

一种数据处理方法及相关设备

本申请要求于 2023 年 8 月 22 日提交国家知识产权局、申请号为 202311063709.1、申请名称为“一种数据处理方法及相关设备”的中国专利申请的优先权,其全部内容通过引用结合在本申请中。

技术领域

本申请涉及终端及媒体应用领域,尤其涉及一种数据处理方法及相关设备。

背景技术

随着手机等更加方便的拍照设备的普及,以及各种简单高效、功能强大的内容编辑软件(例如,AIGC 类软件)的发展,人们进行媒体创作和修改的门槛越来越低,并且可以在各类社交软件上发布。但是,对媒体内容的修改加剧了一些错误信息和虚假信息的传播,破坏了媒体内容作为信息载体的可信性,尤其是随着 AI 技术的发展,产生的虚假内容与真实内容肉眼已经很难分辨,眼见不一定为“实”。因此,能够帮助人们更加有效判断内容的可信度的技术至关重要。

以媒体内容为图像为例,在现有的实现中,为了检测媒体内容的是否包括虚假内容,可以通过大量的真实图像集和虚假图像集训练 AI 检测模型,检测模型检测输入图像中是否含有与虚假图像相似的特征,以判断图像是否可信。但是这种 AI 检测模型只能针对部分特定的虚假内容进行可信度的证明。

因此,亟需一种能够为媒体内容提供可信度证明的方法。

发明内容

第一方面,本申请提供了一种数据处理方法,该方法包括:通过对媒体资产的一个或多个信任因子判定是否对应的指标要求,来得到媒体资产的可信信息,用户可以基于可信信息判断出媒体资产的可信度。其中,所述媒体资产包括媒体内容,所述媒体资产还包括媒体内容的元数据以及媒体内容的信任记录中的至少一种;信任因子为指示媒体资产的可信度的参数。

在一种可能的实现中,该方法还包括生成所述媒体资产的可信信息。

在一种可能的实现中,可信信息可以封装为信任报告。

在一种可能的实现中,所述一个或多个信任因子是根据所述媒体内容、媒体内容对应的元数据以及媒体内容对应的信任记录中的至少一种确定的。例如,可以是媒体内容、媒体内容对应的元数据以及媒体内容对应的信任记录中提取的特征,也可以是对媒体内容、媒体内容对应的元数据以及媒体内容对应的信任记录中做过一定处理后得到的数据。

在一种可能的实现中,所述可信信息用于指示所述一个或多个信任因子是否满足指标,所述信任因子包括指示媒体资产的可信度的参数。以媒体内容为图像为例,可以选择元数据中的拍摄时间、拍摄地点、拍摄者、相机镜头参数、拍摄参数等特征作为元数据的信任因子。

以媒体内容为图像为例,可以选择信任记录中的图像生成方式、图像编辑方式等作为信任记录的信任因子,图像生成方式可以但不限于包括:是否是通过 AIGC 生成的、是否是通过相机生成的、是否是通过软件辅助生成的,是否是通过合成媒体生成的,媒体内容是否可被用来训练模型,图像编辑方式可以但不限于包括:旋转,resize,剪切,内容的编辑等。

以媒体内容为图像为例,可以选择媒体内容中的人物、场景、物体类型、物体之间的位置关系、图像风格(例如,色彩、光线、明度)等特征作为媒体内容的信任因子。

在一种可能的实现中,信任因子对应的指标为配置文件中规定的,可以获取第一信任配置信息,所述第一信任配置信息包括媒体资产需满足的指标。

在一种可能的实现中,可以根据该媒体内容、媒体内容对应的元数据以及媒体内容对应的信任记录中的至少一种,确定该媒体资产的一个或多个信任因子。

在一种可能的实现中,该一个或多个信任因子可以封装在信任凭据中。

在一种可能的实现中,该方法还包括:将该通过确定每个该信任因子是否满足指标得到的可信信息,

添加至该信任记录。

通过将这个新生成的可信信息添加到该媒体资产的信任记录中，可以进一步增强媒体资产的可信性。

5 在一种可能的实现中，所述确定所述一个或多个信任因子是否满足指标包括：确定所述指标中的信任因子是否包括在所述一个或多个信任因子中，或者确定所述一个或多个信任因子中是否包括所述指标中的信任因子。

也就是说，指标也可以包括信任因子，可以将媒体资产的信任因子是否在指标中有所包含（也就是指标是否包含媒体资产的信任因子），来确定媒体资产的信任因子是否满足指标。

在一种可能的实现中，该信任记录包括信任清单；所述将所述可信信息添加至所述信任记录，包括：将所述可信信息添加至所述信任清单。

10 在一种可能的实现中，该方法还包括：将该可信信息的哈希值和签名添加至该信任清单。

在一种可能的实现中，该方法还包括：获取该媒体资产的指示信息；该该添加至该信任记录，包括：根据该指示信息，将该可信信息添加至该指示信息指示的媒体资产对应的该信任记录。当需要批量处理多个媒体资产的可信信息时，可以在过程中传输媒体资产的指示信息。

在一种可能的实现中，该方法还包括：根据该可信信息，生成与该媒体资产相关联的文件。

15 在一种可能的实现中，所述第一信任配置信息包括多个信任配置信息中的一个，不同的信任配置信息指示不同地区或用户对所述媒体资产需满足指标的要求。针对于不同的场景（例如地区或者用户）可以对不同地区的要求，产生不同的可信信息，从而可以满足不同场景的可信评估需求。

在一种可能的实现中，所述获取媒体资产的一个或多个信任因子的动作为基于硬件传感器采集到所述媒体内容、或者生成软件生成所述媒体内容触发。

20 例如，可以通过自身携带的摄像头采集图像，或者是通过媒体内容编辑软件（例如通过 AIGC）生成新的媒体内容。终端设备在获取到媒体内容时还需要通过媒体资产管理模块生成对应的媒体资产，媒体资产可以包括元数据、信任记录等。在本申请实施例中，媒体资产管理模块可以基于硬件传感器采集到该媒体内容、或者生成软件生成该媒体内容，根据媒体资产中的内容生成可信信息并增加到媒体资产中。

25 在一种可能的实现中，该获取媒体资产的一个或多个信任因子之前，该方法还包括：接收到针对于该媒体内容的可信评估请求。

例如，用户可以通过可信评估应用程序来输入针对于该媒体内容的可信评估请求。

例如，端侧可以通过用于提供可信评估服务的云服务的接口来输入针对于该媒体内容的可信评估请求。

30 在一种可能的实现中，该媒体内容为图像、视频或者音频中的至少一种。

第二方面，本申请提供了一种数据处理方法，所述方法包括：获取媒体资产；所述媒体资产包括媒体内容，所述媒体资产还包括媒体内容的元数据以及媒体内容的信任记录中的至少一种；确定所述媒体资产的一个或多个信任因子，所述一个或多个信任因子用于评估所述媒体资产的可信度。

35 由此，通过可信因子的提取，可以用于媒体资产可信度的评估；后期在进行可信度评估时，不再再去对媒体资产进行读取，只需从可信因子中读取信息进行媒体资产可信度的评估。

在一种可能的实现中，所述一个或多个信任因子封装在信任凭据中。

在一种可能的实现中，所述一个或多个信任因子是根据所述媒体内容、媒体内容对应的元数据以及媒体内容对应的信任记录中的至少一种确定的。

40 在一种可能的实现中，可以根据媒体内容的元数据确定出和媒体资产的可信度相关的一个或多个信任因子 TM。例如，TM 可以是媒体内容的生成时间、媒体内容的作者名称、媒体内容的数字内容标识、媒体内容的生成地点、媒体内容的生成设备的信息、媒体内容的媒体类型或媒体内容的生成方式（Media Type）。例如，媒体内容的生成设备的信息可以包括设备的型号、相机的参数等，相机的参数可以包括相机拍摄图片时的焦距、感光度、曝光度等。应该理解的是，TM 还可以包括其它信息例如版权信息等用于描述媒体内容的信息，本申请对此不作限制。

45 在一种可能的实现中，可以根据媒体内容的信任记录确定出和媒体资产的可信度相关的一个或多个信任因子 TR。例如，可以选择信任记录中的媒体内容的生成时间、媒体内容的作者名称、媒体内容的

数字内容标识、媒体内容的生成地点、媒体内容的生成设备的信息、媒体编辑方式、媒体内容的媒体类型或媒体内容的生成方式 (Media Type)。例如, 媒体内容的生成设备的信息可以包括设备的型号、相机的参数等, 相机的参数可以包括相机拍摄图片时的焦距、感光度、曝光度等。应该理解的是, TR 还可以包括其它信息例如版权信息等用于描述媒体内容的信息, 本申请对此不作限制。媒体生成方式可以但不

5 限于包括: 是否是通过 AIGC 生成的、是否是通过相机生成的、是否是通过软件辅助生成的, 是否是通过合成媒体生成的, 媒体内容是否可被用来训练模型, 媒体编辑方式可以但不限于包括: 旋转, resize, 剪切, 内容的编辑等。TR 还可以包括媒体声明可以包括缩略图、是否可以被修改, 操作权限、使用权限、第二媒体内容的来源等。

在一种可能的实现中, 可以根据媒体内容确定出和媒体资产的可信度相关的一个或多个信任因子

10 TC。例如, 可以选择媒体内容中的人物、场景、物体类型、物体之间的位置关系、媒体风格 (例如, 色彩、光线、明度) 等特征作为媒体内容的信任因子。

在一种可能的实现中, 所述一个或多个信任因子用于确定媒体资产的可信信息, 所述可信信息用于指示所述一个或多个信任因子是否满足指标。

在一种可能的实现中, 所述指标包括指示所述媒体资产需满足的信任因子的数据。以指标指示创作者为例, 指标可以是创作者, 也可是创作者的名字; 以指标指示媒体生成地点为例, 指标可以是地点, 也可以是地点的名称; 在此不进行枚举。

15

在一种可能的实现中, 所述信任因子包括指示媒体资产的可信度的参数。

在一种可能的实现中, 所述媒体内容为图像、视频或者音频中的至少一种。

第三方面, 本申请提供了一种数据处理方法, 所述方法包括: 获取第一媒体内容; 生成第一媒体内容的修改记录, 第一媒体内容的信任记录包括: 第一媒体内容的初始信息、第一媒体内容的硬绑定和第一数字签名; 第一数字签名是第一数据的数字签名, 第一数据是至少根据所述初始信息和所述第一媒体内容的硬绑定确定的数据。信任记录可以用于媒体内容的溯源, 能够一定程度帮助用户判断媒体内容的真实性。

20

在一种可能的实现中, 第一数据是至少由第一媒体内容的硬绑定和第一媒体内容的初始信息组合后的数据, 或者, 第一数据是至少由初始信息的硬绑定 (例如, AI 生成 AIGC 的哈希值 AIGC.Hash, 媒体生成方式的哈希值 Media Type.Hash) 和第一媒体硬绑定的硬绑定 (例如, 第一媒体哈希值的哈希值 Media Hash 0.Hash) 组合后的数据。

25

在一种可能的实现中, 第一数据也可作为第一组合哈希值 (Hash(TD)), 第一组合哈希值包括第一媒体内容的初始信息和第一媒体哈希值组合后的哈希值。示例性地, 第一组合哈希值包括第一媒体内容的初始信息、第一媒体哈希值和其它描述性信息组合后的哈希值, 其它描述性信息可以不是初始信息中的其他描述性信息, 例如, 生成 Trust Profile 的工具的信息或者其它描述第一媒体内容的初始信息的信息。

