(19)中华人民共和国国家知识产权局

(12)发明专利

(10)授权公告号 CN 106412024 B
(45)授权公告日 2019.10.15

(21)申请号 201610808523.8

(22)申请日 2016.09.07

(65)同一申请的已公布的文献号
申请公布号 CN 106412024 A

(43)申请公布日 2017.02.15

(73)专利权人 网易无尾熊(杭州)科技有限公司
地址 310051 浙江省杭州市滨江区长河街道江汉路1786号钱龙大厦803室

(72)发明人 周明明 黄晓军

(74)专利代理机构 北京同达信恒知识产权代理有限公司 11291
代理人 黄志华

(51)Int.Cl.
H04L 29/08(2006.01)
H04L 29/06(2006.01)

(56)对比文件
CN 102984275 A,2013.03.20,说明书第[0009]-[0021]段.
CN 102591877 A,2012.07.18,全文.
CN 102355657 A,2012.02.15,全文.
CN 104243522 A,2014.12.24,全文.
CN 102955847 A,2013.03.06,全文.
月光博客."HTTP使用RSA公钥加密算法加密明文.《HTTP使用RSA公钥加密算法加密明文，www.williamlong.info/srchives/4346.html》.2015,实现思路.
月光博客.HTTP使用RSA公钥加密算法加密明文.《HTTP使用RSA公钥加密算法加密明文，www.williamlong.info/srchives/4346.html》.2015,实现思路.

审查员 王洪蕾

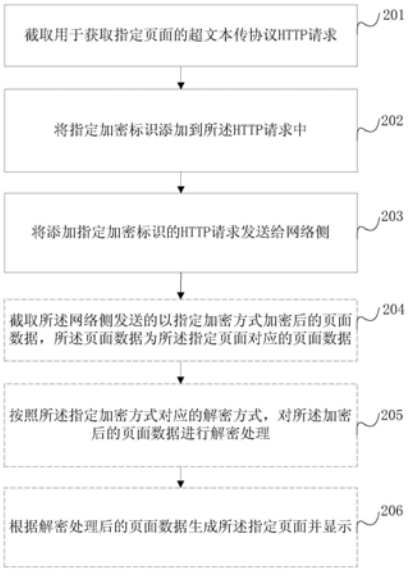
权利要求书3页 说明书15页 附图10页

(54)发明名称

一种页面获取方法和装置

(57)摘要

本发明的实施方式提供了一种页面获取方法。其中,基于用户设备侧的页面获取方法包括:截取用于获取指定页面的HTTP请求;将指定加密标识添加到HTTP请求中;将添加指定加密标识的HTTP请求发送给网络侧。基于网络侧的页面获取方法包括:接收用户设备发送的获取指定页面的HTTP请求;确定HTTP请求中包含指定加密标识时,获取相应的指定加密方式;按照获取的指定加密方式将指定页面对应的页面数据进行加密;将加密后的页面数据返回给用户设备。本发明的方法既能够防止用户设备请求获取的页面被篡改,又能够节约成本。此外,本发明实施方式提供了一种页面获取装置。



CN 106412024 B

1.一种页面获取方法,包括:

截取用于获取指定页面的超文本传协议HTTP请求;

将指定加密标识添加到所述HTTP请求中;

将添加指定加密标识的HTTP请求发送给网络侧;

截取所述网络侧发送的以指定加密方式加密后的页面数据,所述页面数据为所述指定页面对应的页面数据;

按照所述指定加密方式对应的解密方式,对所述加密后的页面数据进行解密处理;

根据解密处理后的页面数据生成所述指定页面并显示,其中所述指定加密方式为所述指定加密标识对应的加密方式;

其中,所述页面数据包括所述指定页面的超文本标记语言HTML数据,所述HTML数据包括文本数据、JS链接地址和资源数据链接地址;所述按照所述指定加密方式对应的解密方式,对所述加密后的页面数据进行解密处理,包括:

按照所述指定加密方式对应的解密方式,对所述加密后的页面数据进行解密,得到所述指定页面的解密后的HTML数据;根据所述HTML数据中的JS链接地址,从所述网络侧获取所述JS链接地址对应的已按照所述指定加密方式加密后的JS数据;按照所述指定加密方式对应的解密方式,对所述已按照所述指定加密方式加密后的JS数据进行解密,得到所述指定页面的JS数据;并,根据所述HTML数据中的资源数据链接地址,从所述网络侧获取所述资源数据链接地址对应的资源数据;其中,针对同一JS数据,按照不同加密方式加密后的该JS数据的JS链接地址不同,未加密的该JS数据的JS链接地址与加密后的该JS数据的JS链接地址也不同。

