LNA), a duplexer, and the like. In addition, the radio frequency unit 110 may further communicate with a network device and another device through wireless communication. The wireless communication may use any communication standard or protocol, including but not limited to global system for mobile communications (Global System for Mobile communications, GSM), general packet radio service (General Packet Radio Service, GPRS), code division multiple access (Code Division Multiple Access, CDMA), wideband code division multiple access (Wideband Code Division Multiple Access, WCDMA), long term evolution (Long Term Evolution, LTE), an email, a short messaging service (Short Messaging Service, SMS), and the like.

[00140] In embodiments of this application, the radio frequency unit 110 may send media content to a server 200, and receive trustworthiness information sent by the server 200.

[00141] It should be understood that the radio frequency unit 110 is optional, and may be replaced with another communication interface, for example, a network interface.

[00142] The terminal 100 further includes the power supply 190 (for example, a battery) that supplies power to each component. For example, the power supply may be logically connected to the processor 170 through a power management system, to implement functions such as charging management, discharging management, and power consumption management through the power

management system.

[00143] The terminal 100 further includes the external interface 180. The external interface may be a standard micro USB interface or a multi-pin connector, and may be configured to connect the terminal 100 to another apparatus for communication or may be configured to connect to a charger to charge the terminal 100.

[00144] Although not shown, the terminal 100 may further include a flash, a wireless fidelity (wireless fidelity, Wi-Fi) module, a Bluetooth module, sensors with different functions, and the like. Details are not described herein. A part or all of the methods described below may be applied to the terminal 100 shown in FIG. 2.

[00145] The following describes a product form that the server 200 takes when the media trustworthiness platform is on a server side.

[00146] FIG. 3 is a diagram of a structure of the server 200. As shown in FIG. 3, the server 200 includes a bus 201, a processor 202, a communication interface 203, and a memory 204. The processor 202, the memory 204, and the communication interface 203 communicate with each other through the bus 201.

[00147] The bus 201 may be a peripheral component interconnect (peripheral component interconnect, PCI) bus, an extended industry standard architecture (extended industry standard architecture, EISA) bus, or the like. Buses may be classified into an address bus, a data bus, a control bus, and the like. For ease of representation, only one thick line is used to represent the bus in FIG. 3, but this does not mean that there is only one bus or only one type of bus.

[00148] The processor 202 may be any one or more of processors such as a central processing unit (central processing unit, CPU), a graphics processing unit (graphics processing unit, GPU), a microprocessor (microprocessor, MP), or a digital signal processor (digital signal processor, DSP).

[00149] The memory 204 may include a volatile memory (volatile memory), for example, a random access memory (random access memory, RAM). The memory 204 may further include a non-volatile memory (non-volatile memory), for example, a read-only memory (read-only memory, ROM), a flash memory, a hard disk drive (hard diskdrive, HDD), or a solid-state drive (solid-state drive, SSD).

[00150] The memory 204 may be configured to store software code related to a data processing method. The processor 202 may perform steps of a data processing method of a chip, or may schedule another unit to implement a corresponding function.

[00151] It should be understood that the terminal 100 and the server 200 may be centralized or distributed devices. Processors (for example, the processor 170 and the processor 202) in the terminal 100 and the server 200 may be a hardware circuit (for example, an application-specific integrated circuit (application-specific integrated circuit, ASIC), a field-programmable gate array

(field-programmable gate array, FPGA), a general-purpose processor, a digital signal processor (digital signal processor, DSP), a microprocessor, or a microcontroller), or a combination of these hardware circuits. For example, the processor may be a hardware system that has an instruction execution function, for example, a CPU or a DSP, may be a hardware system that does not have an instruction execution function, for example, an ASIC or an FPGA, or may be a combination of the hardware system that does not have an instruction execution function and the hardware system that has an instruction execution function.

[00152] Scenario 2: Cloud service

[00153] In a scenario, embodiments of this application are in the form of cloud service for providing trustworthiness information or a trust credential of a media asset.

[00154] In a possible implementation, a server may provide, to a client side through an application programming interface (application programming interface, API), a service of querying trustworthiness information or a trust credential of a media asset.

[00155] A terminal may send a related parameter (for example, data such as a media asset) to the server through an API provided by a cloud. The server may obtain a processing result (for example, trustworthiness information or a trust credential) based on the received parameter, and return the processing result to the terminal.

[00156] For descriptions of the terminal and the server, refer to the descriptions in the foregoing embodiments. Details are not described herein again.

[00157] FIG. 4 shows a procedure of using a trustworthiness level determining function–type cloud service provided by a cloud platform.

[00158] 1. Activate and purchase a content audit service.

[00159] 2. A user may download a software development kit (software development kit, SDK) corresponding to the content audit service. Usually, the cloud platform provides SDKs of a plurality of development versions for the user to select based on a development environment requirement, for example, a Java-version SDK, a Python-version SDK, a PHP-version SDK, and an Android-version SDK.

[00160] 3. The user downloads an SDK of a corresponding version to a local computer as required, imports an SDK project to a local development environment, and configures and debugs the SDK project in the local development environment, where the local development environment also supports development of another function. As a result, an application that integrates a trustworthiness level determining capability is formed.

[00161] 4. During use of the trustworthiness level determining application, when there is a need to perform a trustworthiness level determining function, an API call for the trustworthiness level determining function may be triggered. When the application triggers the trustworthiness level

determining function, an API request is initiated to a running instance of a trustworthiness level determining service in a cloud environment, where the API request carries media content. The running instance in the cloud environment processes the media content, to obtain trustworthiness information.

[00162] 5. The cloud environment returns the trustworthiness information to the application, thereby completing a single invocation of the trustworthiness level determining function.

[00163] Scenario 3: Media asset management module

[00164] In this scenario, a terminal device may capture or generate media content. For example, the terminal device may capture an image through a camera built in the terminal device, or generate new media content through media content editing software (for example, AIGC).

[00165] When obtaining the media content, the terminal device further needs to generate a corresponding media asset through a media asset management module, where the media asset may include metadata, a trust record, and the like.

[00166] In this scenario, the media asset management module may generate trustworthiness information based on the content in the media asset, and add the trustworthiness information to the media asset or use the trustworthiness information as a file associated with the media asset.

[00167] FIG. 5 is a block diagram of a structure of a terminal device 101 in which a media asset management module is located.

[00168] According to one or more implementations described in this application, the terminal device 101 may include electronic components for managing a media item (for example, a media asset). The terminal device 101 may be accommodated in a single computing system (such as a desktop computer system, a laptop computer system, a tablet computer system, a server computer system, a mobile phone, a media player, a personal digital assistant, a personal communicator, a game device, a network router, a network hub, a wireless access point (AP), a repeater, a set-top box, or a combination thereof). The components in the terminal device 101 may be spatially separated and implemented on separate computing systems connected through communication technologies 110.

[00169] For an implementation, one or more components in the client device 101 may be implemented as one or more integrated circuits (IC). For example, at least one of a processing unit 104, a media content capture device 102, a peripheral device 118, a sensor 122, or a memory 110 may be implemented as a system-on-chip (SoC) IC, a three-dimensional (3D) IC, any other known IC, or any combination of known ICs. For another implementation, two or more components in the client device 101 are implemented together as one or more ICs. For example, at least two of a processing unit 104, a media content capture device 102, a peripheral device 118, a sensor 122, or a memory 110 may be implemented together as an SoC IC. The following describes each

component of the client device 101.

[00170] The terminal device 101 may include the media content capture device 102 (for example, an imaging device for capturing an image, an audio device for capturing a sound, a multimedia device for capturing an audio and a video, or any other known user media content capture device). For an implementation, the media content capture device 102 may further include a signal processing pipeline implemented as hardware, software, or a combination thereof. The signal processing pipeline may perform one or more operations on data received from one or more components in the device 102. The signal processing pipeline may also provide processed data to the memory 110, the peripheral device 118 (as further discussed below), and/or the processing unit 104.