30

在一种可能的实现中, 第一数据也可作为第一组合哈希值, 第一组合哈希值可以包括第一媒体内容的初始信息的哈希值和第一媒体哈希值的哈希值 (Media Hash 0. Hash) 组合后的哈希值。示例性地, 第一组合哈希值是第一媒体内容的初始信息的哈希值、第一媒体哈希值的哈希值和其它元数据信息的哈希值组合后的哈希值。这里, 在第一媒体内容的初始信息包括至少两个的情况下, 第一媒体内容的初始信息的哈希值可以包括第一媒体内容的初始信息中的每一个的哈希值, 或者, 第一媒体内容的初始信息的哈希值可以包括第一媒体内容的所有初始信息组合后的哈希值。

35

在一种可能的实现中, 媒体内容的初始信息可以是指媒体内容生成时产生的信息。示例性地, 媒体内容的初始信息包括以下至少一种: 媒体内容的生成时间、媒体内容的作者名称、媒体内容的数字内容标识、媒体内容的生成地点、媒体内容的生成设备的信息、媒体内容的分辨率、媒体内容的大小、媒体内容的媒体类型或媒体内容的生成方式 (Media Type)。例如, 媒体内容的生成设备的信息可以包括设备的型号、相机的参数等, 相机的参数可以包括相机拍摄图片时的焦距、感光度、曝光度等。应该理解的是, 媒体内容的初始信息还可以包括其它信息例如版权信息等用于描述媒体内容的信息。

40

在一种可能的实现中, 媒体类型可以包括但不限于: 图像类、视频类、音频类以及图形类等。生成方式可以包括: AI 生成方式和非 AI 生成方式等。一种可能的方式中, 初始信息中的生成方式可以采用 AI 生成 (AIGC) 标识替换; 例如, 当媒体内容是由 AI 生成时, AIGC 标识的值为 1; 当媒体内容不是

45

由 AI 生成时, AIGC 标识的值为 0。媒体内容的作者名称可以是媒体内容的创作者的名称或者媒体内容的拍摄设备名称。

第四方面, 本申请提供了一种数据处理装置, 该装置包括:

获取模块, 用于获取媒体资产的一个或多个信任因子; 所述媒体资产包括媒体内容, 所述媒体资产还包括媒体内容的元数据以及媒体内容的信任记录中的至少一种;

处理模块, 用于确定所述一个或多个信任因子是否满足指标。

在一种可能的实现中, 所述获取模块, 还用于:

获取第一信任配置信息, 所述第一信任配置信息包括媒体资产需满足的指标。

在一种可能的实现中, 所述一个或多个信任因子是根据所述媒体内容、媒体内容对应的元数据以及媒体内容对应的信任记录中的至少一种确定的。

在一种可能的实现中, 所述一个或多个信任因子封装在信任凭据中。

在一种可能的实现中, 所述指标包括指示所述媒体资产需满足的信任因子的数据。

在一种可能的实现中, 所述处理模块, 具体用于:

确定所述指标中对应的信任因子是否包括在所述一个或多个信任因子中, 或者确定所述一个或多个信任因子中是否包括所述指标中对应的信任因子。

在一种可能的实现中, 所述处理模块, 还用于:

生成所述媒体资产的可信信息, 所述可信信息用于指示所述一个或多个信任因子是否满足指标, 所述信任因子包括指示媒体资产的可信度的参数。在一种可能的实现中, 所述处理模块, 还用于:

将所述可信信息添加至所述信任记录。

在一种可能的实现中, 所述信任记录包括信任清单;

所述处理模块, 具体用于:

将所述可信信息, 添加至所述信任清单。

在一种可能的实现中, 所述获取模块, 还用于:

获取所述媒体资产的指示信息;

所述处理模块, 具体用于:

根据所述指示信息, 将所述可信信息添加至所述指示信息指示的媒体资产对应的所述信任记录。

在一种可能的实现中, 所述可信信息封装在信任报告中。

在一种可能的实现中, 所述处理模块, 还用于:

根据所述可信信息, 生成与所述媒体资产相关联的文件。

在一种可能的实现中, 所述第一信任配置信息包括多个信任配置信息中的一个, 不同的信任配置信息指示不同地区或用户对所述媒体资产需满足指标的要求。

在一种可能的实现中, 所述获取媒体资产的一个或多个信任因子的动作为基于硬件传感器采集到所述媒体内容、或者生成软件生成所述媒体内容触发。

在一种可能的实现中, 所述获取媒体资产的多个指标以及配置文件之前, 所述获取模块, 还用于:

接收到针对于所述媒体内容的可信评估请求。

在一种可能的实现中, 所述媒体内容为图像、视频或者音频中的至少一种。

第五方面, 本申请提供了一种数据处理装置, 所述装置包括:

获取模块, 用于获取媒体资产; 所述媒体资产包括媒体内容, 所述媒体资产还包括媒体内容的元数据以及媒体内容的信任记录中的至少一种;

处理模块, 用于确定所述媒体资产的一个或多个信任因子, 所述一个或多个信任因子用于评估所述媒体资产的可信度。

在一种可能的实现中, 所述一个或多个信任因子封装在信任凭据中。

在一种可能的实现中, 所述一个或多个信任因子是根据所述媒体内容、媒体内容对应的元数据以及媒体内容对应的信任记录中的至少一种确定的。

在一种可能的实现中, 所述一个或多个信任因子用于确定媒体资产的可信信息, 所述可信信息用于指示所述一个或多个信任因子是否满足指标。

在一种可能的实现中，所述指标包括所述媒体资产需满足的信任因子。
在一种可能的实现中，所述信任因子包括指示媒体资产的可信度的参数。
在一种可能的实现中，所述媒体内容为图像、视频或者音频中的至少一种。

第六方面，本申请实施例提供了一种数据处理装置，所述装置包括：

5 获取模块，用于获取第一媒体内容；
处理模块，用于生成第一媒体内容的修改记录，第一媒体内容的信任记录包括：第一媒体内容的初始信息、第一媒体内容的硬绑定和第一数字签名；第一数字签名是第一数据的数字签名，第一数据是至少根据所述初始信息和所述第一媒体内容的硬绑定确定的数据。

第七方面，本申请的实施例提供一种数据处理系统，包括：

10 第一设备，用于获取媒体资产；
第二设备，用于根据媒体资产获取所述媒体资产的一个或多个信任因子；第一设备和第二设备可以是相同或者不同的设备；

第三设备，用于获取根据媒体资产的一个或多个信任因子和信任配置信息生成信任报告。在一种可能的实现中，媒体资产的一个或多个信任因子记录到信任凭据中。在一种可能的实现中，第二设备响应于第三设备的请求，将所述媒体资产的一个或多个信任因子发送给第三设备。信任配置信息可以记录在信任配置文件中，在一种可能的实现中，第三设备可以从信任配置文件库中获取信任配置文件；在一种可能的实现中，第三设备可以直接读取本地存储器中的信任配置文件。

第八方面，本申请实施例提供了一种数据处理装置，可以包括存储器、处理器以及总线系统，其中，存储器用于存储程序，处理器用于执行存储器中的程序，以执行如上述第一方面及其任一可选的方法，
20 上述第二方面及其任一可选的方法，以及上述第三方面及其任一可选的方法。

第九方面，本申请实施例提供了一种计算机可读存储介质，计算机可读存储介质中存储有计算机程序，当其在计算机上运行时，使得计算机执行上述第一方面及其任一可选的方法，上述第二方面及其任一可选的方法，以及上述第三方面及其任一可选的方法。

第十方面，本申请实施例提供了一种包括指令的计算机程序产品，当其在计算机上运行时，使得计算机执行上述第一方面及其任一可选的方法，上述第二方面及其任一可选的方法，以及上述第三方面及其任一可选的方法。

第十一方面，本申请提供了一种芯片系统，该芯片系统包括处理器，用于支持数据处理装置实现上述方面中所涉及的部分或全部功能，例如，发送或处理上述方法中所涉及的数据；或，信息。在一种可能的设计中，芯片系统还包括存储器，存储器，用于保存数据处理装置必要的程序指令和数据。该芯片系统，可以由芯片构成，也可以包括芯片和其他分立器件。

附图说明

图 1 为一种应用场景示意；
图 2 为一种终端设备的结构示意；
35 图 3 为一种服务器的结构示意；
图 4 为一种云服务示意；
图 5 为一种应用架构示意；
图 6A 为一种信任记录的框架示意；
图 6B 为一种数据处理方法的流程示意；
40 图 7 为一种可信信息的生成示意；
图 8 为一种可信信息的生成示意；
图 9 为一种数据处理方法的流程示意；
图 10 为一种数据处理方法的流程示意；
图 11 为一种数据处理方法的流程示意；
45 图 12 为一种数据处理方法的流程示意；
图 13 为一种数据处理方法的流程示意；

图 14 为一种数据处理方法的流程示意；
图 15 为一种数据处理方法的流程示意；
图 16A 为一种数据处理方法的流程示意；
图 16B 为一种数据处理方法的流程示意；
图 16C 为一种数据处理方法的流程示意；
图 17 为一种数据处理装置的结构示意；
图 18 为一种数据处理装置的结构示意；
图 19 为一种服务器的结构示意。

具体实施方式

下面结合本发明实施例中的附图对本发明实施例进行描述。本发明的实施方式部分使用的术语仅用于对本发明的具体实施例进行解释，而非旨在限定本发明。

下面结合附图，对本申请的实施例进行描述。本领域普通技术人员可知，随着技术的发展和场景的出现，本申请实施例提供的技术方案对于类似的技术问题，同样适用。

本申请的说明书和权利要求书及上述附图中的术语“第一”、“第二”等是用于区别类似的对象，而不必用于描述特定的顺序或先后次序。应该理解这样使用的术语在适当情况下可以互换，这仅仅是描述本申请的实施例中具有相同属性的对象在描述时所采用的区分方式。此外，术语“包括”和“具有”以及他们的任何变形，意图在于覆盖不排他的包含，以便包含一系列单元的过程、方法、系统、产品或设备不限于那些单元，而是可包括没有清楚地列出的或对于这些过程、方法、产品或设备固有的其它单元。

本文中所用用语“基本(substantially)”、“大约(about)”及类似用语用作近似用语、而并非用作程度用语，且旨在考虑到所属领域中的普通技术人员将知的测量值或计算值的固有偏差。此外，在阐述本发明实施例时使用“可(may)”是指“可能的一个或多个实施例”。本文中所用用语“使用(use)”、“正使用(using)”、“及“被使用(used)”可被视为分别与用语“利用(utilize)”、“正利用(utilizing)”、“及“被利用(utilized)”同义。另外，用语“示例性(exemplary)”旨在指代实例或例示。

首先介绍本申请的应用场景。

本申请可以给用户提供用于作为媒体资产的可信度的判断依据的可信信息（或者可以称之为信任报告）。

在一种场景中，本申请实施例可以应用于提供媒体资产的可信信息的应用程序。

在一种场景中，本申请实施例可以应用于提供媒体资产的可信信息的云服务。

在一种场景中，本申请实施例可以应用于媒体资产管理模块，该模块可以生成媒体资产的可信信息，且利用该可信信息更新媒体资产中的信任记录，或者根据该可信信息生成媒体资产的关联文件，来帮助用户对媒体资产进行可信度判断。

本申请可以给用户提供用于作为媒体资产的可信度的判断依据的信任因子（或者可以称之为信任凭据）。

在一种场景中，本申请实施例可以应用于提供信任凭据的应用程序。

在一种场景中，本申请实施例可以应用于提供信任凭据的云服务。

在一种场景中，本申请实施例可以应用于媒体资产管理模块，该模块可以生成媒体资产的信任凭据，且利用该信任凭据更新媒体资产中的信任记录，或者根据该信任凭据生成媒体资产的关联文件，来帮助用户对媒体资产进行可信度判断。