2.根据权利要求1所述的方法,还包括:

截取所述网络侧发送的以指定加密方式加密后的加载资源白名单;

按照所述指定加密方式对应的解密方式,对所述加密后的加载资源白名单进行解密处理,所述加载资源白名单中包括所述指定页面中受信任的链接地址。

3.根据权利要求2所述的方法,其中,根据所述HTML数据中的资源数据链接地址,从所述网络侧获取所述资源数据链接地址对应的资源数据,包括:

确定所述资源数据链接地址为所述加载资源白名单中的资源数据链接地址时,从服务器获取所述资源数据链接地址对应的资源数据。

4.根据权利要求1-3任一所述的方法,其中,将指定加密标识添加到所述HTTP请求中,包括:

将指定加密标识添加到所述HTTP请求的头部。

5.一种页面获取方法,包括:

接收用户设备发送的获取指定页面的超文本传输协议HTTP请求;

确定所述HTTP请求中包含指定加密标识时,获取相应的指定加密方式;

按照所述获取的指定加密方式将所述指定页面对应的页面数据进行加密;

将所述加密后的页面数据返回给所述用户设备;

其中,将所述加密后的页面数据返回给所述用户设备,包括:

确定所述获取的指定加密方式对应的JS链接地址,其中,所述JS链接地址对应的JS数据为所述指定页面对应的JS数据,并且该JS数据预先按照所述获取的指定加密方式进行加

密；

将获取的指定加密方式对应的JS链接地址放置在所述指定页面的HTLM数据中；

将所述指定页面的HTLM数据按照所述获取的指定加密方式加密后返回给所述用户设备；其中，针对任一JS数据，使用不同的加密方式加密后的所述任一JS数据对应的JS链接地址不同，未加密的所述任一JS数据以及预先按照各个加密方式进行加密后的所述任一JS数据预先存储在备份服务器中。

6.根据权利要求5所述的方法，其中，采用如下方式确定所述HTTP请求中包含指定加密标识：

判断所述HTTP请求的头部的指定字段是否为预设值；

如果是，确定所述HTTP请求中包含指定加密标识。

7.根据权利要求5所述的方法，还包括：

从针对所述HTTP请求的HTTP响应消息的头部获取加载资源白名单；

按照所述获取的指定加密方式对加载资源白名单进行加密；

将所述加密后的加载资源白名单返回给所述用户设备。

8.一种页面获取装置，包括：

第一截取模块，用于截取用于获取指定页面的超文本传协议HTTP请求；

添加模块，用于将指定加密标识添加到所述HTTP请求中；

发送模块，用于将添加指定加密标识的HTTP请求发送给网络侧；

第二截取模块，用于截取所述网络侧发送的以指定加密方式加密后的页面数据，所述页面数据为所述指定页面对应的页面数据；

解密模块，用于按照所述指定加密方式对应的解密方式，对所述加密后的页面数据进行解密处理；

显示模块，用于根据解密处理后的页面数据生成所述指定页面并显示，其中所述指定加密方式为所述指定加密标识对应的加密方式；

其中，所述页面数据包括所述指定页面的超文本标记语言HTML数据，所述HTML数据包括文本数据、JS链接地址和资源数据链接地址；

所述解密模块，包括：第一解密单元，用于按照所述指定加密方式对应的解密方式，对所述加密后的页面数据进行解密，得到所述指定页面的解密后的HTML数据；第一获取单元，用于根据所述HTML数据中的JS链接地址，从所述网络侧获取所述JS链接地址对应的已按照所述指定加密方式加密后的JS数据；第二解密单元，用于按照所述指定加密方式对应的解密方式，对所述已按照所述指定加密方式加密后的JS数据进行解密，得到所述指定页面的JS数据；第二获取单元，用于根据所述HTML数据中的资源数据链接地址，从所述网络侧获取所述资源数据链接地址对应的资源数据。

9.根据权利要求8所述的装置，其中，

所述第二截取模块还用于，截取所述网络侧发送的以指定加密方式加密后的加载资源白名单；

所述解密模块还用于，按照所述指定加密方式对应的解密方式，对所述加密后的加载资源白名单进行解密处理，所述加载资源白名单中包括所述指定页面中受信任的链接地址。

10.根据权利要求9所述的装置,其中,所述第二获取单元具体用于:

确定所述资源数据链接地址为所述加载资源白名单中的资源数据链接地址时,从服务器获取所述资源数据链接地址对应的资源数据。

11.根据权利要求8-10任一所述的装置,其中,所述添加模块具体用于:

将指定加密标识添加到所述HTTP请求的头部。

12.一种页面获取装置,包括:

