(19)中华人民共和国国家知识产权局

(12)发明专利申请

(10)申请公布号 CN 106686395 A
(43)申请公布日 2017.05.17

(21)申请号 201611250132.5

(22)申请日 2016.12.29

(71)申请人 北京奇艺世纪科技有限公司
地址 100080 北京市海淀区北一街2号鸿城拓展大厦10、11层

(72)发明人 刘志红 项东涛 刘磊

(74)专利代理机构 北京柏杉松知识产权代理事务所(普通合伙) 11413
代理人 马敬 项京

(51)Int.Cl.
H04N 21/2187(2011.01)
H04N 21/234(2011.01)
H04N 21/24(2011.01)
G06K 9/00(2006.01)

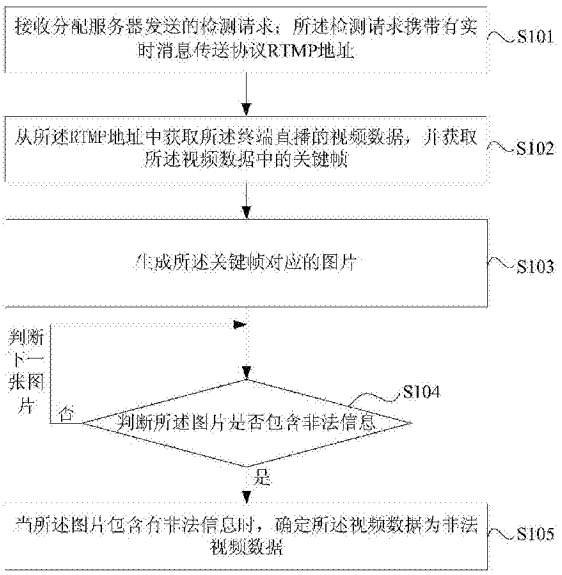
权利要求书2页 说明书8页 附图6页

(54)发明名称

一种直播非法视频的检测方法及系统

(57)摘要

本发明实施例提供了一种直播非法视频的检测方法及系统，该方法包括：接收分配服务器发送的检测请求；所述检测请求携带有实时消息传送协议RTMP地址；所述RTMP地址为：所述分配服务器向终端分配的直播视频所使用的地址；从所述RTMP地址中获取所述终端直播的视频数据，并获取所述视频数据中的关键帧；生成所述关键帧对应的图片；判断所述图片是否包含非法信息；当所述图片包含有非法信息时，确定所述视频数据为非法视频数据。应用本发明实施例，可以对终端直播的视频进行实时检测，提高了直播视频的检测效率。



CN 106686395 A

1.一种直播非法视频的检测方法,其特征在于,包括:

接收分配服务器发送的检测请求;所述检测请求携带有实时消息传送协议RTMP地址;所述RTMP地址为:所述分配服务器向终端分配的直播视频所使用的地址;

从所述RTMP地址中获取所述终端直播的视频数据,并获取所述视频数据中的关键帧;

生成所述关键帧对应的图片;

判断所述图片是否包含非法信息;

当所述图片包含有非法信息时,确定所述视频数据为非法视频数据。

2.根据权利要求1所述的方法,其特征在于,所述获取所述视频数据中的关键帧,包括:

根据关键帧的标识位,从所述视频数据中获取关键帧,其中,所述关键帧为具有全帧图像信息的帧。

3.根据权利要求1所述的方法,其特征在于,判断所述图片是否包含非法信息,包括:

将所述图片与已存储的指纹库中的非法信息进行比对;

当所述图片中包括所述指纹库中存储的非法信息时,判断所述图片中包含非法信息。

4.根据权利要求1所述的方法,其特征在于,所述检测请求还包括:直播ID,所述直播ID为:所述分配服务器向终端分配的直播视频所使用直播间的标识符;

所述在确定所述视频数据为非法视频之后,所述方法还包括:

根据所述图片及所述直播ID,确定直播所述视频数据的直播间。

5.一种直播非法视频的检测方法,其特征在于,包括:

接收终端发送的直播请求,其中,所述直播请求携带有主播的账号和密码;

判断所述直播请求是否合法;

当所述直播请求合法时,向终端分配实时消息传送协议RTMP地址及直播ID;所述RTMP地址为:所述分配服务器向终端分配的直播视频所使用的地址;

从所述RTMP地址中获取所述终端直播的视频数据,并获取所述视频数据中的关键帧;

生成所述关键帧对应的图片;

判断所述图片是否包含非法信息;

当所述图片包含有非法信息时,确定所述视频数据为非法视频数据。

6.一种直播非法视频的检测系统,其特征在于,所述系统包括:调度服务器、至少一个截图服务器及检测服务器;

其中,

所述调度服务器用于接收分配服务器发送的检测请求;所述检测请求携带有实时消息传送协议RTMP地址;所述RTMP地址为:所述分配服务器向终端分配的直播视频所使用的地址;以及,用于从所述至少一个截图服务器中,确定目标截图服务器,其中,所述目标截图服务器为所述至少一个截图服务器中负载最低的截图服务器;向所述目标截图服务器发送所述检测请求;

所述目标截图服务器用于从所述RTMP地址中获取所述终端直播的视频数据,并获取所述视频数据中的关键帧;以及,用于生成所述关键帧对应的图片;

所述检测服务器用于判断所述图片是否包含非法信息;当所述图片包含有非法信息时,确定所述视频数据为非法视频数据。

7.根据权利要求6所述的系统,其特征在于,所述目标截图服务器具体用于,

根据关键帧的标识位，从所述视频数据中获取关键帧，其中，所述关键帧为具有全帧图像信息的帧。

8.根据权利要求6所述的系统，其特征在于，所述检测服务器具体用于，

当图片包含的信息与所述指纹库包含的非法信息相同时，判断所述图片中包含非法信息。

9.根据权利要求6所述的系统，其特征在于，所述检测请求还包括：直播ID，所述直播ID为：所述分配服务器向终端分配的直播视频所使用直播间的标识符；

所述系统还包括：审核服务器；

所述审核服务器用于，根据所述图片及所述直播ID，确定直播所述视频数据的直播间。

10.一种直播非法视频的检测系统，其特征在于，所述系统包括：分配服务器及检测子系统；

其中，

所述分配服务器用于接收终端发送的直播请求，其中，所述直播请求携带有主播的账号和密码；以及，用于判断所述直播请求是否合法；当所述直播请求合法时，向终端分配实时消息传送协议RTMP地址及直播ID；向所述检测子系统发送检测请求，其中，所述检测请求携带有RTMP地址及ID；其中，所述RTMP地址为所述终端直播视频所使用的地址；所述直播ID为：所述分配服务器向终端分配的直播视频所使用直播间的标识符；