接下来分别对上述几个应用场景进行介绍：

场景 1. 应用程序。

在一种场景中，本申请实施例的形态为用于提供媒体资产的可信信息或者信任凭据的应用程序（本申请实施例可以简称为可信判断类应用程序）。

本申请实施例的产品形态可以为可信判断类应用程序。可信判断类应用程序可以运行在终端设备或者云侧的服务器上。

在一种可能的实现中，可信判断类应用程序可以响应于输入的媒体内容或者媒体资产的指示信息，向用户呈现媒体资产的可信信息或者信任凭据。

图 1 为示例性示出的应用场景示意图。

当用户需要判断该媒体内容的可信度时，可以打开终端设备中的媒体可信平台客户端（如应用程序、小程序、网页等）进行查询。

示例性地，用户 A 的手机 A 接收到用户 B 的手机 B 发送的媒体内容后，若用户 A 需要使用该媒体内容（如转发）时，可以先对该媒体内容进行可信度判断。在确定媒体内容的可信度后，再确定是否使用该媒体内容。

应该理解的是，手机 A 也可以是其他运算能力较强的电子设备，如个人计算机、计算机工作站、平板电脑等等，本申请对此不作限制。

示例性地，当用户需要判断智能手表中媒体内容的可信度时，可以将智能手表中的媒体内容发送给手机，由手机对该媒体内容进行可信度判断，然后发送可信信息给智能手表。

应该理解的是，智能手表也可以是其他运算能力较弱的电子设备如媒体消费设备、可穿戴设备、机顶盒、游戏机等，本申请对此不作限制。手机也可以是其他运算能力较强的电子设备，如个人计算机、计算机工作站、平板电脑等等，本申请对此不作限制。

参照图 1 中的 (1)，媒体可信平台的主界面 101 可以包括一个或多个控件，包括但不限于：输入框、可信度判断按钮等等，本申请对此不作限制。

示例性地，用户可以点击输入框，媒体可信平台可以响应于用户的操作行为，展示文件选择界面。接着，用户在文件选择界面中选取对应的媒体内容后，可以点击主界面 101 中的可信信息生成按钮；对应的，媒体可信平台可以响应于用户的操作行为，获取媒体资产的可信信息。

示例性地，媒体可信平台可以显示可信信息。例如，本申请实施例中，可信信息可以包括针对于媒体内容的媒体资产的至少一个信任因子是否满足预配置文件中的指标要求。

参照图 1 中的 (2)，图 1 中的 (2) 中显示的验证结果 102 包括媒体内容在信任因子 T1、T3、T4 和 Tn 上对于预配置文件中规定的指标要求的满足性，例如，信任因子 T1 满足指标要求，信任因子 T2 满足指标要求，信任因子 T3 不满足指标要求，信任因子 T4 满足指标要求。

一种可能的方式中，可以由媒体可信平台的客户端执行媒体资产的可信信息的识别。例如，当待识别的媒体资产为一个时，媒体可信平台的客户端可以在本地进行识别。

一种可能的方式中，可以由媒体可信平台的服务器端执行媒体资产的可信信息的识别。例如，当待识别的媒体资产为多个时，媒体可信平台的客户端可以将多个待识别的媒体资产发送给媒体可信平台的服务器端，由媒体可信平台的服务器端执行媒体资产的可信信息的识别，并将识别的可信信息返回给媒体可信平台的客户端。

需要说明的是，本申请中是由媒体可信平台的客户端执行媒体资产的可信信息的识别，还是由媒体可信平台的服务器端执行媒体资产的可信信息的识别，不受待识别的媒体内容的数量的限制。

应理解，图 1 对应的场景描述还可以适用于信任凭据的生成，相似之处这里不再赘述。

接下来描述在媒体可信平台位于终端侧时，终端 100 的产品形态；

本申请实施例中的终端 100 可以为手机、平板电脑、可穿戴设备、车载设备、增强现实(augmented reality, AR)/虚拟现实(virtual reality, VR)设备、笔记本电脑、超级移动个人计算机(ultra-mobile personal computer, UMPC)、上网本、个人数字助理(personal digital assistant, PDA)等，本申请实施例对此不作任何限制。

图 2 示出了终端 100 的一种可选的硬件结构示意图。

参考图 2 所示，终端 100 可以包括射频单元 110、存储器 120、输入单元 130、显示单元 140、摄像头 150（可选的）、音频电路 160（可选的）、扬声器 161（可选的）、麦克风 162（可选的）、处理器 170、外部接口 180、电源 190 等部件。本领域技术人员可以理解，图 2 仅仅是终端或多功能设备的举例，并不构成对终端或多功能设备的限定，可以包括比图示更多或更少的部件，或者组合某些部件，或者不同的部件。

输入单元 130 可用于接收输入的数字或字符信息，以及产生与该便携式多功能装置的用户设置以及

功能控制有关的键信号输入。具体地,输入单元 130 可包括触摸屏 131(可选的)和/或其他输入设备 132。该触摸屏 131 可收集用户在其上或附近的触摸操作(比如用户使用手指、关节、触笔等任何适合的物体在触摸屏上或在触摸屏附近的操作),并根据预先设定的程序驱动相应的连接装置。触摸屏可以检测用户对触摸屏的触摸动作,将该触摸动作转换为触摸信号发送给该处理器 170,并能接收该处理器 170 发来的命令并加以执行;该触摸信号至少包括触点坐标信息。该触摸屏 131 可以提供该终端 100 和用户之间的输入界面和输出界面。此外,可以采用电阻式、电容式、红外线以及表面声波等多种类型实现触摸屏。除了触摸屏 131,输入单元 130 还可以包括其他输入设备 132。具体地,其他输入设备 132 可以包括但不限于物理键盘、功能键(比如音量控制按键、开关按键等)、轨迹球、鼠标、操作杆等中的一种或多种。

其中,其他输入设备 132 可以接收到指定进行可信度判断的媒体资产。

该显示单元 140 可用于显示由用户输入的信息或提供给用户的信息、终端 100 的各种菜单、交互界面、文件显示和/或任意一种多媒体文件的播放。在本申请实施例中,显示单元 140 可用于显示可信信息(例如信任报告)等。

该存储器 120 可用于存储指令和数据,存储器 120 可主要包括存储指令区和存储数据区,存储数据区可存储各种数据,如多媒体文件、文本等;存储指令区可存储操作系统、应用、至少一个功能所需的指令等软件单元,或者他们的子集、扩展集。还可以包括非易失性随机存储器;向处理器 170 提供包括管理计算处理设备中的硬件、软件以及数据资源,支持控制软件和应用。还用于多媒体文件的存储,以及运行程序和应用的存储。

处理器 170 是终端 100 的控制中心,利用各种接口和线路连接整个终端 100 的各个部分,通过运行或执行存储在存储器 120 内的指令以及调用存储在存储器 120 内的数据,执行终端 100 的各种功能和处理数据,从而对终端设备进行整体控制。可选的,处理器 170 可包括一个或多个处理单元;优选的,处理器 170 可集成应用处理器和调制解调处理器,其中,应用处理器主要处理操作系统、用户界面和应用程序等,调制解调处理器主要处理无线通信。可以理解的是,上述调制解调处理器也可以不集成到处理器 170 中。在一些实施例中,处理器、存储器、可以在单一芯片上实现,在一些实施例中,他们也可以在独立的芯片上分别实现。处理器 170 还可以用于产生相应的操作控制信号,发给计算处理设备相应的部件,读取以及处理软件中的数据,尤其是读取和处理存储器 120 中的数据和程序,以使其中的各个功能模块执行相应的功能,从而控制相应的部件按指令的要求进行动作。

其中,存储器 120 可以用于存储数据处理方法相关的软件代码,处理器 170 可以执行芯片的数据处理方法的步骤,也可以调度其他单元(例如上述输入单元 130 以及显示单元 140)以实现相应的功能。

该射频单元 110(可选的)可用于收发信息或通话过程中信号的接收和发送,例如,将基站的下行信息接收后,给处理器 170 处理;另外,将设计上的数据发送给基站。通常,RF 电路包括但不限于天线、至少一个放大器、收发信机、耦合器、低噪声放大器(Low Noise Amplifier, LNA)、双工器等。此外,射频单元 110 还可以通过无线通信与网络设备和其他设备通信。该无线通信可以使用任一通信标准或协议,包括但不限于全球移动通讯系统(Global System of Mobile communication, GSM)、通用分组无线服务(General Packet Radio Service, GPRS)、码分多址(Code Division Multiple Access, CDMA)、宽带码分多址(Wideband Code Division Multiple Access, WCDMA)、长期演进(Long Term Evolution, LTE)、电子邮件、短消息服务(Short Messaging Service, SMS)等。

其中,在本申请实施例中,该射频单元 110 可以将媒体内容发送至服务器 200,并接收到服务器 200 发送的可信信息。

应理解,该射频单元 110 为可选的,其可以被替换为其他通信接口,例如可以是网口。

终端 100 还包括给各个部件供电的电源 190(比如电池),优选的,电源可以通过电源管理系统与处理器 170 逻辑相连,从而通过电源管理系统实现管理充电、放电、以及功耗管理等功能。

终端 100 还包括外部接口 180,该外部接口可以是标准的 Micro USB 接口,也可以使多针连接器,可以用于连接终端 100 与其他装置进行通信,也可以用于连接充电器为终端 100 充电。

尽管未示出,终端 100 还可以包括闪光灯、无线保真(wireless fidelity, WiFi)模块、蓝牙模块、不同功能的传感器等,在此不再赘述。下文中描述的部分或全部方法均可以应用在如图 2 所示的终端 100 中。

接下来描述在媒体可信平台位于服务器侧时，服务器 200 的产品形态；

图 3 提供了一种服务器 200 的结构示意图，如图 3 所示，服务器 200 包括总线 201、处理器 202、通信接口 203 和存储器 204。处理器 202、存储器 204 和通信接口 203 之间通过总线 201 通信。

总线 201 可以是外设部件互连标准（peripheral component interconnect, PCI）总线或扩展工业标准结构（extended industry standard architecture, EISA）总线等。总线可以分为地址总线、数据总线、控制总线等。为便于表示，图 3 中仅用一条粗线表示，但并不表示仅有一根总线或一种类型的总线。

处理器 202 可以为中央处理器（central processing unit, CPU）、图形处理器（graphics processing unit, GPU）、微处理器（micro processor, MP）或者数字信号处理器（digital signal processor, DSP）等处理器中的任意一种或多种。

存储器 204 可以包括易失性存储器（volatile memory），例如随机存取存储器（random access memory, RAM）。存储器 204 还可以包括非易失性存储器（non-volatile memory），例如只读存储器（read-only memory, ROM）、快闪存储器、机械硬盘（hard drive drive, HDD）或固态硬盘（solid state drive, SSD）。

其中，存储器 204 可以用于存储数据处理方法相关的软件代码，处理器 202 可以执行芯片的数据处理方法的步骤，也可以调度其他单元以实现相应的功能。

应理解，上述终端 100 和服务器 200 可以为集中式或者是分布式的设备，上述终端 100 和服务器 200 中的处理器（例如处理器 170 以及处理器 202）可以为硬件电路（如专用集成电路（application specific integrated circuit, ASIC）、现场可编程门阵列（field-programmable gate array, FPGA）、通用处理器、数字信号处理器（digital signal processing, DSP）、微处理器或微控制器等等）、或这些硬件电路的组合，例如，处理器可以为具有执行指令功能的硬件系统，如 CPU、DSP 等，或者为不具有执行指令功能的硬件系统，如 ASIC、FPGA 等，或者为上述不具有执行指令功能的硬件系统以及具有执行指令功能的硬件系统的组合。

场景 2. 云服务。

在一种场景中，本申请实施例的形态为用于提供媒体资产的可信信息或者信任凭据的云服务。

在一种可能的实现中，服务器可以通过应用程序编程接口（application programming interface, API）为端侧提供媒体资产的可信信息或者信任凭据的查询服务的服务。

其中，终端设备可以通过云端提供的 API，将相关参数（例如媒体资产等数据）发送至服务器，服务器可以基于接收到的参数，得到处理结果（例如可信信息或者信任凭据等），并将处理结果返回至终端。