[00171] The terminal device 101 may include the processing unit 104, such as a CPU, a GPU, another integrated circuit (IC), a memory, and/or another electronic circuit. For an implementation, the processing unit 104 may generate a media asset 111 associated with media content 114 through the media asset management module 106. In some implementations, the processing unit 104 may generate trustworthiness information based on the content in the media asset, and add the trustworthiness information to the media asset or use the trustworthiness information as a file associated with the media asset (for example, a trust report 121 shown in FIG. 5).

[00172] The terminal device 101 may further include the peripheral device 118. For an implementation, the peripheral device 118 may include at least one of the following: (i) one or more input devices (for example, a mouse, a keyboard, and the like) that interact with or send data to one or more components of the client device 101; (ii) one or more output devices (for example, a monitor, a printer, and a display device) that provide an output from one or more components of the client device 101; or (iii) one or more storage devices that store data other than the memory 110. The peripheral device 118 is shown in a dashed box to indicate that the peripheral device 118 is an optional component of the client device 101. The peripheral device 118 may alternatively be a single component or device that may be used as both an input device and an output device (for example, a touchscreen). The client device 101 may include at least one peripheral control circuit (not shown) for the peripheral device 118. The peripheral control circuit may be a controller (for example, a chip, an expansion card, or an independent device). The controller interacts with the peripheral device 118 and is configured to indicate an operation to be performed by the peripheral device. The peripheral device controller may be a separate processing unit or may be integrated into the processing unit 104. The peripheral device 118 may also be referred to as an input/output (I/O) device 118 throughout this specification.

[00173] The terminal device 101 may further include one or more sensors 122. The one or more sensors are shown in a dashed box to indicate that the sensor may be an optional component of the

client device 101. For an implementation, the sensor 122 may detect one or more characteristics of an environment. Examples of the sensor include but are not limited to an optical sensor, an imaging sensor, an accelerometer, a sound sensor, a barometric pressure sensor, a proximity sensor, a vibration sensor, a gyroscope sensor, a compass, a barometer, a thermal sensor, a rotation sensor, a velocity sensor, and an inclinometer.

[00174] With reference to FIG. 4 and FIG. 10, this embodiment provides a trust evaluation system, including:

a first device, configured to obtain a media asset;

a second device, configured to obtain one or more trust indicators of the media asset based on the media asset, where the first device and the second device may be same or different devices; and

a third device, configured to generate a trust report based on the one or more trust indicators of the media asset that are obtained and trust configuration information. In a possible implementation, the one or more trust indicators of the media asset are recorded in a trust credential. In a possible implementation, the second device sends the one or more trust indicators of the media asset to the third device in response to a request from the third device. The trust configuration information may be recorded in a trust profile. In a possible implementation, the third device may obtain the trust profile from a trust profile repository. In a possible implementation, the third device may directly read the trust profile in a local memory.

[00175] FIG. 6A shows a framework of a trust record of a media asset.

[00176] For example, as shown in FIG. 7, a media asset may include media content (Media Content), metadata (Metadata) of the media content, and a trust record of the media content. The metadata and the trust record of the media content are bound to the media content, or the metadata and the trust record of the media content are associated with the media content.

[00177] When the media asset for the media content is obtained, the metadata and the trust record of the media content are also obtained correspondingly. For example, when an image is obtained, the image in a digital form, and metadata and a trust record of the image can be obtained.

[00178] It should be noted that in some scenarios, a media asset (Media Asset) is also referred to as a media file or a digital asset.

[00179] Media content may be an image, an audio, a video, or a text.

[00180] The media asset may include a trust record (Trust record). In an implementation, the trust record may be a portion of metadata. In an implementation, the trust record and metadata may exist independent of each other in the media asset. For example, the media content may also be referred to as digital content (Digital content). The media content may be a portion of the media asset, and represents actual content of media. The digital content is content, of different content

types that exists in a digital form such as a text, an image, and a sound, and may be stored on digital carriers such as an optical disc and a hard disk and transmitted through means such as a network. The digital content is the entirety of products or services that integrate and use content such as an image, a text, an audio, and a video through digital technologies, and is a product of combining digital media technologies and cultural creativity. For example, the media content may be pixel data of an image, and any additional technical metadata (for example, a color profile or an encoding parameter) required for understanding or presenting the content.

[00181] A digital technology (Digital Technology) is a science and technology that develops alongside electronic computers, and is a technology that uses specific devices to convert various information, including images, texts, audios, videos, and the like, into binary digits "0" and "1" that can be identified by the electronic computers for computing, processing, storage, transmission, dissemination, and restoration. Because processes such as computing and storage need to use the computers for encoding, compression, decoding, and the like of information, the digital technology is also referred to as a digital tech, a computer digital technology, and the like. The digital technology is also referred to as a digital control technology.

[00182] For example, the metadata may include data used to describe the media content, and the metadata may record non-technical information about the media asset or the media content. For example, the metadata may include information that describes a property (property) of the media content. For example, the metadata may be a trust document (or referred to as a trust manifest (Trust Manifest)). For example, the metadata may be a creation location, a creator, an annotation, or IPR information of the media content.

[00183] For example, as shown in FIG. 8, a trust record of media content may be a type of metadata of the media content (or does not belong to metadata, but is independent of the metadata and belongs to a media asset). The trust record records related information about generation and transition of the media content, and may be used for tracing provenance of the media content.

[00184] In an embodiment, as shown in FIG. 6A, the trust record may include a trust declaration and a trust manifest.

[00185] For example, the trust declaration (Trust declaration) may be a type of trust manifest, and may be at the 1st place of the trust record. The trust declaration may alternatively be a type of metadata of media content.

[00186] In a possible implementation, the trust declaration (Trust declaration) in the trust record may include initial information of first media content, a hard binding (Hard binding) of the first media content, and a first digital signature $Signature_{sk0}$; the first digital signature is a digital signature of first data; and the first data is data determined based on at least the initial information and the hard binding of the first media content.

[00187] The first media content may be content of different content types that exists in a digital form, such as a text, an image, and a sound. For example, the first media content may be pixel data of an image, and any additional technical metadata (for example, a color profile or an encoding parameter) required for understanding or presenting the content.

[00188] A hard binding refers to data obtained by performing hard binding processing on original data. The hard binding processing is a processing method used to prevent the original data from being forged, and the original data cannot be obtained by performing reverse processing on a hard binding of the original data. Hard binding processing is performed on the original data to obtain the hard binding of the original data. For example, the original data is processed using a one-way function. For example, hash processing may be a type of hard binding processing. In other words, a hard binding may include a hash value. The hard binding of the first media content may also include a first media hash value, where the first media hash value (Media Hash 0) is a hash value of the first media content.

[00189] For example, the first data is data obtained by combining at least the hard binding of the first media content and the initial information of the first media content, or the first data is data obtained by combining at least a hard binding of the initial information (for example, a hash value AIGC.Hash of AI generation AIGC, or a hash value Media Type.Hash of a media generation manner) and a hard binding of a first media hard binding (for example, a hash value Media Hash 0.Hash of the first media hash value).

[00190] For example, the first data may alternatively be a first combined hash value (Hash(TD)), and the first combined hash value includes a hash value obtained by combining the initial information of the first media content and the first media hash value. For example, the first combined hash value includes a hash value obtained by combining the initial information of the first media content, the first media hash value, and other descriptive information; and the other descriptive information may not be other descriptive information in the initial information, for example, information about a tool for generating a trust profile or other information describing the initial information of the first media content. This is not limited in this application.

[00191] For example, the first data may alternatively be a first combined hash value, and the first combined hash value may include a hash value obtained by combining a hash value of the initial information of the first media content and the hash value (Media Hash 0. Hash) of the first media hash value. For example, the first combined hash value is a hash value obtained by combining the hash value of the initial information of the first media content, the hash value of the first media hash value, and a hash value of other metadata information. Herein, when there are at least two pieces of initial information of the first media content, the hash value of the initial information of the first media content may include a hash value of each piece of initial information

of the first media content, or the hash value of the initial information of the first media content may include a hash value obtained by combining all the pieces of initial information of the first media content.