所述检测子系统用于接收分配服务器发送的检测请求；以及，用于从所述RTMP地址中获取所述终端直播的视频数据，并获取所述视频数据中的关键帧；以及，用于生成所述关键帧对应的图片；以及，用于判断所述图片是否包含非法信息；以及用于当所述图片包含有非法信息时，确定所述视频数据为非法视频数据。

一种直播非法视频的检测方法及系统

技术领域

[0001] 本发明涉及互联网技术领域，特别是涉及一种直播非法视频的检测方法及系统。

背景技术

[0002] 视频直播已经成为移动互联网巨头的标配服务，网络用户可以通过终端直播视频数据，其中，直播视频数据的网络用户又称主播。

[0003] 目前，对个别主播直播非法视频的检测的方式，主要包括：网络用户举报与监控人员实时监控，其中，网络用户举报为：当网络用户观看到主播正在直播非法视频或者已经直播的非法视频时，向直播平台的监控人员举报或者向有关部门举报；监控人员实时监控为：直播平台的监控人员24小时的观看直播视频，来监控直播平台是否有主播在直播非法视频。

[0004] 随着直播平台日趋平民化，越来越多的人通过直播平台来进行视频直播，当网络用户观看到非法视频数据时，再去举报该非法视频数据时，该非法视频数据已经造成了不良影响，与此同时，监控人员通过观看直播视频来判断直播视频是否非法，造成人力成本过大，检测直播视频的效率较低。

发明内容

[0005] 本发明实施例的目的在于提供一种直播非法视频的检测方法及系统，以提高直播非法视频的检测效率。具体技术方案如下：

[0006] 第一方面，本发明实施例公开了一种直播非法视频的检测方法，包括：

[0007] 接收分配服务器发送的检测请求；所述检测请求携带有实时消息传送协议RTMP地址；所述RTMP地址为：所述分配服务器向终端分配的直播视频所使用的地址；

[0008] 从所述RTMP地址中获取所述终端直播的视频数据，并获取所述视频数据中的关键帧；

[0009] 生成所述关键帧对应的图片；

[0010] 判断所述图片是否包含非法信息；

[0011] 当所述图片包含有非法信息时，确定所述视频数据为非法视频数据。

[0012] 可选的，所述获取所述视频数据中的关键帧，包括：

[0013] 根据关键帧的标识位，从所述视频数据中获取关键帧，其中，所述关键帧为具有全帧图像信息的帧。

[0014] 可选的，判断所述图片是否包含非法信息，包括：

[0015] 将所述图片与已存储的指纹库中的非法信息进行比对；

[0016] 当所述图片中包括所述指纹库中存储的非法信息时，判断所述图片中包含非法信息。

[0017] 可选的，所述检测请求还包括：直播ID，所述直播ID为：所述分配服务器向终端分配的直播视频所使用直播间的标识符；

[0018] 所述在确定所述视频数据为非法视频之后，所述方法还包括：

[0019] 根据所述图片及所述直播ID，确定直播所述视频数据的直播间。

[0020] 第二方面，本发明实施例公开了一种直播非法视频的检测方法，包括：

[0021] 接收终端发送的直播请求，其中，所述直播请求携带有主播的账号和密码；

[0022] 判断所述直播请求是否合法；

[0023] 当所述直播请求合法时，向终端分配实时消息传送协议RTMP地址及直播ID；所述RTMP地址为：所述分配服务器向终端分配的直播视频所使用的地址；

[0024] 从所述RTMP地址中获取所述终端直播的视频数据，并获取所述视频数据中的关键帧；

[0025] 生成所述关键帧对应的图片；

[0026] 判断所述图片是否包含非法信息；

[0027] 当所述图片包含有非法信息时，确定所述视频数据为非法视频数据。

[0028] 第三方面，本发明实施例公开了一种直播非法视频的检测系统，所述系统包括：调度服务器、至少一个截图服务器及检测服务器；

[0029] 其中，

[0030] 所述调度服务器用于接收分配服务器发送的检测请求；所述检测请求携带有实时消息传送协议RTMP地址；所述RTMP地址为：所述分配服务器向终端分配的直播视频所使用的地址；以及，用于从所述至少一个截图服务器中，确定目标截图服务器，其中，所述目标截图服务器为所述至少一个截图服务器中负载最低的截图服务器；向所述目标截图服务器发送所述检测请求；

[0031] 所述目标截图服务器用于从所述RTMP地址中获取所述终端直播的视频数据，并获取所述视频数据中的关键帧；以及，用于生成所述关键帧对应的图片；

[0032] 所述检测服务器用于判断所述图片是否包含非法信息；当所述图片包含有非法信息时，确定所述视频数据为非法视频数据。

[0033] 可选的，所述目标截图服务器具体用于，

[0034] 根据关键帧的标识位，从所述视频数据中获取关键帧，其中，所述关键帧为具有全帧图像信息的帧。

[0035] 可选的，所述检测服务器具体用于，

[0036] 当图片包含的信息与所述指纹库包含的非法信息相同时，判断所述图片中包含非法信息。

[0037] 可选的，所述检测请求还包括：直播ID，所述直播ID为：所述分配服务器向终端分配的直播视频所使用直播间的标识符；

[0038] 所述系统还包括：审核服务器；

[0039] 所述审核服务器用于，根据所述图片及所述直播ID，确定直播所述视频数据的直播间。

[0040] 第四方面，本发明实施例还公开了一种直播非法视频的检测系统，所述系统包括：分配服务器及检测子系统；

[0041] 其中，

[0042] 所述分配服务器用于接收终端发送的直播请求，其中，所述直播请求携带有主播

的账号和密码;以及,用于判断所述直播请求是否合法;当所述直播请求合法时,向终端分配实时消息传送协议RTMP地址及直播ID;向所述检测子系统发送检测请求,其中,所述检测请求携带有RTMP地址及ID;所述RTMP地址为所述终端直播视频所使用的地址;所述直播ID为:所述分配服务器向终端分配的直播视频所使用直播间的标识符;

[0043] 所述检测子系统用于接收分配服务器发送的检测请求;以及,用于从所述RTMP地址中获取所述终端直播的视频数据,并获取所述视频数据中的关键帧;以及,用于生成所述关键帧对应的图片;以及,用于判断所述图片是否包含非法信息;以及用于当所述图片包含有非法信息时,确定所述视频数据为非法视频数据。

[0044] 本发明实施例提供的一种直播非法视频的检测方法及系统,通过接收分配服务器发送的检测请求,其中,该检测请求携带有实时消息传送协议RTMP地址,从RTMP地址获取终端直播的视频数据,并获取视频数据中的关键帧,生成该关键帧对应的图片,判断该图片中是否包含非法信息,当图片中包含非法信息时,确定该视频数据为非法视频数据,也就是确定直播该视频数据的终端正在直播非法视频数据。可见,本发明实施例中,可以及时检测到正在直播的非法视频数据,降低了非法视频数据对网络用户造成的不良影响,同时,应用本发明实施例,可以降低了人力成本,提高了直播非法视频的检测效率。