关于终端以及服务器的描述可以上述实施例的描述，这里不再赘述。

如图 4 示出了使用一项云平台提供的可信度判断功能类云服务的流程。

1. 开通并购买内容审核服务。

2. 用户可以下载内容审核服务对应的软件开发工具包（software development kit, SDK），通常云平台提供多个开发版本的 SDK，供用户根据开发环境的需求选择，例如 JAVA 版本的 SDK、python 版本的 SDK、PHP 版本的 SDK、Android 版本的 SDK 等。

3. 用户根据需求下载对应版本的 SDK 到本地后，将 SDK 工程导入至本地开发环境，在本地开发环境中进行配置和调试，本地开发环境还可以进行其他功能的开发，使得形成一个集合了可信度判断类能力的应用。

4. 可信度判断类应用在被使用的过程中，当需要进行可信度判断功能时，可以触发可信度判断功能的 API 调用。当应用触发可信度判断功能时，发起 API 请求至云环境中的可信度判断类服务的运行实例，其中，API 请求中携带媒体内容，由云环境中的运行实例对媒体内容进行处理，获得可信信息。

5. 云环境将可信信息返回至应用，由此完成一次的可信度判断功能的调用。

场景 3. 媒体资产管理模块。

在本场景中，终端设备自身可以采集或者生成媒体内容，例如，可以通过自身携带的摄像头采集图像，或者是通过媒体内容编辑软件（例如通过 AIGC）生成新的媒体内容。

终端设备在获取到媒体内容时还需要通过媒体资产管理模块生成对应的媒体资产，媒体资产可以包括元数据、信任记录等。

本场景中，媒体资产管理模块可以根据媒体资产中的内容生成可信信息并增加到媒体资产中，或者将该可信信息作为和媒体资产相关联的文件。

图 5 以框图形式示出了媒体资产管理模块所在的终端设备 101 的一个结构示意图。

根据本申请中描述的一个或多个实施方案，终端设备 101 可以包括用于执行媒体项目（例如，媒体资产）管理的电子部件。客户端设备 101 可容纳在单个计算系统（诸如台式计算机系统、膝上型计算机系统、平板电脑系统、服务器计算机系统、移动电话、媒体播放器、个人数字助理、个人通信器、游戏设备、网络路由器或集线器、无线接入点(AP)或中继器、机顶盒或它们的组合)中。终端设备 101 中的部件可在空间上分离并且通过通信技术连接的单独计算系统上实现。

对于一个实施方案，客户端设备 101 中的一个或多个部件可被实现为一个或多个集成电路(IC)。例如，处理单元 104、媒体内容捕获设备 102、外围设备 118、传感器 122 或存储器 110 中的至少一者可被实现为片上系统(SoC)IC、三维(3D)IC、任何其他已知的 IC 或任何已知 IC 的组合。对于另一个实施方案，客户端设备 101 中的两个或更多个部件一起被实现为一个或多个 IC。例如，处理单元 104、媒体内容捕获设备 102、外围设备 118、传感器 122 或存储器 110 中的至少两者可被一起实现为 SoC IC。下文描述了客户端设备 101 的每个部件。

终端设备 101 可包括媒体内容捕获设备 102(例如，用于捕获图像的成像设备、用于捕获声音的音频设备、用于捕获音频和视频的多媒体设备、任何其他已知的用户媒体内容捕获设备等)。对于一个实施方案，媒体内容捕获设备 102 还可包括被实现为硬件、软件或它们的组合的信号处理流水线。信号处理流水线可对从设备 102 中的一个或多个部件接收的数据执行一个或多个操作。信号处理流水线还可向存储器 110、外围设备 118(如下文进一步所讨论的)和/或处理单元 104 提供经处理的数据。

终端设备 101 可包括处理单元 104，诸如 CPU、GPU、其他集成电路(IC)、存储器和/或其他电子电路。对于一个实施方案，处理单元 104 可以通过媒体资产管理模块 106 来生成与媒体内容 114 相关联的媒体资产 111。在一些实现中，处理单元 104 可以根据媒体资产中的内容生成可信信息并增加到媒体资产中，或者将该可信信息作为和媒体资产相关联的文件（例如图 5 所示的信任报告 121）。

终端设备 101 还可包括外围设备 118。对于一个实施方案，外围设备 118 可包括以下中的至少一者：(i)与客户端设备 101 中的一个或多个部件(例如，鼠标、键盘等)进行交互或向其发送数据的一个或多个输入设备；(ii)从客户端设备 101 中的一个或多个部件(例如，监视器、打印机、显示设备等)提供输出的一个或多个输出设备；或(iii)除存储器 110 之外还存储数据的一个或多个存储设备。外围设备 118 以虚线框示出，以示出其为客户设备 101 的任选部件。外围设备 118 还可指既可用作输入设备又可用作输出设备(例如，触摸屏等)的单个部件或设备。客户端设备 101 可包括用于外围设备 118 的至少一个外围控制电路(未示出)。外围控制电路可以为控制器(例如，芯片、扩展卡或独立设备等)，该控制器与外围设备 118 交互并用于指示由该外围设备执行的操作。外围设备控制器可以为单独的处理单元或集成在处理单元 104 中。外围设备 118 在整个本文档中也可称为输入/输出(I/O)设备 118。

终端设备 101 还可包括一个或多个传感器 122，该一个或多个传感器以虚线框示出，以示出传感器可为客户端设备 101 的任选部件。对于一个实施方案，传感器 122 可以检测一个或多个环境的特性。传感器的示例包括但不限于：光传感器、成像传感器、加速度计、声音传感器、气压传感器、接近传感器、振动传感器、陀螺仪传感器、罗盘、气压计、热传感器、旋转传感器、速度传感器和倾斜仪。

结合图 4 和图 10，本实施例中提供一种信任评估系统，包括：

第一设备，用于获取媒体资产；

第二设备，用于根据媒体资产获取所述媒体资产的一个或多个信任因子；第一设备和第二设备可以是相同或者不同的设备；

第三设备，用于获取根据媒体资产的一个或多个信任因子和信任配置信息生成信任报告。在一种可能的实现中，媒体资产的一个或多个信任因子记录到信任凭据中。在一种可能的实现中，第二设备响应于第三设备的请求，将所述媒体资产的一个或多个信任因子发送给第三设备。信任配置信息可以记录在信任配置文件中，在一种可能的实现中，第三设备可以从信任配置文件库中获取信任配置文件；在一种可能的实现中，第三设备可以直接读取本地存储器中的信任配置文件。

参照图 6A 所示，图 6A 是媒体资产的信任记录的框架，

示例性地,如图 7 所示,媒体资产可以包括媒体内容(Media Content)、媒体内容的元数据(Metadata)和媒体内容的信任记录。其中,媒体内容的元数据、信任记录与媒体内容是绑定的,或者说媒体内容的元数据、信任记录与媒体内容是关联的)。

在获取该媒体内容的媒体资产的情况下,对应的,也获取到了该媒体内容的元数据和信任记录。例如,获取图象,可以获取到数字形式的图象、图象的元数据和信任记录。

需要说明的是,部分场景中,媒体资产也被称为媒体文件或数字资产(Media Asset)。

媒体内容可以是图像、音频、视频或者文本。

媒体资产可以包括信任记录(Trust record),在一种实现中,信任记录可以作为元数据的一部分,在一种实现中,信任记录可以和元数据相互独立存在于媒体资产中。示例性地,媒体内容,也可以称为数字内容(Digital content)。媒体内容可以是媒体资产的一部分,表示媒体的实际内容,数字内容是以数字形式存在的文本、图像、声音等不同内容类型的内容,它可以存储在如光盘、硬盘等数字载体上,并通过网络等手段传播。数字内容是将图像、文字、影音等内容通过数字技术进行整合应用的产品或服务的总体,是数字媒体技术与文化创意结合的产物。例如,媒体内容可以是图像的像素数据,以及理解或呈现内容所需的任何附加技术元数据(例如,颜色配置文件或编码参数)。

数字技术(Digital Technology),是一项与电子计算机相伴相生的科学技术,它是指借助一定的设备将各种信息,包括:图、文、声、像等,转化为电子计算机能识别的二进制数字“0”和“1”后进行运算、加工、存储、传送、传播、还原的技术。由于在运算、存储等环节中要借助计算机对信息进行编码、压缩、解码等,因此也称为数码技术、计算机数字技术等。数字技术也称数字控制技术。

示例性地,元数据可以包括用于描述媒体数据的数据,元数据可以记载有关媒体资产或媒体内容的非技术信息;例如,元数据可以包括描述媒体内容属性(property)的信息。其中,示例性地,元数据可以为信任档案(或称为信任清单(Trust Manifest))。示例性地,元数据可以是媒体内容的创作位置、创建者、注释或 IPR 信息。

示例性地,如图 8 所示,媒体内容的信任记录可以是媒体内容的一种元数据(或者不属于元数据而是和元数据相互独立且属于媒体资产),信任记录中记录了媒体内容生成以及变迁的相关信息,可以用于媒体内容的溯源。

在一种实施例中,如图 6A 所示,信任记录可以包括信任声明和信任清单。

示例性地,信任声明(Trust declaration)可以一种信任清单,可以位于信任记录的第一位。信任声明也可以是媒体内容的一种元数据。

在一种可能的实现中,其中信任记录中的信任声明(Trust declaration)可以包括:第一媒体内容的初始信息、第一媒体内容的硬绑定(Hard binding)和第一数字签名 Signaturesk0;所述第一数字签名是第一数据的数字签名,所述第一数据是至少根据初始信息和第一媒体内容的硬绑定确定的数据。

第一媒体内容可以是以数字形式存在的文本、图象、声音等不同内容类型的内容,例如,第一媒体内容可以是图象的像素数据,以及理解或呈现内容所需的任何附加技术元数据(例如,颜色配置文件或编码参数)。

硬绑定指的是对原始数据进行硬绑定处理后得到的数据,硬绑定处理为使原始数据不被伪造的处理方法,无法通过对原始数据的硬绑定进行逆向处理得到原始数据。通过对原始数据进行硬绑定处理,得到原始数据的硬绑定。例如,采用单向函数对原始数据进行处理。例如,哈希处理可以是硬绑定处理的一种,也就是说,硬绑定可以包括哈希值,第一媒体内容的硬绑定也可以包括第一媒体哈希值,第一媒体哈希值(Media Hash 0)是第一媒体内容的哈希值。

示例性地,第一数据是至少由第一媒体内容的硬绑定和第一媒体内容的初始信息组合后的数据,或者,第一数据是至少由初始信息的硬绑定(例如,AI 生成 AIGC 的哈希值 AIGC.Hash,媒体生成方式的哈希值 Media Type.Hash)和第一媒体硬绑定的硬绑定(例如,第一媒体哈希值的哈希值 Media Hash 0.Hash)组合后的数据。

示例性地,第一数据也可第一组合哈希值(Hash(TD)),第一组合哈希值包括第一媒体内容的初始信息和第一媒体哈希值组合后的哈希值。示例性地,第一组合哈希值包括第一媒体内容的初始信息、第一媒体哈希值和其它描述性信息组合后的哈希值,其它描述性信息可以不是初始信息中的其他描述性

信息,例如,生成 Trust Profile 的工具的信息或者其它描述第一媒体内容的初始信息的信息,本申请对此不作限制。

示例性地,第一数据也可作为第一组合哈希值,第一组合哈希值可以包括第一媒体内容的初始信息的哈希值和第一媒体哈希值的哈希值(Media Hash 0.Hash)组合后的哈希值。示例性地,第一组合哈希值是5 第一媒体内容的初始信息的哈希值、第一媒体哈希值的哈希值和其它元数据信息的哈希值组合后的哈希值。这里,在第一媒体内容的初始信息包括至少两个的情况下,第一媒体内容的初始信息的哈希值可以包括第一媒体内容的初始信息中的每一个的哈希值,或者,第一媒体内容的初始信息的哈希值可以包括第一媒体内容的所有初始信息组合后的哈希值。