[00192] For example, the initial information of the media content may be information generated when the media content is generated. For example, the initial information of the media content includes at least one of the following: generation time of the media content, an author name of the media content, a digital content identifier of the media content, a generation location of the media content, information about a generation device of the media content, a resolution of the media content, a size of the media content, a media type (Media Type) of the media content, or a generation manner of the media content. For example, the information about the generation device of the media content may include a model of the device, a parameter of a camera, and the like; and the parameter of the camera may include a focal length, photosensitivity, exposure, and the like of the camera during picture-taking. It should be understood that the initial information of the media content may further include other information, for example, information used to describe the media content such as copyright information. This is not limited in this application.

[00193] For example, the media type may include but is not limited to an image type, a video type, an audio type, a graphics type, and the like. The generation manner may include an AI generation manner, a non-AI generation manner, and the like. In a possible manner, the generation manner in the initial information may be replaced with an AI generation (AIGC) identifier. For example, when the media content is generated by AI, a value of the AIGC identifier is 1; or when the media content is not generated by AI, a value of the AIGC identifier is 0. The author name of the media content may be a name of a creator of the media content or a name of a shooting device of the media content. This is not limited in this application.

[00194] The first data is usually digitally signed by using a private key, to obtain the digital signature of the first data.

[00195] For example, the private key may be a private key of an electronic device or a user. For example, the first data may be digitally signed by using a digital signature algorithm and the private key, to obtain the digital signature of the first data. It should be understood that the digital signature algorithm is not limited in this application.

[00196] For example, the trust manifest (trust manifest) records information indicating provenance of the media asset. The trust manifest is a portion of the trust record. The trust manifest may alternatively be a type of metadata.

[00197] For example, the trust manifest may include a hard binding of $(N+1)^{th}$ media content (for example, a second media hash value Media Hash 1). For example, media content obtained by performing editing processing on N^{th} media content based on an editing operation, or media

content obtained by modifying metadata of N^{th} media content, or to-be-forwarded (or to-be-shared) N^{th} media content may be referred to as the $(N+1)^{th}$ media content.

[00198] For example, the trust manifest may further include a media assertion (Assertion), and the media assertion may include copyright information, a thumbnail, whether modification is allowed, an operation permission, a use permission, provenance of second media content, and the like.

[00199] For example, the trust manifest may further include a second digital signature $Signature_{sk1}$, the second digital signature is a digital signature of second data, and the second data may be data determined based on at least the second media hash value and a modification assertion.

[00200] For example, the second data is data obtained by combining at least an $(N+1)^{th}$ media hash value and an $(N+1)^{th}$ assertion, or the data is data obtained by combining at least a hash value (Assertion Hash) of an $(N+1)^{th}$ assertion and a hash value of an $(N+1)^{th}$ media hash value.

[00201] For example, the second data may alternatively be an $(N+1)^{th}$ combined hash value, and the $(N+1)^{th}$ combined hash value includes a hash value obtained by combining an $(N+1)^{th}$ assertion and an $(N+1)^{th}$ media hash value. For example, the $(N+1)^{th}$ combined hash value includes a hash value obtained by combining the (N+1)th assertion, the (N+1)th media hash value, and other descriptive information, and the other descriptive information may not be other descriptive information in the $(N+1)^{th}$ assertion, for example, information about a tool for generating a trust manifest or other information describing the $(N+1)^{th}$ assertion. This is not limited in this application.

[00202] For example, the second data may alternatively be an $(N+1)^{th}$ combined hash value, and the $(N+1)^{th}$ combined hash value may include a hash value obtained by combining a hash value of an $(N+1)^{th}$ assertion and a hash value of an $(N+1)^{th}$ media hash value (for example, a hash value of the second media hash value Media Hash 1. Hash). For example, the $(N+1)^{th}$ combined hash value is a hash value obtained by combining the hash value of the $(N+1)^{th}$ assertion, the hash value of the $(N+1)^{th}$ media hash value, and a hash value of other metadata information (Other Information).

[00203] For example, the trust manifest may further include a first uniform resource identifier (URI, Uniform Resource Identifier), and the first URI indicates a location of the initial information of the first media content or the hard binding of the first media content in a modification record of the first media content. For example, URI1 indicates a location of the hard binding of the first media content in the trust record of the first media content, URI2 indicates a location of a media type in the trust record of the first media content, URI3 indicates a location of AIGC in the trust record of the first media content, URI4 indicates a location of the hard binding of the $(N+1)^{th}$ media content (for example, the second media hash value Media Hash 1) in the trust record, and URI5

indicates a location of the media assertion (Assertion) in the trust record.

[00204] For example, the modification record may further include other information, and the other information may be information that is not used to confirm authenticity of the media content, for example, a file name and a name of a hash algorithm. The hash algorithm is used to calculate the hash value mentioned in the foregoing embodiment.

[00205] The following describes a method procedure in embodiments of this application by using examples.

[00206] FIG. 6B shows a procedure of a data processing method according to an embodiment of this application. The procedure mainly describes a process of generating trustworthiness information. As shown in FIG. 6B, the data processing method provided in this embodiment of this application includes the following steps.

[00207] 601: Obtain one or more trust indicators of a media asset, where the media asset includes media content, and at least one of metadata corresponding to the media content and a trust record corresponding to the media content.

[00208] For example, the trust indicator (trust indicator) is a parameter indicating a trustworthiness level of the media asset. In a possible implementation, the trust indicator of the media asset may be obtained from a trust credential, that is, the trust indicator of the media asset is encapsulated in the trust credential. In a possible implementation, the trust indicator may be obtained from the media asset, and a corresponding trust indicator is directly read from the media asset. In a possible implementation, the media asset includes at least one of the media content, the metadata corresponding to the media content, and the trust record corresponding to the media content. In this embodiment of this application, to enable a user to determine the trustworthiness level of the media asset, the one or more trust indicators related to the trustworthiness level of the media asset may be determined based on the media asset. The user can analyze and determine the trustworthiness level of the media asset based on a verification result of the trust indicator.

[00209] In a possible implementation, as shown in FIG. 8, the media asset may include the media content and the metadata of the media content. The metadata of the media content is bound to the media content, or the metadata of the media content is associated with the media content. The metadata may include the trust record; or the metadata may not include the trust record, and the trust record and the metadata may be different portions of the media asset. In other words, as shown in FIG. 8, the media asset may include the media content and the metadata corresponding to the media content (the trust record is encapsulated in the metadata); or as shown in FIG. 7, the media asset may include the media content, the metadata corresponding to the media content, and the trust record corresponding to the media content.

[00210] In a possible implementation, the trust record may further be divided into a trust

declaration (trust declaration) and several trust manifests (trust manifests). The trust manifest (trust manifest) is a set of media asset provenance information. The trust declaration (trust declaration) is a special type of trust manifest, and includes only a mandatory assertion (mandatory provenance information). The trust declaration (trust declaration) may appear at the 1st place of the trust record (trust record).

[00211] In a possible implementation, the one or more trust indicators related to the trustworthiness level of the media asset may be determined based on the media asset. Specifically, as shown in FIG. 7, the one or more trust indicators related to the trustworthiness level of the media asset may be determined based on at least one of the media content, the metadata corresponding to the media content, and the trust record corresponding to the media content. As shown in FIG. 8, the one or more trust indicators related to the trustworthiness level of the media asset may be determined based on at least one of the media content and the metadata corresponding to the media content (the trust record is a portion of the metadata).

[00212] For example, the trust indicator of the media asset may be a feature extracted from the media content, the metadata corresponding to the media content, and the trust record corresponding to the media content, or may be data obtained by performing specific processing on features in the media content, the metadata corresponding to the media content, and the trust record corresponding to the media content.

[00213] For example, one or more trust indicators TM related to the trustworthiness level of the media asset may be determined based on the metadata of the media content. For example, TM may be generation time of the media content, an author name of the media content, a digital content identifier of the media content, a generation location of the media content, information about a generation device of the media content, a media type (Media Type) of the media content, or a generation manner of the media content. For example, the information about the generation device of the media content may include a model of the device, a parameter of a camera, and the like; and the parameter of the camera may include a focal length, photosensitivity, exposure, and the like of the camera during picture-taking. It should be understood that TM may further include other information, for example, information used to describe the media content such as copyright information. This is not limited in this application.