[0045] 当然,实施本发明的任一产品或方法必不一定需要同时达到以上所述的所有优点。

附图说明

[0046] 为了更清楚地说明本发明实施例或现有技术中的技术方案,下面将对实施例或现有技术描述中所需要使用的附图作简单地介绍,显而易见地,下面描述中的附图仅仅是本发明的一些实施例,对于本领域普通技术人员来讲,在不付出创造性劳动的前提下,还可以根据这些附图获得其他的附图。

[0047] 图1为本发明实施例提供的直播非法视频的检测方法的一种流程图;

[0048] 图2为本发明实施例提供的直播非法视频的检测方法的另一种流程图;

[0049] 图3为本发明实施例提供的直播非法视频的检测方法的另一种流程图;

[0050] 图4为本发明实施例提供的直播非法视频的检测方法的又一种流程图;

[0051] 图5为本发明实施例提供的直播非法视频的检测系统的一种结构示意图;

[0052] 图6为本发明实施例提供的直播非法视频的检测系统的另一种结构示意图;

[0053] 图7为本发明实施例提供的直播非法视频的检测系统又一种结构示意图。

具体实施方式

[0054] 下面将结合本发明实施例中的附图,对本发明实施例中的技术方案进行清楚、完整地描述,显然,所描述的实施例仅仅是本发明一部分实施例,而不是全部的实施例。基于本发明中的实施例,本领域普通技术人员在没有做出创造性劳动前提下所获得的所有其他实施例,都属于本发明保护的范围。

[0055] 直播平台是各大移动互联网商为网络用户提供的互动平台,目前,越来越多的网络用户使用直播平台来直播视频数据。这里的直播平台实际上是由一些服务器组成的网络系统。当有网络用户需要直播视频数据时,网络用户所在的终端首先发送一个直播请求给

分配服务器，分配服务器在接收到该直播请求后，向该终端分配一个实时消息传送协议(Real Time Messaging Protocol，RTMP)地址及直播ID(用于表示该终端直播视频数据的身份标识)，同时，分配服务器将RTMP地址及直播ID发送给存储服务器，存储服务器从RTMP地址获取网络用户正在直播的视频数据，审核人员24小时的观看所获取的视频数据。这样，当直播平台上有很多网络用户直播视频数据时，就需要多个审核人员同时观看不同RTMP地址所获取的视频数据，造成人力成本过大，使得检测直播视频的效率较低。

[0056] 为了解决现有技术的问题，本发明实施例提供了一种直播非法视频的检测方法及系统，以提高直播非法视频的检测效率。

[0057] 下面首先对本发明实施例所提供的一种直播非法视频的检测方法进行介绍。

[0058] 需要说明的是，本发明实施例所提供的一种直播非法视频的检测方法应用于移动互联网的各直播平台的检测服务器中。

[0059] 如图1所示，本发明实施例所提供的一种直播非法视频的检测方法，可以包括如下步骤：

[0060] S101，接收分配服务器发送的检测请求；所述检测请求携带有实时消息传送协议RTMP地址。

[0061] 其中，所述RTMP地址为：所述分配服务器向终端分配的直播视频所使用的地址。

[0062] 可以理解的是，当有网络用户登录直播平台，向分配服务器请求进行直播视频数据时，就会接收到分配服务器发送的检测请求，该检测请求携带有实时消息传送协议RTMP地址。RTMP地址支持播放器和服务器之间音频、视频和数据传输的开放协议。

[0063] 实际应用中，当有一个网络用户登录直播平台时，网络用户所在的终端向分配服务器发送一个直播请求，该直播请求为：终端请求分配服务器分配一个可以上传视频数据的地址；同时，分配服务器向检测服务器发送一个检测请求，请求检测服务器检测终端所上传的视频数据。

[0064] S102，从所述RTMP地址中获取所述终端直播的视频数据，并获取所述视频数据中的关键帧。

[0065] 可以理解的是，当检测服务器接收到分配服务器发送的检测请求后，该检测服务器根据检测请求中的RTMP地址，获取终端直播的视频数据。

[0066] 需要注意的是，分配服务器在发送检测请求之前，首先为网络用户所使用的终端分配直播视频的RTMP地址及直播ID，这里的终端包括：手机、平板电脑、台式电脑以及可以直播视频的电子设备。这样，检测服务器可以根据RTMP地址获取终端正在直播的视频数据，也就是检测服务器从RTMP地址的路径中下载视频数据。同时，在下载视频数据时，获取该视频数据中的关键帧。

[0067] 具体的，所述获取所述视频数据中的关键帧，包括：

[0068] 根据关键帧的标识位，从所述视频数据中获取关键帧，其中，所述关键帧为具有全帧图像信息的帧。

[0069] 需要注意的是，在终端生成视频数据时，对视频数据进行编码，视频数据是由帧组构成，根据每个帧组的基础帧(也就是第一帧，又称关键帧)对该帧组的非关键帧(帧组内除了关键帧的其他帧)进行编码，关键帧是一个全帧压缩编码帧，编码关键帧时不需要参照帧组内非关键帧的，而编码非关键帧时，需要参照关键帧进行编码，可见，关键帧具有全帧图

像信息。通常，关键帧有标识位，该标识位用于区分关键帧和非关键帧。当获取到视频数据时，根据视频数据中关键帧的标志位，提取视频数据中的所有关键帧。

[0070] S103，生成所述关键帧对应的图片。

[0071] 具体的，关键帧具有全帧图片信息，所以根据关键帧就可以重构完整的图片。

[0072] 可以理解的是，一个关键帧对应一张图片，例如，在视频数据中获得1000个关键帧时，可以对应生成1000张图片，在视频数据中获取2000个关键帧时，可以对应生成2000张图片。

[0073] S104，判断所述图片是否包含非法信息。

[0074] 根据视频数据中的关键帧，生成关键帧对应的图片，图片的信息中包含终端上传的网络用户所在的图像背景和运动的所有信息，所以，通过判断图片是否包含非法信息，来确定终端上传的视频数据是否为非法的视频数据。