示例性地,媒体内容的初始信息可以是指媒体内容生成时产生的信息。示例性地,媒体内容的初始10 信息包括以下至少一种:媒体内容的生成时间、媒体内容的作者名称、媒体内容的数字内容标识、媒体内容的生成地点、媒体内容的生成设备的信息、媒体内容的分辨率、媒体内容的大小、媒体内容的媒体类型或媒体内容的生成方式(Media Type)。例如,媒体内容的生成设备的信息可以包括设备的型号、相机的参数等,相机的参数可以包括相机拍摄图片时的焦距、感光度、曝光度等。应该理解的是,媒体内容的初始信息还可以包括其它信息例如版权信息等用于描述媒体内容的信息,本申请对此不作限制。

示例性地,媒体类型可以包括但不限于:图像类、视频类、音频类以及图形类等。生成方式可以包括:15 AI生成方式和非AI生成方式等。一种可能的方式中,初始信息中的生成方式可以采用AI生成(AIGC)标识替换;例如,当媒体内容是由AI生成时,AIGC标识的值为1;当媒体内容不是由AI生成时,AIGC标识的值为0。媒体内容的作者名称可以是媒体内容的创作者的名称或者媒体内容的拍摄设备名称,本申请对此不作限制。

第一数据的数字签名通常采用私钥对第一数据进行数字签名,得到第一数据的数字签名。

示例性地,私钥可以是电子设备或者用户的私钥。示例性地,可以基于数字签名算法,采用私钥对20 第一数据进行数字签名,得到第一数据的数字签名。应该理解的是,本申请对数字签名算法不作限制。

示例性地,信任清单(trust manifest)记载指示媒体资产来源的信息。信任清单是信任记录的一部分。信任清单也可以是一种元数据。

示例性地,信任清单可以包括第N+1媒体内容的硬绑定(例如,第二媒体哈希值Media hash1)。示25 例性地,可以将根据编辑操作对第N媒体内容进行编辑处理之后得到的媒体内容,或者,对第N媒体内容的元数据进行修改后得到的媒体内容,或者,待转发(或分享)的第N媒体内容,称为N+1媒体内容。

示例性地,信任清单可以还包括媒体声明Assertion,媒体声明可以包括版权信息,缩略图、是否可30 以被修改,操作权限、使用权限、第二媒体内容的来源等。

示例性地,信任清单可以还包括第二数字签名Signaturesk1,第二数字签名是第二数据的数字签名,第二数据可以是至少基于第二媒体哈希值和修改声明确定的数据。

示例性地,第二数据是至少由第N+1媒体哈希值和第N+1声明组合后的数据,或者,第一数据是至少由第N+1声明的哈希值(Assertion Hash)和第N+1媒体哈希值的哈希值组合后的数据。

示例性地,第二数据也可作为第N+1组合哈希值,第N+1组合哈希值包括第N+1声明和第N+1媒体35 哈希值的哈希值组合后的哈希值。示例性地,第N+1组合哈希值包括第N+1声明、第N+1媒体哈希值的哈希值组合后的哈希值和其它描述性信息组合后的哈希值,其它描述性信息可以不是第N+1声明中的其他描述性信息,例如,生成Trust Manifest的工具的信息或者其它描述第N+1声明的信息,本申请对此不作限制。

示例性地,第二数据也可作为第N+1组合哈希值,第N+1组合哈希值可以包括第N+1声明的哈希值40 和第N+1媒体哈希值的哈希值(例如,第二媒体哈希值Media Hash 1.Hash)组合后的哈希值。示例性地,第N+1组合哈希值是第N+1声明的哈希值、第N+1媒体哈希值的哈希值和其它元数据信息(Other Information)的哈希值组合后的哈希值。

示例性地,信任清单还可以包括第一统一资源标识符(URI, Uniform Resource Identifier),第一URI45 指示第一媒体内容的初始信息或第一媒体内容的硬绑定在第一媒体内容的修改记录中的位置。例如,URI1指示第一媒体内容的硬绑定在第一媒体内容的信任记录中的位置,URI2指示Media Type在第一媒

体内容的信任记录中的位置，URI3 指示 AIGC 在第一媒体内容的信任记录中的位置，URI4 指示第 N+1 媒体内容（例如，第二媒体哈希值 Media Hash 1）在信任记录中的位置，URI5 指示媒体声明 Assertion 在信任记录中的位置。

示例性地，修改记录还可以包括其它信息，其它信息可以是不用于证实媒体内容的真实性的信息。

5 例如：文件名、哈希算法的名称，哈希算法用于计算得到上述实施例中提到的哈希值。

下面对本申请实施例的方法流程举例说明。

参照图 6B，图 6B 为本申请实施例提供的一种数据处理方法的流程示意，该流程主要描述可信信息的生成过程，如图 6B 所示，本申请实施例提供的一种数据处理方法包括：

601、获取媒体资产的一个或多个信任因子；所述媒体资产包括媒体内容，所述媒体资产还包括媒体内容的元数据以及媒体内容的信任记录中的至少一种。

10 示例性地，信任因子（trust indicators）是指示媒体资产的可信度的参数。在一种可能的实现中，媒体资产的信任因子可以从信任凭据中获取，也就是说，媒体资产的信任因子封装在信任凭据中；在一种可能的实现中，信任因子可以从媒体资产获取，直接从媒体资产中读取对应的信任因子。在一种可能的实现中，所述媒体资产包括媒体内容、媒体内容对应的元数据以及媒体内容对应的信任记录中的至少一种。本申请实施例中，为了能够让用户可以判断出媒体资产的可信度，可以根据媒体资产确定出和媒体资产的可信度相关的一个或多个信任因子，基于对信任因子的校验结果，用户可以分析判断出媒体资产的可信度。

20 在一种可能的实现中，如图 8 所示，媒体资产可以包括媒体内容、媒体内容的元数据。其中，媒体内容的元数据与媒体内容是绑定的，或者说媒体内容的元数据与媒体内容是关联的。元数据可以包括信任记录，或者元数据可以不包括信任记录，信任记录和元数据可以为媒体资产中不同的部分。也就是说，如图 8 所示，媒体资产可以包括媒体内容以及媒体内容对应的元数据（信任记录封装在元数据中），如图 7 所示，媒体资产也可以包括媒体内容、媒体内容对应的元数据以及媒体内容对应的信任记录。

25 在一种可能的实现中，信任记录进一步可以分为信任声明（trust declaration）和若干信任清单（trust manifests）。信任清单（trust manifests）是媒体资产溯源信息的集合，而信任声明（trust declaration）是一种特殊类型的信任清单，它只包含强制断言（强制存在的溯源信息）。信任声明（trust declaration）可以出现在信任记录（trust record）中的第一位。

30 在一种可能的实现中，可以根据媒体资产确定出和媒体资产的可信度相关的一个或多个信任因子。具体地，如图 7 所示，可以根据媒体内容、媒体内容对应的元数据以及媒体内容对应的信任记录中的至少一种确定出和媒体资产的可信度相关的一个或多个信任因子。如图 8 所示，可以根据媒体内容和媒体内容对应的元数据（信任记录是元数据的一部分）中的至少一种确定出和媒体资产的可信度相关的一个或多个信任因子。

35 例如，媒体资产的信任因子可以是媒体内容、媒体内容对应的元数据以及媒体内容对应的信任记录中提取的特征，也可以是对媒体内容、媒体内容对应的元数据以及媒体内容对应的信任记录中的特征做过一定处理后得到的数据。

40 例如，可以根据媒体内容的元数据确定出和媒体资产的可信度相关的一个或多个信任因子 TM。例如，TM 可以是媒体内容的生成时间、媒体内容的作者名称、媒体内容的数字内容标识、媒体内容的生成地点、媒体内容的生成设备的信息、媒体内容的媒体类型或媒体内容的生成方式（Media Type）。例如，媒体内容的生成设备的信息可以包括设备的型号、相机的参数等，相机的参数可以包括相机拍摄图片时的焦距、感光度、曝光度等。应该理解的是，TM 还可以包括其它信息例如版权信息等用于描述媒体内容的信息，本申请对此不作限制。

例如，可以根据媒体内容的元数据以及媒体内容的信任记录确定出和媒体资产的可信度相关的一个或多个信任因子。

例如，可以根据媒体内容的元数据、媒体内容以及媒体内容的信任记录确定出和媒体资产的可信度相关的一个或多个信任因子。

45 例如，可以根据媒体内容的信任记录确定出和媒体资产的可信度相关的一个或多个信任因子 TR。例如，可以选择信任记录中的媒体内容的生成时间、媒体内容的作者名称、媒体内容的数字内容标识、

媒体内容的生成地点、媒体内容的生成设备的信息、媒体编辑方式、媒体内容的媒体类型或媒体内容的生成方式 (Media Type)。例如, 媒体内容的生成设备的信息可以包括设备的型号、相机的参数等, 相机的参数可以包括相机拍摄图片时的焦距、感光度、曝光度等。应该理解的是, TR 还可以包括其它信息例如版权信息等用于描述媒体内容的信息, 本申请对此不作限制。媒体生成方式可以但不限于包括: 是否是通过 AIGC 生成的、是否是通过相机生成的、是否是通过软件辅助生成的, 是否是通过合成媒体生成的, 媒体内容是否可被用来训练模型, 媒体编辑方式可以但不限于包括: 旋转, resize, 剪切, 内容的编辑等。TR 还可以包括媒体声明可以包括缩略图、是否可以被修改, 操作权限、使用权限、第二媒体内容的来源等。

例如, 可以根据媒体内容以及媒体内容的信任记录确定出和媒体资产的可信度相关的一个或多个信任因子。

例如, 可以根据媒体内容确定出和媒体资产的可信度相关的一个或多个信任因子 TC。例如, 可以选择媒体内容中的人物、场景、物体类型、物体之间的位置关系、媒体风格 (例如, 色彩、光线、明度) 等特征作为媒体内容的信任因子。

例如, 可以根据媒体内容的元数据以及媒体内容确定出和媒体资产的可信度相关的一个或多个信任因子。

其中, 信任因子可以为媒体资产的一个特征描述。例如, 所述信任因子可以包括指示媒体资产的可信度的参数。

在一种可能的实现中, 信任凭据可以包括每个信任因子和对应的来源之间关系, 也就是信任因子对应于媒体资产的哪一部分 (元数据、信任列表还是媒体内容)。信任凭据 (trust credential) 是基于媒体资产得到的一个或多个信任因子。

在一种可能的实现中, 在获取到信任因子时, 可以将信任因子本身作为信任凭据。在一种可能的实现中, 在获取到多个信任因子时, 可对所有的信任因子进行封装, 得到信任凭据。在一种可能的实现中, 也可以将信任因子和其他的数据一起封装, 得到信任凭据。

在一种可能的实现中, 针对于获取到的媒体资产的一个或多个信任因子, 可以获取到对应的要求, 也就是在特定场景下对媒体资产的信任因子的评估约束, 评估约束可以认为是和媒体资产的可信度相关的约束。

本申请实施例, 对媒体资产的信任因子的评估约束可以通过配置文件来描述, 配置文件可以包括每个所述信任因子对应的指标要求。配置文件也可以称之为信任配置文件 (trust profile)。信任配置文件记载一组制定好的信任指标, 它可以被用来对某个特定的媒体资产的信任凭据进行评估。

602、确定所述一个或多个信任因子是否满足指标。

在一种实现中, 指标可以存储在存储器中, 在需要对媒体资产进行可信评估时, 获取媒体资产的一个或多个可信因子, 将指标对应的信任因子与媒体资产的一个或多个可信因子进行匹配, 以确定一个或多个信任因子是否满足指标。