[00214] For example, the one or more trust indicators related to the trustworthiness level of the media asset may be determined based on the metadata of the media content and the trust record of the media content.

[00215] For example, the one or more trust indicators related to the trustworthiness level of the media asset may be determined based on the metadata of the media content, the media content, and the trust record of the media content.

[00216] For example, one or more trust indicators TR related to the trustworthiness level of the media asset may be determined based on the trust record of the media content. For example, generation time of the media content, an author name of the media content, a digital content identifier of the media content, a generation location of the media content, information about a generation device of the media content, a media editing manner, a media type (Media Type) of the media content, or a generation manner of the media content in the trust record may be selected as TR. For example, the information about the generation device of the media content may include a model of the device, a parameter of a camera, and the like; and the parameter of the camera may include a focal length, photosensitivity, exposure, and the like of the camera during picture-taking. It should be understood that TR may further include other information, for example, information used to describe the media content such as copyright information. This is not limited in this application. The media generation manner may include but is not limited to whether the media content is generated through AIGC, whether the media content is generated through a camera, whether the media content is generated with software assistance, whether the media content is generated through synthetic media, and whether the media content can be used to train a model. The media editing manner may include but is not limited to rotation, resizing, cropping, content editing, and the like. TR may further include a media assertion, and the media assertion may include a thumbnail, whether modification is allowed, an operation permission, a use permission, provenance of second media content, and the like.

[00217] For example, the one or more trust indicators related to the trustworthiness level of the media asset may be determined based on the media content and the trust record of the media content.

[00218] For example, one or more trust indicators TC related to the trustworthiness level of the media asset may be determined based on the media content. For example, features such as a person, a scene, an object type, a position relationship between objects, and a media style (for example, color, lighting, or brightness) in the media content may be selected as trust indicators of the media content.

[00219] For example, the one or more trust indicators related to the trustworthiness level of the media asset may be determined based on the metadata of the media content and the media content.

[00220] The trust indicator may be a feature description of the media asset. For example, the trust indicator may include a parameter indicating the trustworthiness level of the media asset.

[00221] In a possible implementation, the trust credential may include a relationship between each trust indicator and corresponding provenance, that is, the trust indicator corresponds to a specific portion (metadata, a trust record, or media content) of the media asset. The trust credential (trust credential) is the one or more trust indicators obtained based on the media asset.

[00222] In a possible implementation, when a trust indicator is obtained, the trust indicator may be used as the trust credential. In a possible implementation, when a plurality of trust indicator are obtained, all of the trust indicators may be encapsulated to obtain the trust credential. In a possible implementation, the trust indicator and other data may alternatively be encapsulated together to obtain the trust credential.

[00223] In a possible implementation, for the one or more obtained trust indicators of the media asset, a corresponding requirement, namely, an evaluation constraint on the trust indicator of the media asset in a specific scenario may be obtained. The evaluation constraint may be considered as a constraint related to the trustworthiness level of the media asset.

[00224] In this embodiment of this application, the evaluation constraint on the trust indicator of the media asset may be described by using a profile, and the profile may include a metric requirement corresponding to each trust indicator. The profile may also be referred to as a trust profile (trust profile). The trust profile records a set of specified trust metrics, and the set of trust metrics can be used to evaluate a trust credential of a specific media asset.

[00225] 602: Determine whether the one or more trust indicators satisfy a metric.

[00226] In an implementation, the metric may be stored in a memory. When there is a need to evaluate trustworthiness of the media asset, the one or more trust indicators of the media asset are obtained, and matching is performed between a trust indicator corresponding to the metric and the one or more trust indicators of the media asset, to determine whether the one or more trust indicators satisfy the metric.

[00227] In an implementation, each metric specified in the trust profile is specific to a trust indicator. A corresponding trust indicator may be obtained from the media asset based on a metric specified in the profile, and trustworthiness information of the media asset may be obtained based on the trust profile and the one or more trust indicators of the media asset.

[00228] For example, the trust profile records trust configuration information, and the trust configuration information includes a metric that the media asset needs to satisfy. In other words, the trust configuration information includes a metric that the trust credential needs to satisfy, and the trust configuration information may be a set of trust indicators, used to evaluate the trust credential and indicating a trustworthiness level of the media asset.

[00229] In an implementation, a plurality of metrics of the media asset may be first obtained, and the plurality of metrics may include a metric other than a constraining metric in the profile. Therefore, satisfaction of each trust indicator against a metric may be determined based on the metric specified in a profile, to obtain the trustworthiness information of the media asset.

[00230] In an implementation, the metric may be data obtained through processing based on a trust indicator, but the metric may indicate the corresponding trust indicator. That is, the metric

may be a trust indicator of the media asset, a value of a trust indicator, or data obtained by performing specific processing on a trust indicator.

[00231] In an implementation, the metric may include one or more trust indicators, and whether the trust indicator in the metric is included in the one or more trust indicators of the media asset may be determined, to determine whether the one or more trust indicators of the media asset satisfy the metric.

[00232] In an implementation, whether the one or more trust indicators of the media asset include a trust indicator in the metric is determined, to determine whether the one or more trust indicators of the media asset satisfy the metric. In other words, when a trust indicator included in the trust profile is included in the trust indicator of the media asset, it may be considered that the trust indicator of the media asset satisfies the metric, or the trust indicator may be content of the metadata of the media asset or content of a modification record of the media asset, or a feature of the media content. As shown in FIG. 7, metrics in the trust profile include TM1', TR1', TC1', and TM11'; and TM1', TR1', TC1', and TM11' correspond to trust indicators TM1, TR1, TC1, and TM11. For example, TM1 is Shenzhen, Guangdong Province, and TM1' may be a location or China. In this case, TM1 satisfies the metric. Because TM11 does not exist in the one or more trust indicators of the media asset, TM11 does not satisfy the corresponding metric. In other words, when a trust indicator indicated by the metric in the trust configuration information does not exist in the one or more trust indicators of the media asset, the media asset does not satisfy a metric requirement of the trust configuration information. When the trust indicator of the media asset includes the trust indicator included in the trust profile, it may be considered that the trust indicator of the media asset satisfies the metric.

[00233] As shown in FIG. 8, metrics in the trust profile include TM1', TM2', TM3', and TC1', and corresponding trust indicators TM1, TM2, TM3, and TC1 exist in the trust credential. In other words, when all trust indicators indicated by the metric in the trust configuration information exist in the one or more trust indicators of the media asset, the media asset satisfies a metric requirement of the trust configuration information.

[00234] In an implementation, the metric may include a determining condition, and the determining condition indicates whether a target trust indicator exists in the one or more trust indicators of the media asset. Whether the one or more trust indicators satisfy the determining condition may be determined, to determine whether the one or more trust indicators satisfy the metric. The trustworthiness information may be represented as a trust report. A result of evaluating the trust credential based on the trust configuration information is generated and recorded by using the trust profile and the trust credential as inputs. The evaluation is evaluation of a trustworthiness level of the given media asset. The result may be provided to the user as the trustworthiness

information.

[00235] Subsequently, the trustworthiness information may be used to generate a new trust manifest (details are described in subsequent embodiments), or may be used as a file associated with the media asset.

[00236] Satisfaction of the one or more trust indicators of the media asset against the metric in the profile may be indicated by the trustworthiness information. The user can determine the trustworthiness level of the media asset based on the trustworthiness information.

[00237] The foregoing describes the basic procedure of the method shown in FIG. 6B. The following describes specific implementations that may be used for some steps of the method shown in FIG. 6B by using examples.

[00238] In step 602, because different regions or different users may have different metric requirements for a same media asset, a plurality of profiles may be obtained. The plurality of profiles may be stored in a profile repository, and each profile is a metric requirement of one region or user for a media asset. Therefore, there are a plurality of possible specific implementations of obtaining the trustworthiness information of the media asset based on the profile and the trust indicator. The following provides descriptions by using examples with reference to implementations A to D.