[0075] 具体的，在本发明实施例的一种可能的实现方式中，判断所述图片是否包含非法信息，包括以下步骤：

[0076] 步骤一，将所述图片与已存储的指纹库中的非法信息进行比对。

[0077] 步骤二，当所述图片中包括所述指纹库中存储的非法信息时，判断所述图片中包含非法信息。

[0078] 实际应用中，图片的色彩值的平均值可以作为图片的属性信息，根据图片色彩值的平均值，与已存储的指纹库中的色彩值的平均值进行比对，当图片的色彩值的平均值大于指纹库中的色彩值的平均值时，判断该图片包含非法信息。例如，图片色彩值的平均值包括：红色色彩值的平均值，黄色色彩值的平均值、黑色色彩值的平均值等，当红色色彩值的平均值大于或等于指纹库中色彩值的平均值时，判断该图片包含非法信息，可以判断终端直播的视频可能为暴力流血事件。

[0079] 具体的，在本发明实施例的一种可能的实现方式中，判断所述图片是否包含非法信息，可以采用AI(Artificial Intelligence，人工智能)，其中，人工智能是计算机科学的一个分支，人工智能实质上指一种新的能以人类智能相似的方式做出反应的智能机器，通过人工智能可以对图片进行识别，当识别到图片包含非法信息时，确定该图片对应的视频数据为非法视频数据，同时，确定了直播视频数据的终端正在直播非法视频数据。

[0080] S105，当所述图片包含有非法信息时，确定所述视频数据为非法视频数据。

[0081] 具体的，当图片不包含非法信息时，判断该图片的下一张图片是否包含非法信息，根据关键帧生成对应的图片，关键帧的数量确定了生成图片的数量，根据获得关键帧的先后顺序，依次判断由关键帧生成的对应图片是否包含非法信息，当前一张图片不包含非法信息时，继续判断该前一张图片之后的下一张图片是否具有非法信息，直至关键帧对应生成的所有图片都被判断完成后，才能确定视频数据是否为非法视频数据。在视频数据的关键帧对应生成的所有图片中至少有一张图片包含非法信息时，确定该视频数据为非法数据。

[0082] 另外，在确定视频数据为非法视频数据后，可以关闭上传非法视频数据的RTMP地址，或者，根据非法视频数据的非法等级，对直播非法视频数据的网络用户发出警告，以使该网络用户停止直播非法视频数据。

[0083] 本发明实施例所提供的直播非法视频的检测方法中，从获得的视频数据中，获得

视频数据的关键帧，再由关键帧生成对应的图片，通过对图片的分析，判断图片是否包含非法信息，从而判断视频数据是否为非法视频数据，与现有技术相比，本方案不是通过监控人员实时观看视频数据，对观看的视频数据进行审核，来判断视频数据是否具有非法性，而是通过视频数据的关键帧，生成该关键帧对应的图片，判断图片是否是非法的，最终从而间接确定视频数据是否具有非法性，降低了人力成本，及时检测终端直播视频数据是否具有非法性，提高了直播非法视频的检测效率。

[0084] 更进一步的，在确定视频数据为非法视频数据之后，需要对直播该非法视频数据的终端进行处理。为了实现上述需求，在S101～S105的基础上，如图2所示，本发明实施例所提供的一种直播非法视频的检测方法还可以包括：

[0085] S106，根据所述图片及所述直播ID，确定直播所述视频数据的直播间。

[0086] 其中，所述检测请求还包括：直播ID，所述直播ID为：所述分配服务器向终端分配的直播视频所使用直播间的标识符。

[0087] 需要强调的是，在接收分配服务器发送的检测请求之前，分配服务器向终端分配了RTMP地址和直播ID，其中，RTMP地址为终端上传视频数据的地址，直播ID为网络用户在直播平台的直播间，在网络用户每次登录直播平台时，分配服务器会随机的将已存储且未被占用的直播ID分配网络用户，在该网络用户直播视频数据时，可以根据分配给该网络用户的直播ID，查找该直播ID对应的直播间，其中，每个直播ID唯一对应一个直播间。在查找到直播间正在直播非法视频数据后，关闭该直播间对应的直播ID，或者，根据非法视频数据的非法等级，向直播非法视频数据的网络用户发送警告。

[0088] 另外，网络用户在直播平台注册时，采用实名制，可以根据直播间对应的直播ID，确定该网络用户的网络身份证ID，其中，网络身份证ID是一种互联网身份认证协议，其具有唯一性和信息不可否认性，当确定该网络用户的网络身份证ID后，可以向相关部门举报该网络用户，请求相关部门查封该网络身份证ID，避免该网络用户再次通过不同的直播平台直播非法视频。

[0089] 下面结合具体的实施例，对本发明实施例所提供的一种直播非法视频的检测方法进行介绍。

[0090] 其中，本发明实施例所提供的一种直播非法视频的检测方法的执行主体可以为一种直播非法视频的检测系统。

[0091] 如图3所示的，一种直播非法视频的检测方法，可以包括如下步骤：

[0092] S301，接收终端发送的直播请求。

[0093] 其中，所述直播请求携带有主播的账号和密码。

[0094] 可以理解的是，网络用户在直播视频数据之前，需要先登录直播平台，也就是网络用户向分配服务器发送直播请求，该直播请求携带有该网络用户(主播)的账号和密码，但不限于此。

[0095] S302，判断所述直播请求是否合法。

[0096] 具体的，判断直播请求中的账号和密码是否与分配服务器中已存储的账号和密码相匹配。

[0097] S303，当所述直播请求合法时，向终端分配实时消息传送协议RTMP地址及直播ID；所述RTMP地址为：所述分配服务器向终端分配的直播视频所使用的地址。

[0098] 当直播请求中的账号和密码与分配服务器中已存储的账号和密码相匹配时，确定该直播请求是合法的，并向主播所在的终端分配RTMP地址及直播ID，则主播可以通过RTMP地址上传该主播所在终端的视频数据，该视频数据在直播ID对应的直播间进行直播。

[0099] 需要注意的是，一个网络用户(主播)分配一个RTMP地址及一个直播ID。

[0100] S304，从所述RTMP地址中获取所述终端直播的视频数据，并获取所述视频数据中的关键帧。

[0101] S305，生成所述关键帧对应的图片。

[0102] S306，判断所述图片是否包含非法信息。

[0103] S307，当所述图片包含有非法信息时，确定所述视频数据为非法视频数据。

[0104] 本实施例中，S304至S307与上述实施例的S102至S105相似，在此不作赘述。

[0105] 与现有技术相比，本方案通过视频数据的关键帧，生成关键帧对应的图片，判断图片是否是非法的，最终从而间接确定视频数据是否具有非法性，降低了人力成本，及时检测终端直播视频数据是否具有非法性，提高了直播非法视频的检测效率。

[0106] 更进一步的，在确定视频数据为非法视频数据之后，需要对直播该非法视频数据的终端进行处理。为了实现上述需求，在S301～S107的基础上，如图4所示，本发明实施例所提供的一种直播非法视频的检测方法还可以包括：