在一种实现中, 信任配置文件中规定的每个指标针对于一个信任因子, 可以根据配置文件中规定的指标, 从媒体资产中获取对应的信任因子, 根据信任配置文件和媒体资产的一个或多个信任因子, 得到所述媒体资产的可信信息。

示例性地, 信任配置文件记载信任配置信息, 信任配置信息包括媒体资产需满足的指标。也可以说, 信任配置信息包括信任凭据需要满足的指标, 信任配置信息可以是一组信任因子, 用于对信任凭证进行评估, 指示媒体资产的可信度水平。

在一种实现中, 可以先获取到媒体资产的多个指标, 多个指标中可能包括除了配置文件中存在约束的指标之外的指标, 因此, 可以根据第一配置文件中规定的指标, 确定每个信任因子对指标的满足性, 得到所述媒体资产的可信信息。

在一种实现中, 指标可以是基于信任因子处理后得到的数据, 但是其可以指示对应的信任因子。也就是说, 指标可以是媒体资产的信任因子、信任因子的值或者对信任因子做过一定处理后得到的数据。

在一种实现中, 指标可以包括一个或多个信任因子, 可以通过确定所述指标中的信任因子是否包括

在媒体资产的一个或多个信任因子中来确定媒体资产的一个或多个信任因子是否满足指标。

在一种实现中，通过确定媒体资产的一个或多个信任因子中是否包括指标中的信任因子来确定媒体资产的一个或多个信任因子是否满足指标。也就是说，信任配置文件中包括的信任因子包含在媒体资产的信任因子中时，可以认为媒体资产的信任因子满足指标，或者说信任因子可以是媒体资产的元数据的内容、修改记录的内容，可以是媒体内容的特征。如图 7 所示，信任配置文件中的指标包括 TM1'、TR1'、TC1'和 TM11'，TM1'、TR1'、TC1'和 TM11'分别与信任因子 TM1、TR1、TC1 和 TM11 对应，例如，TM1 是广东省深圳市，TM1'可以是地点或者中国，那么 TM1 则满足指标。由于媒体资产的一个或多个信任因子不存在 TM11，那么 TM11 不满足对应的指标。也就是说，在媒体资产的一个或多个信任因子不存在信任配置信息中的指标所指示的信任因子时，媒体资产不满足信任配置信息的指标要求。在媒体资产的信任因子中包含了信任配置文件中包括的信任因子时，可以认为媒体资产的信任因子满足指标。

如图 8 所示，信任配置文件中的指标包括 TM1'、TM2'、TM3'和 TC1'，在信任凭据中存在对应的信任因子 TM1、TM2、TM3 和 TC1。也就是说，在媒体资产的一个或多个信任因子存在信任配置信息中的指标所指示的所有信任因子时，媒体资产满足信任配置信息的指标要求。

在一种实现中，指标可以包括判断条件，判断条件指示媒体资产的一个或多个信任因子中是否存在目标信任因子。可以根据确定一个或多个信任因子中是否满足判断条件来确定所述一个或多个信任因子是否满足指标。可信信息可以通过信任报告表示，以信任配置文件和信任凭据作为输入，生成并记录根据信任配置信息评估信任凭据的结果。这个评估是对给定媒体资产的可信程度的一种评估。该结果可以作为可信信息提供给用户。

随后，该可信信息可以用于生成新的信任清单（具体将在后续实施例中介绍），或者是作为媒体资产相关联的文件。

基于可信信息可以表示媒体资产的一个或多个信任因子在配置文件中的满足性，基于该可信信息，用户可以判断出媒体资产的可信度。

以上描述了图 6B 所示方法的基本流程，下面对图 6B 所示方法中一些步骤可能采用的具体实现方式举例说明。

在上述步骤 602 中，由于不同地区或者不同用户对于同一个媒体资产的指标要求可能不同，可以获取到多个配置文件，多个配置文件可以存储在配置文件中，每个配置文件为一个地区或者用户对于媒体资产的指标要求，因此，具体如何根据所述配置文件和信任因子得到所述媒体资产的可信信息，包括多种可能实现方式，下面结合实现方式 A 至 D 举例说明。

实现方式 A：对于信任配置文件仅存在一组指标。

针对于媒体资产的信任因子，可能仅存在一组指标，进而，可以基于唯一对应的指标要求计算媒体资产的信任因子是否满足该组指标，得到可信信息。

应理解，由于仅存在一组指标要求，因此在可信信息中可以不保存信任因子的指标和配置文件之间的关联关系，也就是不体现出是基于哪一个地区或者哪一个用户的指标要求得到的可信信息。

实现方式 B：对于信任因子存在多个信任配置文件，且针对于每个信任配置文件计算得到对应的可信信息。

由于不同的地区或者用户对于可信度的要求不同，每个信任配置文件包括一组指标，不同组的指标指示不同地区或用户对所述媒体资产需满足指标的要求，进而，可以计算信任因子对于多个指标要求的满足性，得到包括多个可信信息。

应理解，可以在可信信息中保存信任因子和对应的指标要求之间的关联关系，以便表达出该可信信息是针对于哪个地区或者用户的指标。

实现方式 C：对于存在多个信任配置文件的情况，且只对其中的部分（例如一个信任配置文件）计算对应的可信信息。

由于不同的地区或者用户对于可信度的要求不同，因针对于媒体资产的信任因子，可能存在多个指标要求（多个要求中不同的指标要求对应于不同的地区或者不同的用户），系统在计算可信信息时，用户可以指定计算媒体资产的信任因子对于哪一组或者多组指标要求的满足性。

应理解，可以在可信信息中保存媒体资产的信任因子和对应的指标要求之间的关联关系，以便表达出该可信信息是针对于哪个地区或者用户的指标要求。

本申请通过上述方式，针对于不同的场景（例如地区或者用户）可以对应不同的指标要求，产生不同的可信信息，从而可以满足不同场景的可信度判断需求。

实现方式D：信任因子可以存在多个信任配置信息，不同的信任配置信息指示不同地区或用户对所述媒体资产需满足指标的要求，多个信任配置信息可以存储于一个信任配置文件或者多个信任配置文件。可以根据第一配置信息和媒体资产的信任因子得到所述媒体资产的可信信息，第一配置信息是多个信任配置信息中的一个。

在得到可信信息之后，可以利用可信信息更新媒体资产。下面对利用可信信息更新媒体资产的一个具体实现方式进行说明。

参照图9，图9为本申请实施例一个数据处理方法的流程示意。

901、基于硬件传感器采集到所述媒体内容、或者生成软件生成所述媒体内容。

终端设备自身可以通过硬件传感器采集媒体内容，或者通过软件生成媒体内容，例如，可以通过自身携带的摄像头采集图像，或者通过媒体内容编辑软件（例如通过AIGC）生成新的媒体内容。

终端设备在获取到媒体内容时还需要通过媒体资产管理模块生成对应的媒体资产，媒体资产可以包括元数据、信任记录等。

在本申请实施例中，媒体资产管理模块可以基于硬件传感器采集到所述媒体内容、或者生成软件生成所述媒体内容，根据媒体资产中的内容生成可信信息并增加到媒体资产中。

应理解，步骤901可以理解为步骤902之前的动作，例如，步骤901可以为步骤902的触发条件（可选的，步骤901可以为步骤902的多个触发条件之一）。

902、获取媒体资产的一个或多个信任因子；所述媒体资产包括媒体内容，所述媒体资产还包括媒体内容的元数据以及媒体内容的信任记录中的至少一种。

关于步骤902的描述可以参照上述实施例中步骤601的介绍，相似之处这里不再赘述。

903、确定每个所述信任因子是否满足指标，得到可信信息。

关于步骤903的描述可以参照上述实施例中步骤602的介绍，相似之处这里不再赘述。

904、将所述可信信息添加至所述信任记录。

在将可信信息添加至信任记录中时，可以将可信信息添加至主张（assertions）中。

具体的，可以将可信信息进行签名后添加至主张（assertions）中。

例如，可以将一个媒体内容对应的可信信息进行签名后添加至主张中，并作为主张的其中一项。

例如，可以将可信信息中每条指标或者部分指标对应的满足性进行签名后添加至主张中，并作为主张的其中一项。

通过将这个新生成的可信信息添加到该媒体资产的信任记录中，可以进一步增强媒体资产的可信性。

此外，还可以将所述可信信息的哈希值添加至所述信任清单中的声明（claim）处。

此外，还可以将所述可信信息的签名添加至所述信任清单中的签名处。

在图6B的基础上，参照图10，图10为本申请实施例一个数据处理方法的流程示意，相比图6B，图10的流程图通过功能模块之间的关系描述了可信信息的生成以及媒体资产的更新过程，具体包括：

生成模块、提取模块、信任配置文件存储模块、验证模块。生成模块用来生成媒体资产，每个媒体资产由元数据、媒体内容和信任记录三个部分组成。提取模块会以媒体资产作为输入，从媒体资产的元数据、信任记录和媒体内容中提取信任指标，并根于提取的信任指标生成该媒体资产的信任凭据。信任配置文件存储模块负责存储信任配置文件，其中信任配置文件是由政府、平台、用户等对象针对特定场景的预定义好的。验证模块以信任凭据和信任配置文件作为输入，评估信任凭据中的信任指标是否满足这个预定义的信任配置文件。最终，根据该评估的结果生成信任报告。

在图6B的基础上，参照图11和图12，图11和图12为本申请实施例一个数据处理方法的流程示意，相比图6B，图11和图12的流程图通过功能模块之间的关系描述了可信信息的生成以及媒体资产的更新过程，图11和图12的不同之处在于，图11是由生成算法发起流程，图12是由验证算法发起流程。

其中，图 11 具体包括：

- 1. 生成算法用来生成媒体资产，每个所述媒体资产包括媒体内容，所述媒体资产还包括媒体内容的元数据以及媒体内容的信任记录中的至少一种。
- 2. 生成算法将媒体资产传递至提取算法。
- 5 3. 提取算法以媒体资产作为输入，从媒体资产的元数据、信任记录和媒体内容中提取信任指标，并根于提取的信任指标生成该媒体资产的信任凭据。
- 4. 提取算法将信任凭据传递至验证算法。
- 5. 验证算法触发验证过程。
- 6. 验证算法从可信文件存储侧中请求获取信任配置文件，信任配置文件是由政府、平台、用户等对象针对特定场景的预定义好的。
- 10 7. 可信文件存储侧将信任配置文件传递至验证算法。
- 8. 验证算法以信任凭据和信任配置文件作为输入，评估信任凭据中的信任指标是否满足这个预定义的信任配置文件，根据该评估的结果生成信任报告。
- 9. 验证算法利用信任报告生成新的信任清单。
- 15 10. 验证算法将信任清单交回生成算法。
- 11. 生成算法将通过将新的信任清单添加到信任记录中，来更新媒体资产。

其中，图 12 具体包括：

- 0. 生成算法用来生成媒体资产，每个媒体资产包括媒体内容，所述媒体资产还包括媒体内容的元数据以及媒体内容的信任记录中的至少一种；
- 20 1. 验证算法触发验证过程。
- 2. 验证算法从可信文件存储侧中请求获取信任配置文件，信任配置文件是由政府、平台、用户等对象针对特定场景的预定义好的。
- 3. 可信文件存储侧将信任配置文件传递至验证算法。
- 4. 验证算法向提取算法请求获取信任凭据。
- 25 5. 提取算法向生成算法请求获取媒体资产。
- 6. 生成算法将媒体资产传递至提取算法。
- 7. 提取算法以媒体资产作为输入，从媒体资产的元数据、信任记录和媒体内容中提取信任指标，并根于提取的信任指标生成该媒体资产的信任凭据。
- 8. 提取算法将信任凭据传递至验证算法。
- 30 9. 验证算法以信任凭据和信任配置文件作为输入，评估信任凭据中的信任指标是否满足这个预定义的信任配置文件，根据该评估的结果生成信任报告。
- 10. 验证算法利用信任报告生成新的信任清单。
- 11. 验证算法将信任清单交回生成算法。
- 12. 生成算法将通过将新的信任清单添加到信任记录中，来更新媒体资产。