[00239] Implementation A: There is only one set of metrics in the trust profile.

[00240] For trust indicators of the media asset, there may be only one set of metrics. In this case, whether the trust indicators of the media asset satisfy the set of metrics may be computed based on uniquely corresponding metric requirements, to obtain the trustworthiness information.

[00241] It should be understood that, because there is only one set of metric requirements, an association relationship between a trust indicator and a corresponding metric requirement may not be stored in the trustworthiness information, that is, a specific region or a specific user whose metric requirements are used for obtaining the trustworthiness information is not indicated.

[00242] Implementation B: There are a plurality of trust profiles for the trust indicator, and for each trust profile, corresponding trustworthiness information is computed.

[00243] Because different regions or users have different requirements on a trustworthiness level, each trust profile includes a set of metrics, and different sets of metrics indicate metric requirements, of different regions or users, that the media asset needs to satisfy. In this case, satisfaction of the trust indicator against a plurality of metric requirements may be computed, to obtain a plurality of pieces of trustworthiness information.

[00244] It should be understood that an association relationship between a trust indicator and a corresponding metric requirement may be stored in the trustworthiness information, to indicate a specific region or a specific user whose metric corresponds to the trustworthiness information.

[00245] Implementation C: There are a plurality of trust profiles, and for only a part of the trust profiles (for example, one trust profile), corresponding trustworthiness information is computed.

[00246] Different regions or users have different requirements on a trustworthiness level, and there may be a plurality of metric requirements for the trust indicator of the media asset (different metric requirements in the plurality of requirements correspond to different regions or different users). When a system computes trustworthiness information, a user may specify computation of satisfaction of the trust indicator of the media asset against a specific set or a plurality of sets of metric requirements.

[00247] It should be understood that an association relationship between a trust indicator of a media asset and a corresponding metric requirement may be stored in the trustworthiness information, to indicate a specific region or a specific user whose metric requirement corresponds to the trustworthiness information.

[00248] According to this application, in the foregoing implementation, different scenarios (for example, regions or users) may correspond to different requirements, and different pieces of trustworthiness information may be generated, so that trustworthiness level determining requirements of the different scenarios can be met.

[00249] Implementation D: There may be a plurality of pieces of trust configuration information for the trust indicator, different pieces of trust configuration information indicate metric requirements, of different regions or users, that the media asset needs to satisfy, and the plurality of pieces of trust configuration information may be stored in one trust profile or a plurality of trust profiles. The trustworthiness information of the media asset may be obtained based on the first configuration information and the trust indicator of the media asset, where the first configuration information is one of the plurality of pieces of trust configuration information.

[00250] After the trustworthiness information is obtained, the media asset may be updated using the trustworthiness information. The following describes a specific implementation of updating the media asset using the trustworthiness information.

[00251] FIG. 9 shows a procedure of a data processing method according to an embodiment of this application.

[00252] 901: Capture media content through a hardware sensor or generate media content through generation software.

[00253] A terminal device may capture media content through a hardware sensor or generate media content through software. For example, the terminal device may capture an image through a camera built in the terminal device, or generate new media content through media content editing software (for example, AIGC).

[00254] When obtaining the media content, the terminal device further needs to generate a

corresponding media asset through a media asset management module, where the media asset may include metadata, a trust record, and the like.

[00255] In this embodiment of this application, the media asset management module may capture the media content through the hardware sensor or generate the media content through the generation software, generate trustworthiness information based on the content in the media asset, and add the trustworthiness information to the media asset.

[00256] It should be understood that step 901 may be understood as an action before step 902. For example, step 901 may be a trigger condition of step 902 (optionally, step 901 may be one of a plurality of trigger conditions of step 902).

[00257] 902: Obtain one or more trust indicators of a media asset, where the media asset includes the media content, and at least one of metadata of the media content and a trust record of the media content.

[00258] For descriptions of step 902, refer to the descriptions of step 601 in the foregoing embodiment. Similarities are not described herein again.

[00259] 903: Determine whether each trust indicator satisfies a metric, to obtain trustworthiness information.

[00260] For descriptions of step 903, refer to the descriptions of step 602 in the foregoing embodiment. Similarities are not described herein again.

[00261] 904: Add the trustworthiness information to the trust record.

[00262] During addition of the trustworthiness information to the trust record, the trustworthiness information may be added to an assertion (assertion).

[00263] Specifically, the trustworthiness information may be signed and then added to the assertion (assertion).

[00264] For example, trustworthiness information corresponding to one piece of media content may be signed and then added to the assertion as one of items of the assertion.

[00265] For example, satisfaction that corresponds to each metric or a part of metrics and that is in the trustworthiness information may be signed and then added to the assertion as one of items of the assertion.

[00266] Adding the newly generated trustworthiness information to the trust record of the media asset can further enhance trustworthiness of the media asset.

[00267] In addition, a hash value of the trustworthiness information may further be added to a claim (claim) in a trust manifest.

[00268] In addition, a signature of the trustworthiness information may further be added to a signature in the trust manifest.

[00269] Based on FIG. 6B, FIG. 10 shows a procedure of a data processing method according

to an embodiment of this application. Compared with FIG. 6, the flowchart in FIG. 10 describes a process of generation of trustworthiness information and update of a media asset, by using a relationship between functional modules. The flowchart in FIG. 10 specifically includes:

a generation module, an extraction module, a trust profile storage module, and a verification module. The generation module is configured to generate a media asset, where each media asset includes three portions: metadata, media content, and a trust record. The extraction module, using the media asset as an input, extracts a trust indicator from metadata, a trust record, and media content of the media asset, and generates a trust credential of the media asset based on the extracted trust metric. The trust profile storage module is responsible for storing a trust profile, where the trust profile is predefined by an entity such as a government, a platform, or a user for a specific scenario. The verification module, using the trust credential and the trust profile as inputs, evaluates whether the trust metric in the trust credential satisfies the predefined trust profile. Finally, a trust report is generated based on a result of the evaluation.

[00270] Based on FIG. 6, FIG. 11A and FIG. 11B, and FIG. 12A and FIG. 12B each show a procedure of a data processing method according to an embodiment of this application. Compared with FIG. 6, the flowchart in FIG. 11A and FIG. 11B and the flowchart in FIG. 12A and FIG. 12B each describe a process of generation of trustworthiness information and update of a media asset, by using a relationship between functional modules. A difference between FIG. 11A and FIG. 11B and FIG. 12A and FIG. 12B lies in that a generation algorithm initiates the procedure in FIG. 11A and FIG. 11B while a verification algorithm initiates the procedure in FIG. 12A and FIG. 12B.

[00271] FIG. 11A and FIG. 11B specifically include the following steps:

[00272] 1: The generation algorithm is configured to generate a media asset, where each media asset includes metadata, media content, and a trust record.

[00273] 2: The generation algorithm passes the media asset to an extraction algorithm.

[00274] 3: The extraction algorithm, using the media asset as an input, extracts a trust metric from metadata, a trust record, and media content of the media asset, and generates a trust credential of the media asset based on the extracted trust metric.

[00275] 4: The extraction algorithm passes the trust credential to a verification algorithm.

[00276] 5: The verification algorithm triggers a verification process.

[00277] 6: The verification algorithm requests to obtain a trust profile from a trust file storage side, where the trust profile is predefined by an entity such as a government, a platform, or a user for a specific scenario.

[00278] 7: The trustworthiness file storage side passes the trust profile to the verification algorithm.

[00279] 8: The verification algorithm, using the trust credential and the trust profile as inputs,

evaluates whether the trust metric in the trust credential satisfies the predefined trust profile, and generates a trust report based on a result of the evaluation.

[00280] 9: The verification algorithm generates a new trust manifest based on the trust report.

[00281] 10: The verification algorithm returns the trust manifest to the generation algorithm.

[00282] 11: The generation algorithm adds the new trust manifest to the trust record, to update the media asset.

[00283] FIG. 12A and FIG. 12B specifically include the following steps:

[00284] 0: A generation algorithm is configured to generate a media asset, where each media asset includes metadata, media content, and a trust record.