[0107] S308，根据所述图片及所述直播ID，确定直播所述视频数据的直播间。

[0108] 其中，S308与上述实施例的S106相似，在此不作赘述。

[0109] 相应于上述提供的直播非法视频的检测方法实施例，本发明实施例还提供了一种直播非法视频的检测系统，如图5所示，所述系统500可以包括：

[0110] 调度服务器510、至少一个截图服务器520及检测服务器530。

[0111] 其中，所述调度服务器510用于接收分配服务器发送的检测请求；所述检测请求携带有实时消息传送协议RTMP地址；所述RTMP地址为：所述分配服务器向终端分配的直播视频所使用的地址；以及，用于从所述至少一个截图服务器520中，确定目标截图服务器，其中，所述目标截图服务器为所述至少一个截图服务器中负载最低的截图服务器；向所述目标截图服务器发送所述检测请求。

[0112] 所述目标截图服务器521用于从所述RTMP地址中获取所述终端直播的视频数据，并获取所述视频数据中的关键帧；以及，用于生成所述关键帧对应的图片。

[0113] 所述检测服务器530用于判断所述图片是否包含非法信息；当所述图片包含有非法信息时，确定所述视频数据为非法视频数据。

[0114] 具体的，所述目标截图服务器521具体用于，根据关键帧的标识位，从所述视频数据中获取关键帧，其中，所述关键帧为具有全帧图像信息的帧。

[0115] 具体的，所述检测服务器530具体用于，当图片包含的信息与所述指纹库包含的非法信息相同时，判断所述图片中包含非法信息。

[0116] 具体的，所述检测请求还包括：直播ID，所述直播ID为：所述分配服务器向终端分配的直播视频所使用直播间的标识符。

[0117] 本发明实施例中，通过视频数据的关键帧，生成关键帧对应的图片，判断图片是否是非法的，最终从而间接确定视频数据是否具有非法性，降低了人力成本，及时检测终端直播视频数据是否具有非法性，提高了直播非法视频的检测效率。

[0118] 更进一步，在包括调度服务器、至少一个截图服务器和检测服务器的基础上，如图6所示，本发明实施例所提供的一种直播非法视频的检测系统还可以包括：审核服务器540。

[0119] 所述审核服务器540用于，根据所述图片及所述直播ID，确定直播所述视频数据的直播间。

[0120] 如图7所示，本发明实施例所提供的一种直播非法视频的检测系统，所述系统700包括：分配服务器710及检测子系统720。

[0121] 其中，所述分配服务器710用于接收终端发送的直播请求，其中，所述直播请求携带有主播的账号和密码；以及，用于判断所述直播请求是否合法；当所述直播请求合法时，向终端分配实时消息传送协议RTMP地址及直播ID；向所述检测子系统发送检测请求，其中，所述检测请求携带有RTMP地址及ID；其中，所述RTMP地址为所述终端直播视频所使用的地址；所述直播ID为：所述分配服务器向终端分配的直播视频所使用直播间的标识符。

[0122] 所述检测子系统720用于接收分配服务器发送的检测请求；以及，用于从所述RTMP地址中获取所述终端直播的视频数据，并获取所述视频数据中的关键帧；以及，用于生成所述关键帧对应的图片；以及，用于判断所述图片是否包含非法信息；以及用于当所述图片包含有非法信息时，确定所述视频数据为非法视频数据。

[0123] 本发明实施例中，通过视频数据的关键帧，生成关键帧对应的图片，判断图片是否是非法的，最终从而间接确定视频数据是否具有非法性，降低了人力成本，及时检测终端直播视频数据是否具有非法性，提高了直播非法视频的检测效率。

[0124] 对于系统实施例而言，由于其基本相似于方法实施例，所以描述的比较简单，相关之处参见方法实施例的部分说明即可。

[0125] 需要说明的是，在本文中，诸如第一和第二等之类的关系术语仅仅用来将一个实体或者操作与另一个实体或操作区分开来，而不一定要求或者暗示这些实体或操作之间存在任何这种实际的关系或者顺序。而且，术语“包括”、“包含”或者其任何其他变体意在涵盖非排他性的包含，从而使得包括一系列要素的过程、方法、物品或者设备不仅包括那些要素，而且还包括没有明确列出的其他要素，或者是还包括为这种过程、方法、物品或者设备所固有的要素。在没有更多限制的情况下，由语句“包括一个……”限定的要素，并不排除在包括所述要素的过程、方法、物品或者设备中还存在另外的相同要素。

[0126] 本说明书中的各个实施例均采用相关的方式描述，各个实施例之间相同相似的部分互相参见即可，每个实施例重点说明的都是与其他实施例的不同之处。尤其，对于系统实施例而言，由于其基本相似于方法实施例，所以描述的比较简单，相关之处参见方法实施例的部分说明即可。

[0127] 以上所述仅为本发明的较佳实施例而已，并非用于限定本发明的保护范围。凡在本发明的精神和原则之内所作的任何修改、等同替换、改进等，均包含在本发明的保护范围内。