35 在得到可信信息之后，可以利用可信信息生成和媒体资产相关联的文件，该文件可以被用户调用和查看，并作为可信度判断时的可信度判断依据。下面进行说明。

参照图 13，图 13 为本申请实施例一个数据处理方法的流程示意，包括：

- 1301、基于硬件传感器采集到所述媒体内容、或者生成软件生成所述媒体内容。
- 关于步骤 1301 的描述可以参照上述实施例中步骤 901 的介绍，相似之处这里不再赘述。
- 40 1302、获取媒体资产的一个或多个信任因子；所述媒体资产包括媒体内容，所述媒体资产还包括媒体内容的元数据以及媒体内容的信任记录中的至少一种；
- 关于步骤 1302 的描述可以参照上述实施例中步骤 902 的介绍，相似之处这里不再赘述。
- 1303、确定每个所述信任因子是否满足指标，得到可信信息。
- 关于步骤 1303 的描述可以参照上述实施例中步骤 903 的介绍，相似之处这里不再赘述。
- 45 1304、根据所述可信信息生成与所述媒体资产相关联的文件。
- 相关联的文件可以为单独封装的文件，该文件可以和媒体资产绑定，用户可以通过查看该文件来进

行媒体内容的可信度判定。

进行可信信息的生成的触发除了图 9 介绍的基于硬件传感器采集到所述媒体内容、或者生成软件生成所述媒体内容的自动触发之外，还可以是基于用户的主动触发。下面进行说明。

参照图 14，图 14 为本申请实施例一个数据处理方法的流程示意，包括：

5 1401、接收到针对于所述媒体资产的可信评估请求。

例如，用户可以通过可信度判断应用程序来输入针对于所述媒体内容的可信评估请求。

例如，端侧可以通过用于提供可信度判断服务的云服务的接口来输入针对于所述媒体内容的可信评估请求。

该请求中可以携带媒体资产。

10 1402、获取媒体资产的一个或多个信任因子；所述媒体资产包括媒体内容，所述媒体资产还包括媒体内容的元数据以及媒体内容的信任记录中的至少一种；

关于步骤 1402 的描述可以参照上述实施例中步骤 902 的介绍，相似之处这里不再赘述。

1403、确定每个所述信任因子是否满足指标，得到可信信息。

关于步骤 1403 的描述可以参照上述实施例中步骤 903 的介绍，相似之处这里不再赘述。

15 1404、向端侧发送所述可信信息。

上述实施例中介绍了针对于一个媒体资产的可信信息的生成过程，下面介绍多个媒体资产批量进行可信信息生成的过程，下面进行说明。

参照图 15，图 15 为本申请实施例一个数据处理方法的流程示意，包括：

1501、获取所述媒体资产的指示信息。

20 例如，该指示信息可以为媒体资产 ID。由于是多个媒体资产批量进行信任报告生成的过程，因此需要传输对应的媒体资产 ID。

1502、根据所述指示信息，获取指示信息指示的媒体资产的一个或多个信任因子；所述媒体资产包括媒体内容，所述媒体资产还包括媒体内容的元数据以及媒体内容的信任记录中的至少一种；

1503、确定每个所述信任因子是否满足指标，得到可信信息。

25 1504、根据所述指示信息，将所述可信信息添加至所述指示信息指示的媒体资产对应的所述信任记录。

在图 15 的基础上，参照图 16A，图 16A 为本申请实施例一个数据处理方法的流程示意，相比图 15，图 16A 的流程图通过功能模块之间的关系描述了批量进行可信信息的生成以及媒体资产的更新过程。

其中，图 16A 具体包括：

30 1. 生成算法用来生成媒体资产，每个所述媒体资产包括媒体内容，所述媒体资产还包括媒体内容的元数据以及媒体内容的信任记录中的至少一种。

2. 生成算法向提取算法发送生成信任凭据的请求（包括媒体资产的 ID 和对应的媒体资产）。

3. 提取算法以媒体资产作为输入，从每个媒体资产的元数据、信任记录和媒体内容中提取信任指标，并基于提取的信任指标生成每个媒体资产的信任凭据。

35 4. 提取算法用（媒体资产 ID，对应的信任凭据）的格式把信任凭据发送给验证算法。

5. 验证算法触发验证过程。

6. 验证算法从可信文件存储侧中请求获取信任配置文件，信任配置文件是由政府、平台、用户等对象针对特定场景的预定义好的。

7. 可信文件存储侧将信任配置文件传递至验证算法。

40 8. 验证算法以每一个媒体资产对应的信任凭据和信任配置文件作为输入，评估每一个媒体资产对应的信任凭据中的信任指标是否满足这个预定义的信任配置文件，根据该评估的结果生成信任报告。验证算法会根据该评估的结果为每一个媒体资产生成信任报告。

9. 验证算法利用信任报告为每个媒体资产生成新的信任清单。

10. 验证算法将这个信任清单用（媒体资产 ID，对应的新信任清单）的格式交回生成算法。

45 11. 生成算法将通过将新的信任清单添加到信任记录中，来更新媒体资产。

上述图 6B 至图 16A 介绍了可信信息的生成或者使用过程，接下来结合附图介绍信任凭据的生成以

及使用过程。

参照图 16B，图 16B 为本申请实施例提供的一种数据处理方法的流程示意，该流程主要描述可信信息的生成过程，如图 16B 所示，本申请实施例提供的一种数据处理方法包括：

1601、获取媒体资产；所述媒体资产包括媒体内容，所述媒体资产还包括媒体内容的元数据以及媒体内容的信任记录中的至少一种。

关于步骤 1601 的描述可以参照上述实施例中关于媒体资产的介绍，相似之处这里不再赘述。

1602、确定所述媒体资产的一个或多个信任因子，所述一个或多个信任因子用于评估所述媒体资产的可信度。

关于步骤 1602 的描述可以参照上述实施例中关于信任因子的介绍，相似之处这里不再赘述。

其中，信任因子可以封装在信任凭据中。

在一种可能的实现中，还可以将信任凭据添加至所述信任记录。

在一种可能的实现中，还可以根据信任凭据生成与所述媒体资产相关联的文件。

相关联的文件可以为单独封装的文件，该文件可以和媒体资产绑定，用户可以通过查看该文件来进行媒体内容的可信度判定。

如图 16C 所示，图 16C 是一种信任记录的生成方法的示意，结合图 6B，本实施例提供一种信任记录的生成方法。可选地，信任记录也可以是元数据。信任记录的生成方法包括：

S161：获取第一媒体内容；

示例性地，第一媒体内容可以是第一电子设备生成的媒体内容，也可以是第一电子设备从其他电子设备接收到的媒体内容。例如，第一媒体内容为图像，则第一媒体内容可以是第一电子设备拍摄的图像或截图或 AI 生成的图像等，本申请对第一电子设备生成图像的方式不作限制；也可以是第一电子设备从其他电子设备接收到的图像，本申请对此不作限制。

S162：生成第一媒体内容的修改记录，第一媒体内容的信任记录包括：第一媒体内容的初始信息、第一媒体内容的硬绑定和第一数字签名；第一数字签名是第一数据的数字签名，第一数据是至少根据所述初始信息和所述第一媒体内容的硬绑定确定的数据。

S161 和 S162 步骤中涉及到的技术术语与上述实施例中的术语解释一致，在此不再赘述。

参照图 17，图 17 为本申请实施例提供的一种数据处理装置的结构示意，其中，所述装置 1700，包括：

获取模块 1701，用于获取媒体资产的一个或多个信任因子；所述媒体资产包括媒体内容，所述媒体资产还包括媒体内容的元数据以及媒体内容的信任记录中的至少一种；

其中，关于获取模块 1701 的具体描述可以参照上述实施例中步骤 601 的描述，这里不再赘述。

处理模块 1702，用于根用于确定所述一个或多个信任因子是否满足指标。

其中，关于处理模块 1702 的具体描述可以参照上述实施例中步骤 602 的描述，这里不再赘述。

在一种可能的实现中，所述获取模块 1701，还用于：

获取第一信任配置信息，所述第一信任配置信息包括媒体资产需满足的指标。

在一种可能的实现中，所述一个或多个信任因子是根据所述媒体内容、媒体内容对应的元数据以及媒体内容对应的信任记录中的至少一种确定的。

在一种可能的实现中，所述一个或多个信任因子封装在信任凭据中。

在一种可能的实现中，所述指标包括所述媒体资产需满足的信任因子。

在一种可能的实现中，所述处理模块 1702，具体用于：

确定所述指标中的信任因子是否包括在所述一个或多个信任因子中，或者确定所述一个或多个信任因子中是否包括所述指标中的信任因子。

在一种可能的实现中，所述处理模块 1702，还用于：

生成所述媒体资产的可信信息，所述可信信息用于指示所述一个或多个信任因子是否满足指标，所述信任因子包括指示媒体资产的可信度的参数。在一种可能的实现中，所述处理模块 1702，还用于：

将所述可信信息添加至所述信任记录。

在一种可能的实现中，所述信任记录包括信任清单；

所述处理模块 1702，具体用于：
将所述可信信息，添加至所述信任清单。
在一种可能的实现中，所述获取模块 1701，还用于：
获取所述媒体资产的指示信息；
5 所述处理模块 1702，具体用于：
根据所述指示信息，将所述可信信息添加至所述指示信息指示的媒体资产对应的所述信任记录。
在一种可能的实现中，所述可信信息封装在信任报告中。
在一种可能的实现中，所述处理模块 1702，还用于：
根据所述可信信息，生成与所述媒体资产相关联的文件。
10 在一种可能的实现中，所述第一信任配置信息包括多个信任配置信息中的一个，不同的信任配置信息指示不同地区或用户对所述媒体资产需满足指标的要求。
在一种可能的实现中，所述获取媒体资产的一个或多个信任因子的动作为基于硬件传感器采集到所述媒体内容、或者生成软件生成所述媒体内容触发。
在一种可能的实现中，所述获取媒体资产的多个指标以及配置文件之前，所述获取模块 1701，还用
15 于：
接收到针对于所述媒体内容的可信评估请求。
在一种可能的实现中，所述媒体内容为图像、视频或者音频中的至少一种。