[00285] 1: The verification algorithm triggers a verification process.

[00286] 2: The verification algorithm requests to obtain a trust profile from a trustworthiness file storage side, where the trust profile is predefined by an entity such as a government, a platform, or a user for a specific scenario.

[00287] 3: The trustworthiness file storage side passes the trust profile to the verification algorithm.

[00288] 4: The verification algorithm requests to obtain a trust credential from an extraction algorithm.

[00289] 5: The extraction algorithm requests to obtain the media asset from the generation algorithm.

[00290] 6: The generation algorithm passes the media asset to the extraction algorithm.

[00291] 7: The extraction algorithm, using the media asset as an input, extracts a trust metric from metadata, a trust record, and media content of the media asset, and generates the trust credential of the media asset based on the extracted trust metric.

[00292] 8: The extraction algorithm passes the trust credential to the verification algorithm.

[00293] 9: The verification algorithm, using the trust credential and the trust profile as inputs, evaluates whether the trust metric in the trust credential satisfies the predefined trust profile, and generates a trust report based on a result of the evaluation.

[00294] 10: The verification algorithm generates a new trust manifest based on the trust report.

[00295] 11: The verification algorithm returns the trust manifest to the generation algorithm.

[00296] 12: The generation algorithm adds the new trust manifest to the trust record, to update the media asset.

[00297] After trustworthiness information is obtained, a file associated with the media asset may be generated based on the trustworthiness information. The file may be used and viewed by the user, and used as a trustworthiness level determining basis during trustworthiness level determining. The following provides descriptions.

[00298] FIG. 13 shows a procedure of a data processing method according to an embodiment of this application. The data processing method includes the following steps.

[00299] 1301: Capture media content through a hardware sensor or generate media content through generation software.

[00300] For descriptions of step 1301, refer to the descriptions of step 901 in the foregoing embodiment. Similarities are not described herein again.

[00301] 1302: Obtain one or more trust indicators of a media asset, where the media asset includes the media content, and at least one of metadata corresponding to the media content and a trust record corresponding to the media content.

[00302] For descriptions of step 1302, refer to the descriptions of step 902 in the foregoing embodiment. Similarities are not described herein again.

[00303] 1303: Determine whether each trust indicator satisfies a metric, to obtain trustworthiness information.

[00304] For descriptions of step 1303, refer to the descriptions of step 903 in the foregoing embodiment. Similarities are not described herein again.

[00305] 1304: Generate, based on the trustworthiness information, a file associated with the media asset.

[00306] The associated file may be an independently encapsulated file, and the file may be bound to the media asset. A user may determine a trustworthiness level of the media content by viewing the file.

[00307] In addition to automatic triggering by capturing the media content through a hardware sensor or generating the media content through generation software as described in FIG. 9, triggering of generation of the trustworthiness information may also be user-based active triggering. The following provides descriptions.

[00308] FIG. 14 shows a procedure of a data processing method according to an embodiment of this application. The data processing method includes the following steps.

[00309] 1401: Receive a trustworthiness evaluation request for a media asset.

[00310] For example, a user may input a trustworthiness evaluation request for media content through a trustworthiness level determining application.

[00311] For example, a client side may input a trustworthiness evaluation request for media content through an interface of a cloud service for providing a trustworthiness level determining service.

[00312] The request may carry the media asset.

[00313] 1402: Obtain one or more trust indicators of the media asset, where the media asset includes media content, and at least one of metadata corresponding to the media content and a trust

record corresponding to the media content.

[00314] For descriptions of step 1402, refer to the descriptions of step 902 in the foregoing embodiment. Similarities are not described herein again.

[00315] 1403: Determine whether each trust indicator satisfies a metric, to obtain trustworthiness information.

[00316] For descriptions of step 1403, refer to the descriptions of step 903 in the foregoing embodiment. Similarities are not described herein again.

[00317] 1404: Send the trustworthiness information to the client side.

[00318] In the foregoing embodiment, a process of generating trustworthiness information of one media asset is described. The following describes a process of generating trustworthiness information of a plurality of media assets in batches.

[00319] FIG. 15 shows a procedure of a data processing method according to an embodiment of this application. The data processing method includes the following steps.

[00320] 1501: Obtain indication information of a media asset.

[00321] For example, the indication information may be a media asset ID. Because this is a process of generating trust reports of a plurality of media assets in batches, there is a need to transmit corresponding media asset IDs.

[00322] 1502: Obtain, based on the indication information, one or more trust indicators of the media asset indicated by the indication information, where the media asset includes media content, and at least one of metadata corresponding to the media content and a trust record corresponding to the media content.

[00323] 1503: Determine whether each trust indicator satisfies a metric, to obtain trustworthiness information.

[00324] 1504: Add, based on the indication information, the trustworthiness information to the trust record corresponding to the media asset indicated by the indication information.

[00325] Based on FIG. 15, FIG. 16A-1 and FIG. 16A-2 show a procedure of a data processing method according to an embodiment of this application. Compared with FIG. 15, the flowchart in FIG. 16A-1 and FIG. 16A-2 describes, by using a relationship between functional modules, a process of generation of trustworthiness information in batches and update of media assets.

[00326] FIG. 16A-1 and FIG. 16A-2 specifically include the following steps:

[00327] 1: A generation algorithm is configured to generate a media asset, where each media asset includes metadata, media content, and a trust record.

[00328] 2: The generation algorithm sends a request to an extraction algorithm for generation of a trust credential (including a media asset ID and a corresponding media asset)

[00329] 3: The extraction algorithm, using the media assets as inputs, extracts a trust metric

from the metadata, the trust record, and the media content of each media asset, and generates a trust credential of each media asset based on the extracted trust metric.

[00330] 4: The extraction algorithm sends the trust credential in a format of (media asset ID, corresponding trust credential) to a verification algorithm.

[00331] 5: The verification algorithm triggers a verification process.

[00332] 6: The verification algorithm requests to obtain a trust profile from a trustworthiness file storage side, where the trust profile is predefined by an entity such as a government, a platform, or a user for a specific scenario.

[00333] 7: The trustworthiness file storage side passes the trust profile to the verification algorithm.

[00334] 8: The verification algorithm, using the trust credential and a trust profile of each media asset as inputs, evaluates whether the trust metric in the trust credential corresponding to each media asset satisfies the predefined trust profile, and generate a trust report based on a result of the evaluation. The verification algorithm generates a trust report for each media asset based on the result of the evaluation.

[00335] 9: The verification algorithm generates a new trust manifest for each media asset based on the trust report.

[00336] 10: The verification algorithm returns the trust manifest in a format of (media asset ID, corresponding new trust manifest) to the generation algorithm.

[00337] 11: The generation algorithm adds the new trust manifest to the trust record, to update the media asset.

[00338] FIG. 6 to FIG. 16A-2 describe a process of generating or using trustworthiness information. The following describes a process of generating and using a trust credential with reference to the accompanying drawings.

[00339] FIG. 16B shows a procedure of a data processing method according to an embodiment of this application. The procedure mainly describes a process of generating trustworthiness information. As shown in FIG. 16B, the data processing method provided in this embodiment of this application includes the following steps.

[00340] 1601: Obtain a media asset, where the media asset includes media content, and at least one of metadata corresponding to the media content and a trust record corresponding to the media content.

[00341] For descriptions of step 1601, refer to the descriptions related to the media asset in the foregoing embodiments. Similarities are not described herein again.

[00342] 1602: Determine one or more trust indicators of the media asset based on the media asset.

[00343] For descriptions of step 1602, refer to the descriptions related to the trust indicator in the foregoing embodiments. Similarities are not described herein again.

[00344] The trust indicator may be encapsulated in a trust credential.

[00345] In a possible implementation, the trust credential may be further added to the trust record.

[00346] In a possible implementation, a file associated with the media asset may further be generated based on the trust credential.

[00347] The associated file may be an independently encapsulated file, and the file may be bound to the media asset. A user may determine a trustworthiness level of the media content by viewing the file.

[00348] The trust indicator of the media asset may be by obtaining the trust indicator of the media asset.