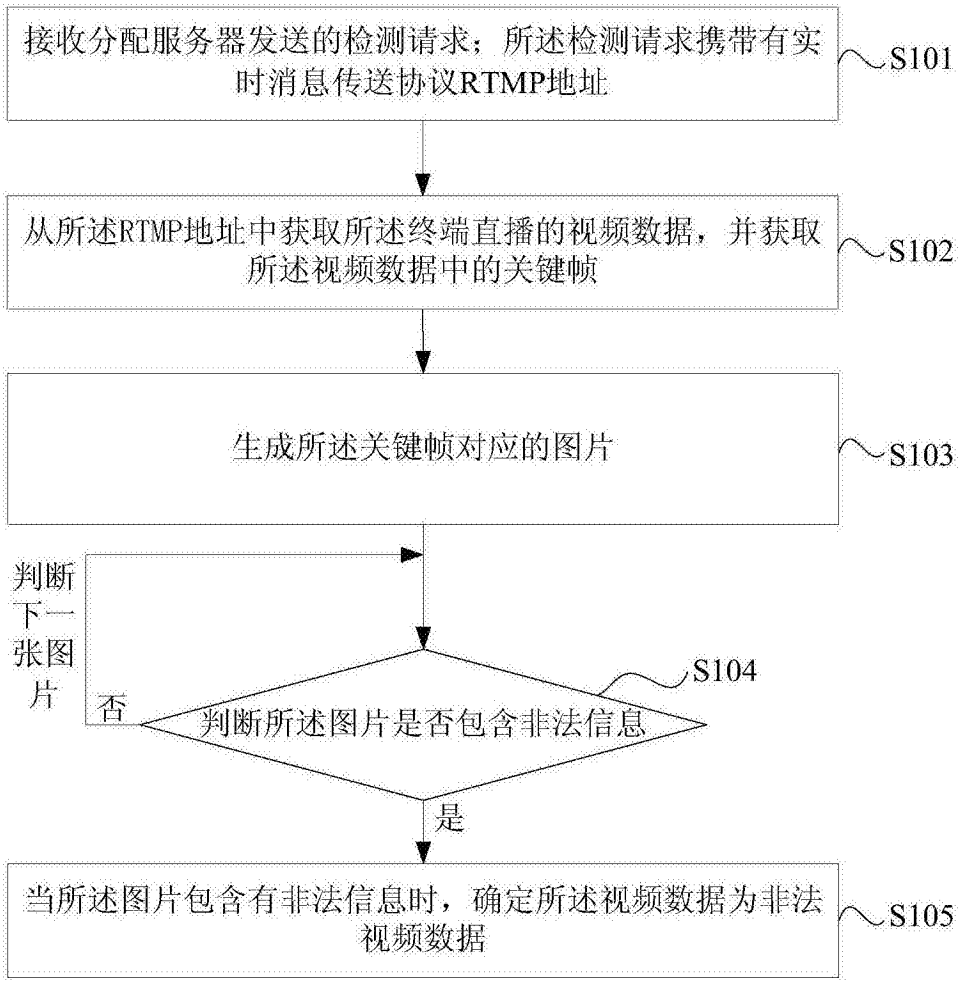

接收分配服务器发送的检测请求；所述检测请求携带有实时消息传送协议RTMP地址
S101
从所述RTMP地址中获取所述终端直播的视频数据，并获取所述视频数据中的关键帧
S102
生成所述关键帧对应的图片
S103
判断下一张图片
否
判断所述图片是否包含非法信息
S104
是
当所述图片包含有非法信息时，确定所述视频数据为非法视频数据
S105

图1

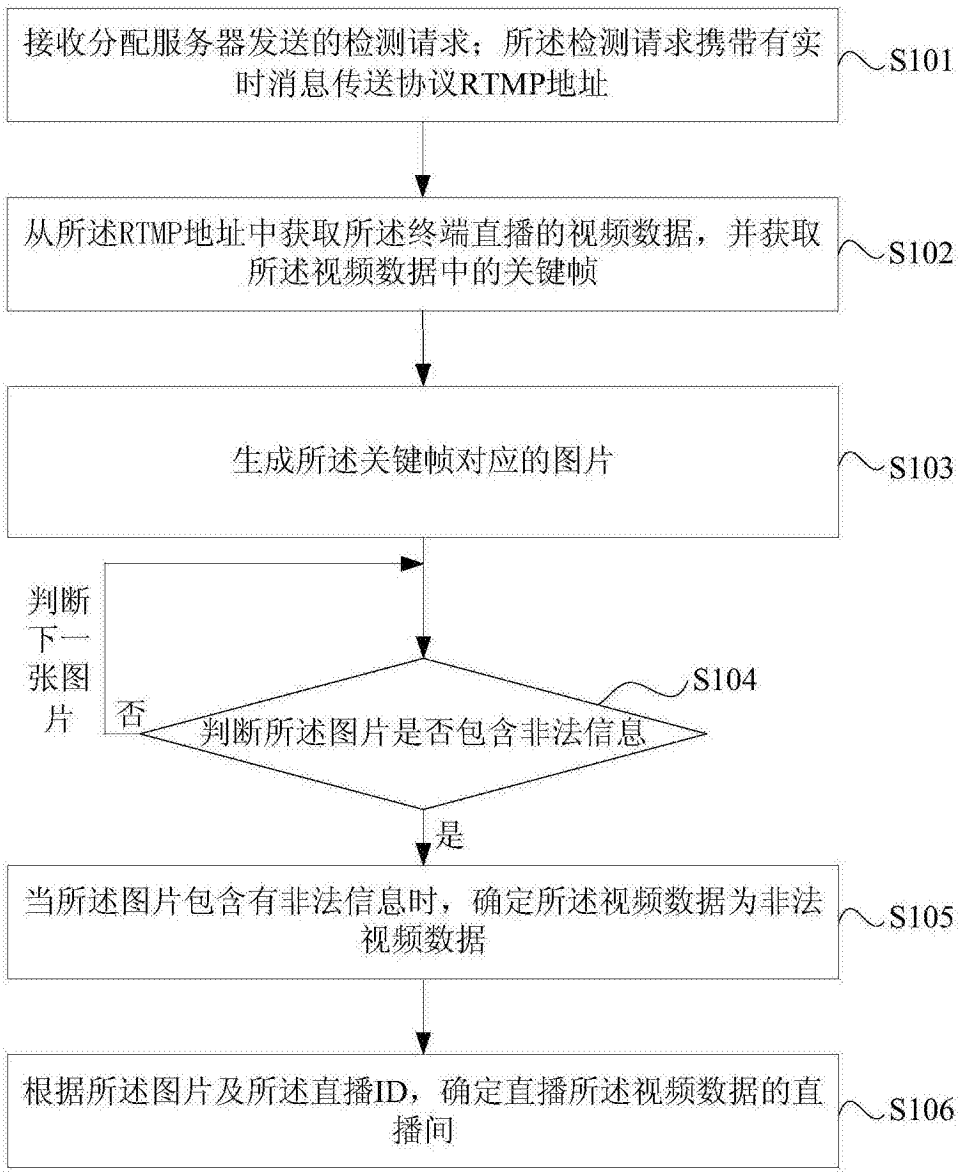

接收分配服务器发送的检测请求；所述检测请求携带有实时消息传送协议RTMP地址
S101
从所述RTMP地址中获取所述终端直播的视频数据，并获取所述视频数据中的关键帧
S102
生成所述关键帧对应的图片
S103
判断下一张图片
否
判断所述图片是否包含非法信息
S104
是
当所述图片包含有非法信息时，确定所述视频数据为非法视频数据
S105
根据所述图片及所述直播ID，确定直播所述视频数据的直播间
S106