此外，本申请实施例还提供了一种数据处理装置，所述装置包括：
20 获取模块 1701，用于获取媒体资产；所述媒体资产包括媒体内容，所述媒体资产还包括媒体内容的元数据以及媒体内容的信任记录中的至少一种；
其中，关于处理模块 1701 的具体描述可以参照上述实施例步骤 1601 的描述，这里不再赘述。
处理模块 1702，用于确定所述媒体资产的一个或多个信任因子，所述一个或多个信任因子用于评估所述媒体资产的可信度。
25 其中，关于处理模块 1702 的具体描述可以参照上述实施例步骤 1602 的描述，这里不再赘述。
在一种可能的实现中，所述一个或多个信任因子封装在信任凭据中。
在一种可能的实现中，所述一个或多个信任因子是根据所述媒体内容、媒体内容对应的元数据以及媒体内容对应的信任记录中的至少一种确定的。
在一种可能的实现中，所述一个或多个信任因子用于确定媒体资产的可信信息，所述可信信息用于
30 指示所述一个或多个信任因子是否满足指标。
在一种可能的实现中，所述指标包括所述媒体资产需满足的信任因子。
在一种可能的实现中，所述信任因子包括指示媒体资产的可信度的参数。
在一种可能的实现中，所述媒体内容为图像、视频或者音频中的至少一种。
接下来介绍本申请实施例提供的一种执行设备，请参阅图 18，图 18 为本申请实施例提供的执行设备
35 的一种结构示意图，执行设备 1800 具体可以表现为手机、平板、笔记本电脑、智能穿戴设备等，此处不做限定。具体的，执行设备 1800 包括：接收器 1801、发射器 1802、处理器 1803 和存储器 1804 (其中执行设备 1800 中的处理器 1803 的数量可以一个或多个，图 18 中以一个处理器为例)，其中，处理器 1803 可以包括应用处理器 18031 和通信处理器 18032。在本申请的一些实施例中，接收器 1801、发射器 1802、处理器 1803 和存储器 1804 可通过总线或其它方式连接。
40 存储器 1804 可以包括只读存储器和随机存取存储器，并向处理器 1803 提供指令和数据。存储器 1804 的一部分还可以包括非易失性随机存取存储器 (non-volatile random access memory, NVRAM)。存储器 1804 存储有处理器和操作指令、可执行模块或者数据结构，或者它们的子集，或者它们的扩展集，其中，操作指令可包括各种操作指令，用于实现各种操作。
处理器 1803 控制执行设备的操作。具体的应用中，执行设备的各个组件通过总线系统耦合在一起，
45 其中总线系统除包括数据总线之外，还可以包括电源总线、控制总线和状态信号总线等。但是为了清楚说明起见，在图中将各种总线都称为总线系统。

上述本申请实施例揭示的方法可以应用于处理器 1803 中, 或者由处理器 1803 实现。处理器 1803 可以是一种集成电路芯片, 具有信号的处理能力。在实现过程中, 上述方法的各步骤可以通过处理器 1803 中的硬件的集成逻辑电路或者软件形式的指令完成。上述的处理器 1803 可以是通用处理器、数字信号处理器 (digital signal processing, DSP)、微处理器或微控制器, 还可进一步包括专用集成电路 (application specific integrated circuit, ASIC)、现场可编程门阵列 (field-programmable gate array, FPGA) 或者其他可编程逻辑器件、分立门或者晶体管逻辑器件、分立硬件组件。该处理器 1803 可以实现或者执行本申请实施例中的公开的各方法、步骤及逻辑框图。通用处理器可以是微处理器或者该处理器也可以是任何常规的处理器等。结合本申请实施例所公开的方法的步骤可以直接体现为硬件译码处理器执行完成, 或者用译码处理器中的硬件及软件模块组合执行完成。软件模块可以位于随机存储器, 闪存、只读存储器, 可编程只读存储器或者电可擦写可编程存储器、寄存器等本领域成熟的存储介质中。该存储介质位于存储器 1804, 处理器 1803 读取存储器 1804 中的信息, 结合其硬件完成上述方法的步骤。

接收器 1801 可用于接收输入的数字或字符信息, 以及产生与执行设备的相关设置以及功能控制有关的信号输入。发射器 1802 可用于输出数字或字符信息; 发射器 1802 还可用于向磁盘组发送指令, 以修改磁盘组中的数据。

本申请实施例中, 在一种情况下, 处理器 1803, 用于执行图 6B 至图 16A 对应实施例中的数据处理方法的步骤。

本申请实施例还提供了一种服务器, 请参阅图 19, 图 19 是本申请实施例提供的服务器一种结构示意图, 具体的, 服务器 1900 由一个或多个服务器实现, 服务器 1900 可因配置或性能不同而产生比较大的差异, 可以包括一个或一个以上中央处理器 (central processing units, CPU) 1919 (例如, 一个或一个以上处理器) 和存储器 1932, 一个或一个以上存储应用程序 1942 或数据 1944 的存储介质 1930 (例如一个或一个以上海量存储设备)。其中, 存储器 1932 和存储介质 1930 可以是短暂存储或持久存储。存储在存储介质 1930 的程序可以包括一个或一个以上模块 (图示没标出), 每个模块可以包括对服务器中的一系列指令操作。更进一步地, 中央处理器 1919 可以设置为与存储介质 1930 通信, 在服务器 1900 上执行存储介质 1930 中的一系列指令操作。

服务器 1900 还可以包括一个或一个以上电源 1920, 一个或一个以上有线或无线网络接口 1950, 一个或一个以上输入输出接口 1958; 或, 一个或一个以上操作系统 1941, 例如 Windows Server™, Mac OS X™, Unix™, Linux™, FreeBSD™ 等等。

本申请实施例中, 中央处理器 1919, 用于执行图 6B 至图 16A 对应实施例中的数据处理方法的步骤。

本申请实施例中还提供一种包括计算机可读指令的计算机程序产品, 当其在计算机上运行时, 使得计算机执行如前述执行设备所执行的步骤, 或者, 使得计算机执行如前述训练设备所执行的步骤。

本申请实施例中还提供一种计算机可读存储介质, 该计算机可读存储介质中存储有用于进行信号处理的程序, 当其在计算机上运行时, 使得计算机执行如前述执行设备所执行的步骤, 或者, 使得计算机执行如前述训练设备所执行的步骤。

另外需说明的是, 以上所描述的装置实施例仅仅是示意性的, 其中所述作为分离部件说明的单元可以是或者也可以不是物理上分开的, 作为单元显示的部件可以是或者也可以不是物理单元, 即可以位于一个地方, 或者也可以分布到多个网络单元上。可以根据实际的需要选择其中的部分或者全部模块来实现本实施例方案的目的。另外, 本申请提供的装置实施例附图中, 模块之间的连接关系表示它们之间具有通信连接, 具体可以实现为一条或多条通信总线或信号线。

通过以上的实施方式的描述, 所属领域的技术人员可以清楚地了解到本申请可借助软件加必需的通用硬件的方式来实现, 当然也可以通过专用硬件包括专用集成电路、专用 CPU、专用存储器、专用元器件等来实现。一般情况下, 凡由计算机程序完成的功能都可以很容易地用相应的硬件来实现, 而且, 用来实现同一功能的具体硬件结构也可以是多多种多样的, 例如模拟电路、数字电路或专用电路等。但是, 对本申请而言更多情况下软件程序实现是更佳的实施方式。基于这样的理解, 本申请的技术方案本质上或者说对现有技术做出贡献的部分可以以软件产品的形式体现出来, 该计算机软件产品存储在可读取的存储介质中, 如计算机的软盘、U 盘、移动硬盘、ROM、RAM、磁碟或者光盘等, 包括若干指令用以

使得一台计算机设备（可以是个人计算机，训练设备，或者网络设备等）执行本申请各个实施例所述的方法。

在上述实施例中，可以全部或部分地通过软件、硬件、固件或者其任意组合来实现。当使用软件实现时，可以全部或部分地以计算机程序产品的形式实现。

5 所述计算机程序产品包括一个或多个计算机指令。在计算机上加载和执行所述计算机程序指令时，全部或部分地产生按照本申请实施例所述的流程或功能。所述计算机可以是通用计算机、专用计算机、计算机网络、或者其他可编程装置。所述计算机指令可以存储在计算机可读存储介质中，或者从一个计算机可读存储介质向另一计算机可读存储介质传输，例如，所述计算机指令可以从一个网站站点、计算机、训练设备或数据中心通过有线（例如同轴电缆、光纤、数字用户线（DSL））或无线（例如红外、无线、微波等）方式向另一个网站站点、计算机、训练设备或数据中心进行传输。所述计算机可读存储介质可以是计算机能够存储的任何可用介质或者是包含一个或多个可用介质集成的训练设备、数据中心等数据存储设备。所述可用介质可以是磁性介质，（例如，软盘、硬盘、磁带）、光介质（例如，DVD）、或者半导体介质（例如固态硬盘（Solid State Disk，SSD））等。

10

权 利 要 求 书

- 1.一种数据处理方法，其特征在于，所述方法包括：
获取媒体资产的一个或多个信任因子；所述媒体资产包括媒体内容，所述媒体资产还包括媒体内容的元数据以及媒体内容的信任记录中的至少一种；
5 确定所述一个或多个信任因子是否满足指标。
2. 根据权利要求1所述的方法，其特征在于，所述方法还包括：
获取第一信任配置信息，所述第一信任配置信息包括媒体资产需满足的指标。
3. 根据权利要求1或2所述的方法，其特征在于，所述一个或多个信任因子是根据所述媒体内容、所述媒体内容对应的元数据以及所述媒体内容对应的信任记录中的至少一种确定的。
- 10 4. 根据权利要求1至3任一所述的方法，其特征在于，所述一个或多个信任因子封装在信任凭据中。
5. 根据权利要求1至4任一所述的方法，其特征在于，还包括：
生成所述媒体资产的可信信息，所述可信信息用于指示所述一个或多个信任因子是否满足指标，所述信任因子包括指示媒体资产的可信度的参数。
6. 根据权利要求1至4任一所述的方法，其特征在于，所述指标包括指示所述媒体资产需满足的信任因子的数据。
- 15 7. 根据权利要求1至6任一的方法，其特征在于，所述确定所述一个或多个信任因子是否满足指标包括：
确定所述指标中对应的信任因子是否包括在所述一个或多个信任因子中，或者确定所述一个或多个信任因子中是否包括所述指标中对应的信任因子。
- 20 8. 根据权利要求1至7任一所述的方法，其特征在于，所述方法还包括：
将所述可信信息添加至所述信任记录。
9. 根据权利要求8所述的方法，其特征在于，所述信任记录包括信任清单；
所述将所述可信信息添加至所述信任记录，包括：
将所述可信信息添加至所述信任清单。
- 25 10. 根据权利要求8或9所述的方法，其特征在于，所述方法还包括：获取所述媒体资产的指示信息；
所述添加至所述信任记录，包括：
根据所述指示信息，将所述可信信息添加至所述指示信息指示的媒体资产对应的所述信任记录。
- 30 11. 根据权利要求1至10任一所述的方法，其特征在于，所述可信信息封装在信任报告中。
12. 根据权利要求1至10任一所述的方法，其特征在于，所述方法还包括：
根据所述可信信息，生成与所述媒体资产相关联的文件。
13. 根据权利要求1至12任一所述的方法，其特征在于，所述第一信任配置信息包括多个信任配置信息中的一个，不同的信任配置信息指示不同地区或用户对所述媒体资产需满足指标的要求。
14. 根据权利要求1至13任一所述的方法，其特征在于，所述获取媒体资产的一个或多个信任因子的动作为基于硬件传感器采集到所述媒体内容、或者生成软件生成所述媒体内容触发。
- 35 15. 根据权利要求1至13任一所述的方法，其特征在于，所述获取媒体资产的一个或多个信任因子之前，所述方法还包括：
接收到针对于所述媒体内容的可信评估请求。
16. 根据权利要求1至15任一所述的方法，其特征在于，所述媒体内容为图像、视频或者音频中的至少一种。
- 40 17. 一种数据处理装置，其特征在于，所述装置包括：
获取模块，用于获取媒体资产的一个或多个信任因子；所述媒体资产包括媒体内容，所述媒体资产还包括媒体内容的元数据以及媒体内容的信任记录中的至少一种；
处理模块，用于确定所述一个或多个信任因子是否满足指标。
- 45 18.一种数据处理装置，其特征在于，所述装置包括存储器和处理器；所述存储器存储有代码，所述处理器被配置为获取所述代码，并执行如权利要求1至16任一所述的方法。

19.一种计算机可读存储介质，其特征在于，包括计算机可读指令，当所述计算机可读指令在计算机设备上运行时，使得所述计算机设备执行权利要求 1 至 16 任一项所述的方法。

20.一种计算机程序产品，其特征在于，包括计算机可读指令，当所述计算机可读指令在计算机设备上运行时，使得所述计算机设备执行如权利要求 1 至 16 任一所述的方法。

5 21. 一种芯片，包括处理器，其特征在于，所述处理器用于支持数据处理装置实现如权利要求 1 至 16 任一所述的方法。