[00349] FIG. 16C shows a trust record generation method. Based on FIG. 6B, this embodiment provides a trust record generation method. Optionally, a trust record may also be metadata. The trust record generation method includes the following steps.

[00350] S161: Obtain first media content.

[00351] For example, the first media content may be media content generated by a first electronic device, or may be media content received by a first electronic device from another electronic device. For example, if the first media content is an image, the first media content may be an image shot by the first electronic device, a screenshot, an AI-generated image, or the like. A manner in which the first electronic device generates an image is not limited in this application. Alternatively, the first media content may be an image received by the first electronic device from another electronic device. This is not limited in this application.

[00352] S162: Generate a modification record of the first media content, where a trust record of the first media content includes initial information of the first media content, a hard binding of the first media content, and a first digital signature; the first digital signature is a digital signature of first data; and the first data is data determined based on at least the initial information and the hard binding of the first media content.

[00353] Explanations of the technical terms used in steps S161 and S162 are consistent with the explanations of the terms in the foregoing embodiments. Details are not described herein again.

[00354] FIG. 17 is a diagram of a structure of a data processing apparatus according to an embodiment of this application. The apparatus 1700 includes the following modules.

[00355] An obtaining module 1701 is configured to obtain one or more trust indicators of a media asset, where the media asset includes media content, and at least one of metadata corresponding to the media content and a trust record corresponding to the media content.

[00356] For specific descriptions of the obtaining module 1701, refer to the descriptions of step 601 in the foregoing embodiment. Details are not described herein again.

[00357] A processing module 1702 is configured to determine whether the one or more trust indicators satisfy a metric.

[00358] For specific descriptions of the processing module 1702, refer to the descriptions of step 602 in the foregoing embodiment. Details are not described herein again.

[00359] In a possible implementation, the obtaining module 1701 is further configured to:

obtain first trust configuration information, where the first trust configuration information includes a metric that the media asset needs to satisfy.

[00360] In a possible implementation, the one or more trust indicators are determined based on at least one of the media content, the metadata corresponding to the media content, and the trust record corresponding to the media content.

[00361] In a possible implementation, the one or more trust indicators are encapsulated in a trust credential.

[00362] In a possible implementation, the metric includes data indicating a trust indicator that the media asset needs to satisfy.

[00363] In a possible implementation, the processing module 1702 is specifically configured to:

determine whether a trust indicator in the metric is included in the one or more trust indicators, or determining whether the one or more trust indicators include a trust indicator in the metric.

[00364] In a possible implementation, the processing module 1702 is further configured to:

generate trustworthiness information of the media asset, where the trustworthiness information indicates whether the one or more trust indicators satisfy the metric, and the trust indicator includes a parameter indicating a trustworthiness level of the media asset. In a possible implementation, the processing module 1702 is further configured to:

add the trustworthiness information to the trust record.

[00365] In a possible implementation, the trust record includes a trust manifest; and

the processing module 1702 is specifically configured to:

add the trustworthiness information to the trust manifest.

[00366] In a possible implementation, the obtaining module 1701 is further configured to:

obtain indication information of the media asset; and

the processing module 1702 is specifically configured to:

add, based on the indication information, the trustworthiness information to the trust record corresponding to the media asset indicated by the indication information.

[00367] In a possible implementation, the trustworthiness information is encapsulated in a trust

report.

[00368] In a possible implementation, the processing module 1702 is further configured to:

generate, based on the trustworthiness information, a file associated with the media asset.

[00369] In a possible implementation, the first trust configuration information includes one of a plurality of pieces of trust configuration information, and different pieces of trust configuration information indicate metric requirements, of different regions or users, that the media asset needs to satisfy.

[00370] In a possible implementation, the action of obtaining the one or more trust indicators of the media asset is triggered by capturing the media content through a hardware sensor or generating the media content through generation software.

[00371] In a possible implementation, before obtaining a plurality of metrics and a profile of the media asset, the obtaining module 1701 is further configured to:

receive a trustworthiness evaluation request for the media content.

[00372] In a possible implementation, the media content is at least one of an image, a video, or an audio.

[00373] In addition, an embodiment of this application further provides a data processing apparatus. The apparatus includes the following modules.

[00374] An obtaining module 1701 is configured to obtain a media asset, where the media asset includes media content, and at least one of metadata corresponding to the media content and a trust record corresponding to the media content.

[00375] For specific descriptions of the obtainingmodule 1701, refer to the descriptions of step 1601 in the foregoing embodiment. Details are not described herein again.

[00376] A processing module 1702 is configured to determine one or more trust indicators of the media asset, where the one or more trust indicators are used to evaluate a trustworthiness level of the media asset.

[00377] For specific descriptions of the processing module 1702, refer to the descriptions of step 1602 in the foregoing embodiment. Details are not described herein again.

[00378] In a possible implementation, the one or more trust indicators are encapsulated in a trust credential.

[00379] In a possible implementation, the one or more trust indicators are determined based on at least one of the media content, the metadata corresponding to the media content, and the trust record corresponding to the media content.

[00380] In a possible implementation, the one or more trust indicators are used to determine trustworthiness information of the media asset, and the trustworthiness information indicates

whether the one or more trust indicators satisfy a metric.

[00381] In a possible implementation, the metric includes data indicating a trust indicator that the media asset needs to satisfy.

[00382] In a possible implementation, the trust indicator includes a parameter indicating the trustworthiness level of the media asset.

[00383] In a possible implementation, the media content is at least one of an image, a video, or an audio.

[00384] The following describes an execution device provided in an embodiment of this application. FIG. 18 is a diagram of a structure of an execution device according to an embodiment of this application. The execution device 1800 may be specifically represented as a mobile phone, a tablet computer, a notebook computer, a smart wearable device, or the like. This is not limited herein. Specifically, the execution device 1800 includes a receiver 1801, a transmitter 1802, a processor 1803, and a memory 1804 (the execution device 1800 may include one or more processors 1803, and one processor is used as an example in FIG. 18). The processor 1803 may include an application processor 18031 and a communication processor 18032. In some embodiments of this application, the receiver 1801, the transmitter 1802, the processor 1803, and the memory 1804 may be connected through a bus or in another manner.

[00385] The memory 1804 may include a read-only memory and a random access memory, and provide instructions and data to the processor 1803. A part of the memory 1804 may further include a non-volatile random access memory (non-volatile random access memory, NVRAM). The memory 1804 stores a processor and operation instructions, an executable module or a data structure, a subset thereof, or an extended set thereof. The operation instructions may include various operation instructions for implementing various operations.

[00386] The processor 1803 controls an operation of the execution device. In a specific application, the components of the execution device are coupled together through a bus system. In addition to a data bus, the bus system may further include a power bus, a control bus, a status signal bus, and the like. However, for clear description, various types of buses in the figure are referred to as the bus system.

[00387] The methods disclosed in the foregoing embodiments of this application may be applied to the processor 1803, or implemented by the processor 1803. The processor 1803 may be an integrated circuit chip with a signal processing capability. In an implementation process, the steps of the foregoing methods may be completed by a hardware integrated logic circuit in the processor 1803 or through instructions in a form of software. The processor 1803 may be a general-purpose processor, a digital signal processor (digital signal processor, DSP), a microprocessor, or a microcontroller; or may further include an application-specific integrated circuit (application-

specific integrated circuit, ASIC), a field-programmable gate array (field-programmable gate array, FPGA) or another programmable logic device, a discrete gate or transistor logic device, or a discrete hardware component. The processor 1803 may implement or perform the methods, steps, and logical block diagrams disclosed in embodiments of this application. The general-purpose processor may be a microprocessor, or the processor may be any conventional processor or the like. The steps in the methods disclosed with reference to embodiments of this application may be directly performed and completed by a hardware decoding processor, or may be performed and completed by using a combination of hardware in the decoding processor and a software module. A software module may be located in a mature storage medium in the art, such as a random access memory, a flash memory, a read-only memory, a programmable read-only memory, an electrically erasable programmable memory, or a register. The storage medium is located in the memory 1804. The processor 1803 reads information in the memory 1804 and completes the steps in the foregoing methods in combination with hardware of the processor 1803.