图2

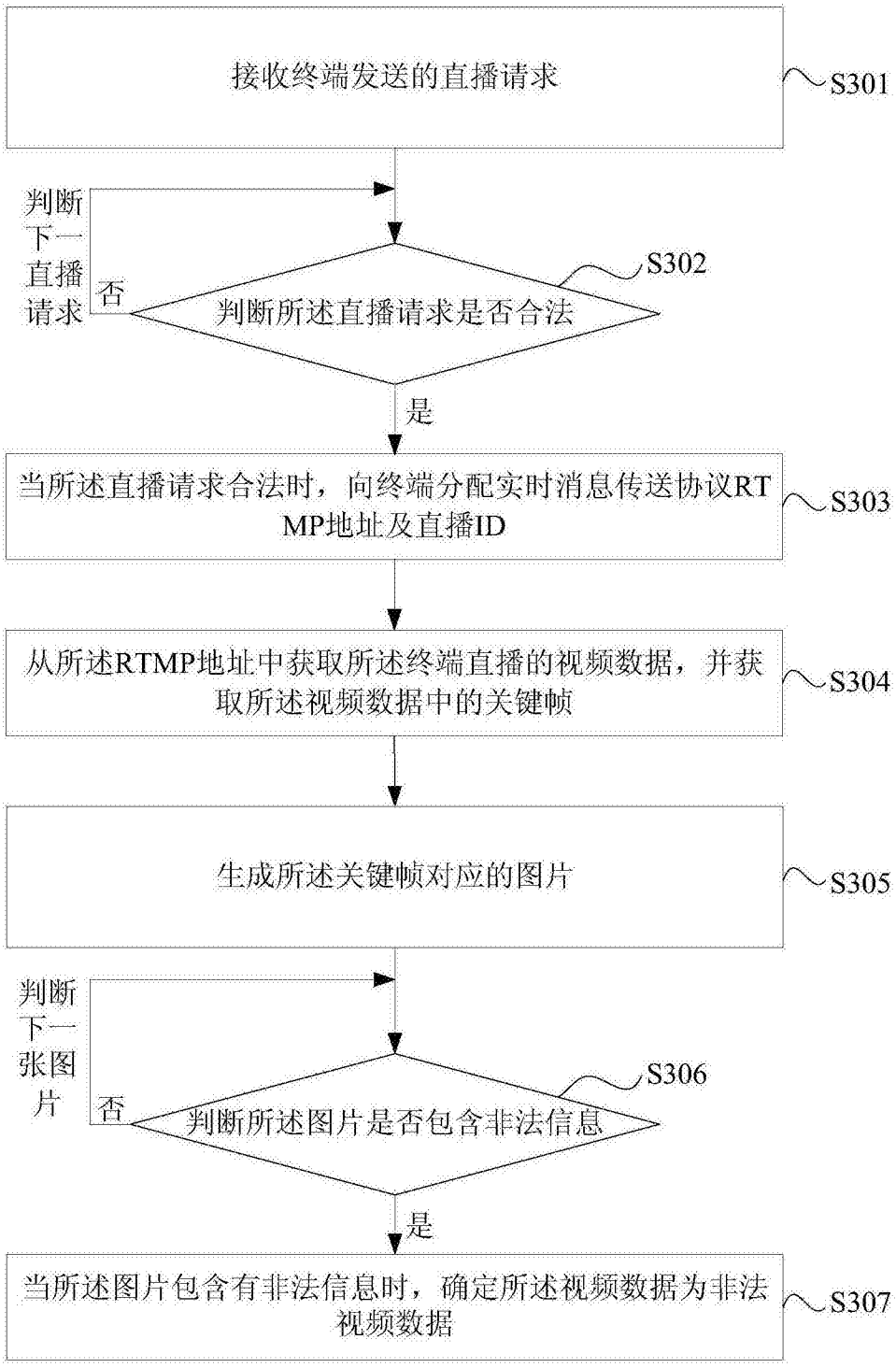

接收终端发送的直播请求
S301
判断下一直播请求
否
判断所述直播请求是否合法
S302
是
当所述直播请求合法时，向终端分配实时消息传送协议RTMP地址及直播ID
S303
从所述RTMP地址中获取所述终端直播的视频数据，并获取所述视频数据中的关键帧
S304
生成所述关键帧对应的图片
S305
判断下一张图片
否
判断所述图片是否包含非法信息
S306
是
当所述图片包含有非法信息时，确定所述视频数据为非法视频数据
S307