[00388] The receiver 1801 may be configured to receive input digit or character information, and generate a signal input related to a related setting and function control of the execution device. The transmitter 1802 may be configured to output digit or character information. The transmitter 1802 may be further configured to send instructions to a disk group, to modify data in the disk group.

[00389] In this embodiment of this application, in one case, the processor 1803 is configured to perform the steps of the data processing methods in the embodiments corresponding to FIG. 6 to FIG. 16A-2.

[00390] An embodiment of this application further provides a server. FIG. 19 is a diagram of a structure of a server according to an embodiment of this application. Specifically, a server 1900 is implemented by one or more servers. The server 1900 may greatly differ due to different configurations or performance, and may include one or more central processing units (central processing units, CPUs) 1919 (for example, one or more processors) and a memory 1932, one or more storage media 1930 (for example, one or more mass storage devices) that store an application 1942 or data 1944. The memory 1932 and the storage medium 1930 may be used for temporary storage or persistent storage. A program stored in the storage medium 1930 may include one or more modules (not shown in the figure), and each module may include a series of instruction operations for the server. Further, the central processing unit 1919 may be configured to: communicate with the storage medium 1930, and perform, on the server 1900, the series of instruction operations in the storage medium 1930.

[00391] The server 1900 may further include one or more power supplies 1920, one or more wired or wireless network interfaces 1950, one or more input/output interfaces 1958, or one or

more operating systems 1941, for example, Windows Server™, Mac OS X™, Unix™, Linux™, and FreeBSD™.

[00392] In this embodiment of this application, the central processing unit 1919 is configured to perform the steps of the data processing methods in the embodiments corresponding to FIG. 6 to FIG. 16A-2.

[00393] An embodiment of this application further provides a computer program product including computer-readable instructions. When the computer-readable instructions are run on a computer, the computer is enabled to perform steps performed by the execution device, or the computer is enabled to perform steps performed by the training device.

[00394] An embodiment of this application further provides a computer-readable storage medium. The computer-readable storage medium stores a program for processing a signal, and when the program is run on a computer, the computer is enabled to perform steps performed by the execution device, or the computer is enabled to perform steps performed by the training device.

[00395] In addition, it should be noted that the described apparatus embodiments are merely examples. The units described as separate parts may or may not be physically separate, and parts displayed as units may or may not be physical units, may be located in one position, or may be distributed on a plurality of network units. Some or all of the modules may be selected according to actual needs to achieve the objectives of the solutions of embodiments. In addition, in the accompanying drawings of the apparatus embodiments provided in this application, connection relationships between modules indicate that the modules are in a communication connection with each other, which may be specifically implemented as one or more communication buses or signal cables.

[00396] Based on the descriptions of the foregoing implementations, a person skilled in the art may clearly understand that this application may be implemented by software in addition to necessary universal hardware, or by dedicated hardware, including a dedicated integrated circuit, a dedicated CPU, a dedicated memory, a dedicated component, and the like. Generally, any functions that can be performed by a computer program can be easily implemented by using corresponding hardware. Moreover, a specific hardware structure used to achieve a same function may be in various forms, for example, in a form of analog circuit, digital circuit, or dedicated circuit. However, as for this application, software program implementation is a better implementation in most cases. Based on such an understanding, the technical solutions of this application essentially or the part contributing to the prior art may be implemented in a form of software product. The computer software product is stored in a readable storage medium, such as a floppy disk, a USB flash drive, a removable hard disk, a ROM, a RAM, a magnetic disk, or an optical disc of a computer, and includes several instructions for instructing a computer device

(which may be a personal computer, a training device, a network device, or the like) to perform the methods in embodiments of this application.

[00397] All or some of the foregoing embodiments may be implemented by using software, hardware, firmware, or any combination thereof. When software is used to implement the embodiments, all or a part of the embodiments may be implemented in a form of computer program product.

[00398] The computer program product includes one or more computer instructions. When the computer program instructions are loaded and executed on the computer, all or some of the procedures or functions according to embodiments of this application are generated. The computer may be a general-purpose computer, a dedicated computer, a computer network, or another programmable apparatus. The computer instructions may be stored in a computer-readable storage medium, or may be transmitted from a computer-readable storage medium to another computer-readable storage medium. For example, the computer instructions may be transmitted from a website, a computer, a training device, or a data center to another website, computer, training device, or data center in a wired (for example, a coaxial cable, an optical fiber, or a digital subscriber line (DSL)) or wireless (for example, infrared, radio, or microwave) manner. The computer-readable storage medium may be any usable medium accessible by a computer, or a data storage device, for example, a training device or a data center, integrating one or more usable media. The usable medium may be a magnetic medium (for example, a floppy disk, a hard disk, or a magnetic tape), an optical medium (for example, a DVD), a semiconductor medium (for example, a solid-state disk (Solid-State Disk, SSD)), or the like.

CLAIMS

1. A data processing method, wherein the method comprises:

obtaining a media asset, wherein the media asset comprises media content, and the media asset further comprises at least one of metadata of the media content and a trust record of the media content; and

determining one or more trust indicators of the media asset, wherein the one or more trust indicators are used to evaluate a trustworthiness level of the media asset.

2. The method according to claim 1, further comprising:

obtaining a trust credential based on the one or more trust indicators of the media asset, wherein the one or more trust indicators are encapsulated in the trust credential.

3. The method according to claim 1 or 2, wherein the one or more trust indicators are determined based on at least one of the media content, the metadata of the media content, and the trust record of the media content.

4. The method according to any one of claims 1 to 3, wherein the one or more trust indicators are used to determine trustworthiness information of the media asset, and the trustworthiness information indicates whether the one or more trust indicators satisfy a metric.

5. The method according to any one of claims 1 to 4, wherein the metric comprises data indicating a trust indicator that the media asset needs to satisfy.

6. The method according to any one of claims 1 to 5, wherein the trust indicator comprises a parameter indicating the trustworthiness level of the media asset.

7. The method according to any one of claims 1 to 6, wherein the media content is at least one of an image, a video, or an audio.

8. The method according to any one of claims 1 to 7, wherein when the media content is first media content, the trust record of the media content comprises initial information of the first media content, a hard binding of the first media content, and a first digital signature; the first digital signature is a digital signature of first data; and the first data is data determined based on at least the initial information and the hard binding of the first media content.

9. The method according to any one of claims 1 to 8, wherein the initial information comprises at least one of the following: generation time of the first media content, an author name of the first media content, a digital content identifier of the first media content, a generation location of the first media content, information about a generation device of the first media content, a resolution of the first media content, a size of the first media content, a media type of the first media content, copyright information of the first media content, or a generation manner of the first media content.

10. A data processing system, comprising:

a first device, configured to obtain a media asset;

a second device, configured to determine one or more trust indicators of the media asset; and

a third device, configured to: obtain trust configuration information, and determine whether the one or more trust indicators of the media asset satisfy a metric in the trust configuration information.

11. The data processing system according to claim 10, wherein the second device is further configured to obtain a trust credential based on the one or more trust indicators of the media asset.

12. The data processing system according to claim 10, wherein the third device is further configured to generate a trust report based on a result of whether the one or more trust indicators of the media asset satisfy the metric in the trust configuration information.

13. A data processing apparatus, wherein the apparatus comprises:

an obtaining module, configured to obtain a media asset, wherein the media asset comprises media content, and the media asset further comprises at least one of metadata of the media content and a trust record of the media content; and

a processing module, configured to determine one or more trust indicators of the media asset, wherein the one or more trust indicators are used to evaluate a trustworthiness level of the media asset.

14. A data processing apparatus, wherein the apparatus comprises a memory and a processor, the memory stores code, and the processor is configured to obtain the code and perform the method according to any one of claims 1 to 9.

15. A computer-readable storage medium, comprising computer-readable instructions, wherein when the computer-readable instructions are run on a computer device, the computer device is enabled to perform the method according to any one of claims 1 to 9.

16. A chip, comprising a processor, wherein the processor is configured to support a data processing apparatus to implement the method according to any one of claims 1 to 9.