图3

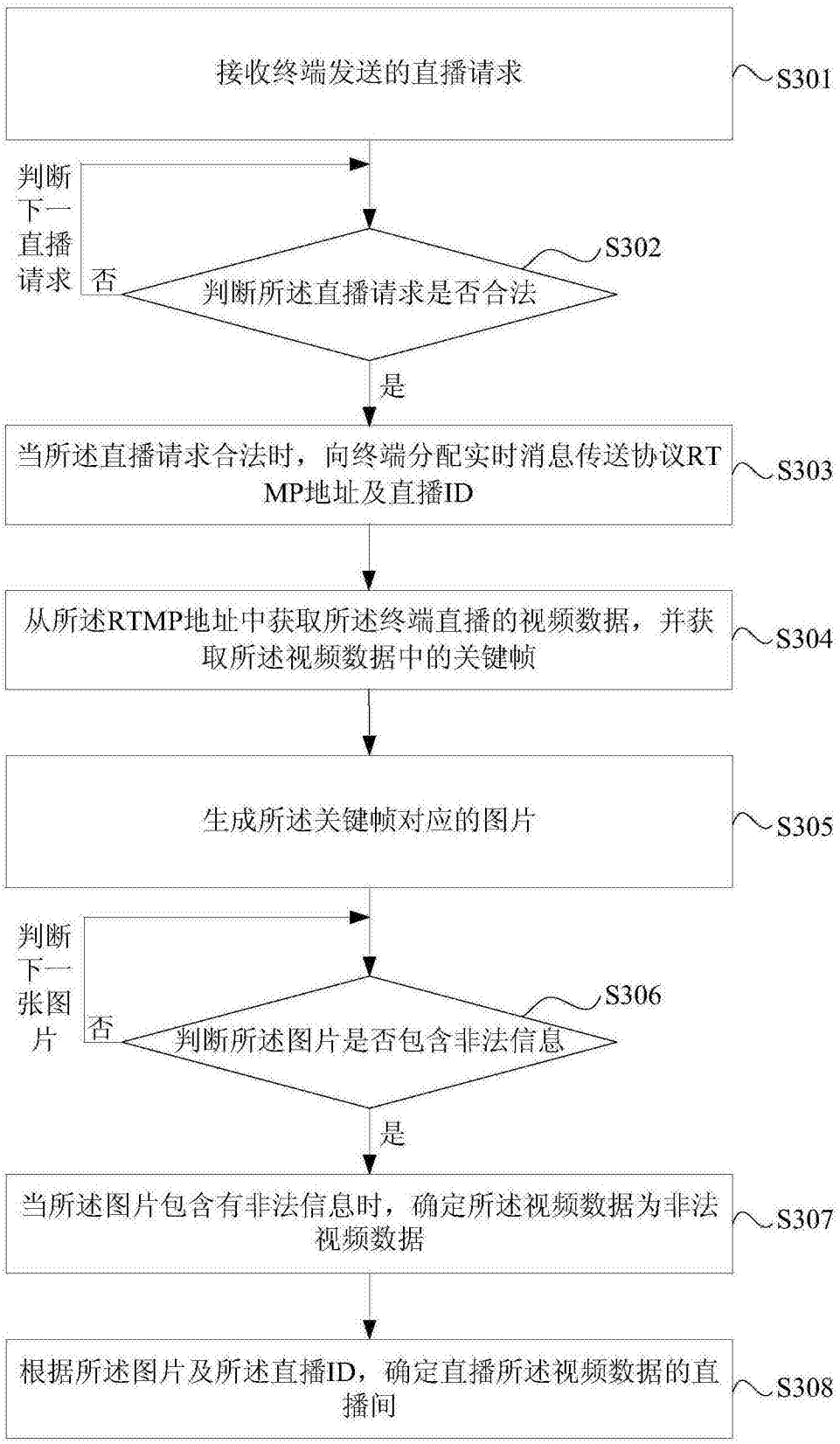

接收终端发送的直播请求
S301
判断下一直播请求
否
判断所述直播请求是否合法
S302
是
当所述直播请求合法时，向终端分配实时消息传送协议RTMP地址及直播ID
S303
从所述RTMP地址中获取所述终端直播的视频数据，并获取所述视频数据中的关键帧
S304
生成所述关键帧对应的图片
S305
判断下一张图片
否
判断所述图片是否包含非法信息
S306
是
当所述图片包含有非法信息时，确定所述视频数据为非法视频数据
S307
根据所述图片及所述直播ID，确定直播所述视频数据的直播间
S308

图4

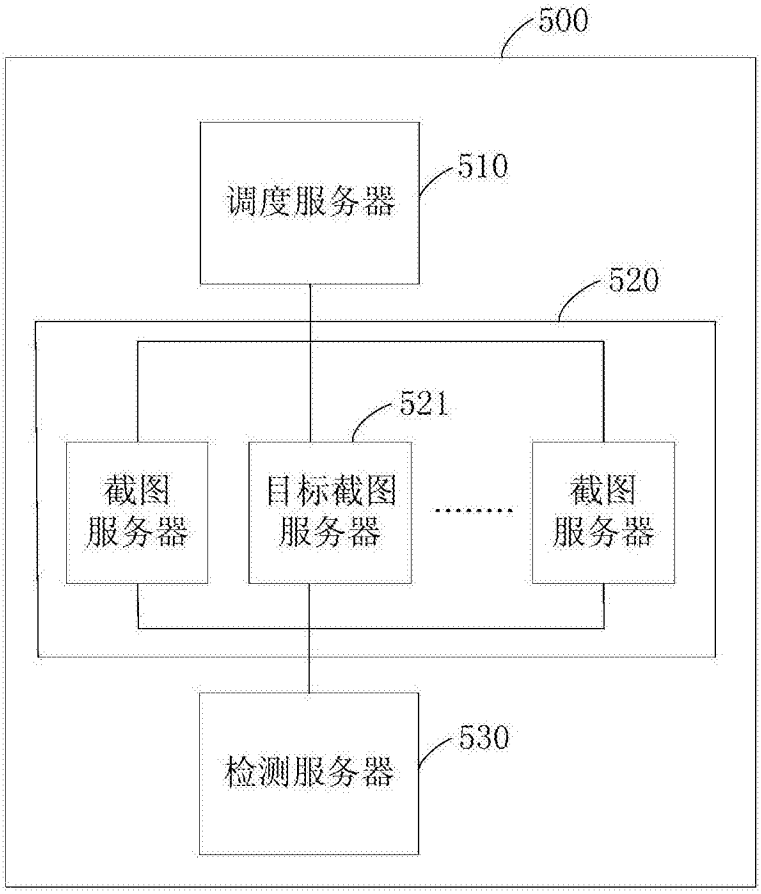


图5

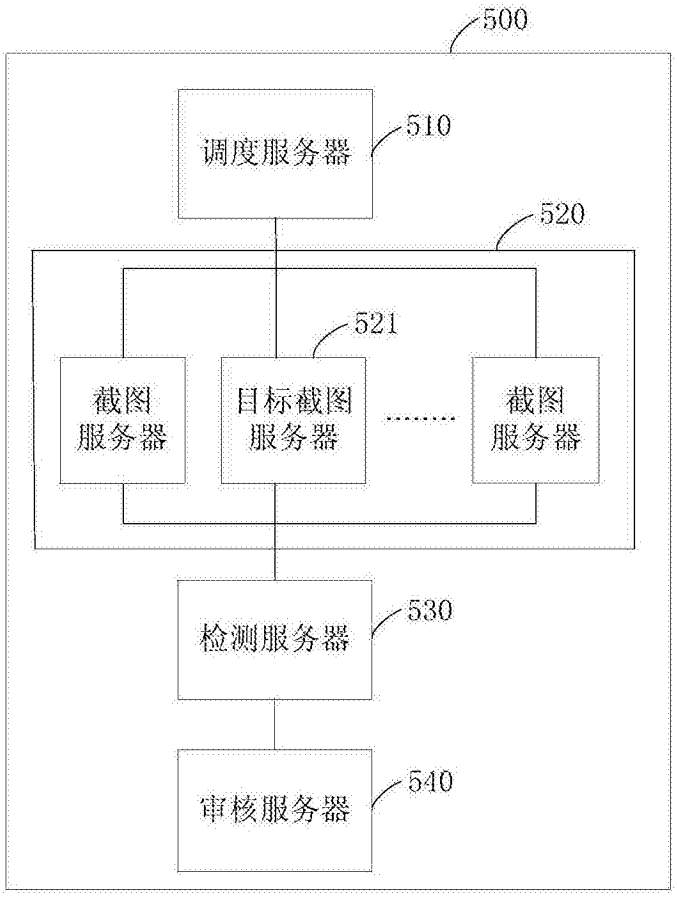

500
调度服务器
510
520
521
截图
服务器
目标截图
服务器
.....
截图
服务器
检测服务器
530
审核服务器
540

图6

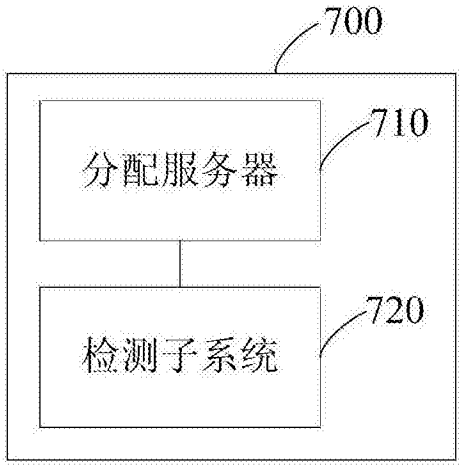

700
分配服务器
710
检测子系统
720

图7