接收模块,用于接收用户设备发送的获取指定页面的超文本传输协议HTTP请求;

获取模块,用于确定所述HTTP请求中包含指定加密标识时,获取相应的指定加密方式;

加密模块,用于按照所述获取的指定加密方式将所述指定页面对应的页面数据进行加密;

发送模块,用于将所述加密后的页面数据返回给所述用户设备;

所述发送模块,包括:

确定单元,用于确定所述获取的指定加密方式对应的JS链接地址,其中,所述JS链接地址对应的JS数据为所述指定页面对应的JS数据,并且该JS数据预先按照所述获取的指定加密方式进行加密;放置单元,用于将获取的指定加密方式对应的JS链接地址放置在所述指定页面的HTLM数据中;返回单元,用于将所述指定页面的HTLM数据按照所述获取的指定加密方式加密后返回给所述用户设备;其中,针对任一JS数据,使用不同的加密方式加密后的所述任一JS数据对应的JS链接地址不同,未加密的所述任一JS数据以及预先按照各个加密方式进行加密后的所述任一JS数据预先存储在备份服务器中。

13.根据权利要求12所述的装置,其中,所述获取模块包括:

判断单元,用于判断所述HTTP请求的头部的指定字段是否为预设值;

确定单元,用于在所述判断单元判断是的情况下,确定所述HTTP请求中包含指定加密标识。

14.根据权利要求12所述的装置,其中,

所述获取模块还用于,从针对所述HTTP请求的HTTP响应消息的头部获取加载资源白名单;

所述加密模块还用于,按照所述获取的指定加密方式对加载资源白名单进行加密;

所述发送模块还用于,将所述加密后的加载资源白名单返回给所述用户设备。

一种页面获取方法和装置

技术领域

[0001] 本发明的实施方式涉及网络安全技术领域，更具体地，本发明的实施方式涉及一种页面获取方法和装置。

背景技术

[0002] 本部分旨在为权利要求书中陈述的本发明的实施方式提供背景或上下文。此处的描述不因为包括在本部分中就承认是现有技术。

[0003] 目前，常用的页面获取的方式为：

[0004] 用户设备中浏览器或者APP的浏览器组件根据用户提交的页面地址，通过HTTP(超文本传输协议)协议向网络侧的服务器端发送HTPP请求，该请求用于获取相应的页面；网络侧的服务器端根据该HTTP请求，提取相应的页面数据，并通过HTTP协议将提取的页面数据响应给用户设备中的浏览器或者浏览器组件；浏览器或者浏览器组件将服务器端响应的页面数据拼接为相应的页面并显示。

[0005] 在HTTP协议下传输的数据均为明文数据，即服务器端利用HTTP协议向浏览器或者浏览器组件响应的页面数据为明文数据，一些网络攻击设备或软件可能会截取服务器响应的页面数据，并对该页面数据进行篡改，将篡改后的页面数据发送给用户设备，这就会造成用户设备无法正常显示页面，或者，显示的页面中包含各种垃圾信息的问题。

[0006] 目前，为了避免上述问题，将HTTP协议替换为HTTPS协议，响应于HTTPS请求，服务器端将相应的页面数据进行加密，并将加密后的页面数据响应给浏览器或者浏览器组件，浏览器或者浏览器组件对页面数据进行解密后，进行页面显示。

[0007] 但是，将HTTP协议替换为HTTPS协议涉及运维配置修改、代码修改以及网络设备性能优化等操作，需要在网络侧进行的改动较多，成本较高。

发明内容

[0008] 现有技术中，由于将HTTP协议替换为HTTPS协议涉及运维配置修改、代码修改以及网络设备性能优化等操作，需要在网络侧进行的改动较多，成本较高。为此，非常需要一种既能够节约成本又能够防止页面被篡改的页面获取方法。

[0009] 在本上下文中，本发明的实施方式期望提供一种页面获取方法和装置。

[0010] 在本发明实施方式的第一方面中，提供了一种页面获取方法，包括：

[0011] 截取用于获取指定页面的超文本传协议HTTP请求；

[0012] 将指定加密标识添加到所述HTTP请求中；

[0013] 将添加指定加密标识的HTTP请求发送给网络侧。

[0014] 在本发明实施方式的第二方面中，提供了一种页面获取装置，包括：

[0015] 截取模块，用于截取用于获取指定页面的超文本传协议HTTP请求；

[0016] 添加模块，用于将指定加密标识添加到所述HTTP请求中；

[0017] 发送模块，用于将添加指定加密标识的HTTP请求发送给网络侧。

[0018] 在本发明实施方式的第三方面中，提供了另一种页面获取方法，包括：

[0019] 接收用户设备发送的获取指定页面的超文本传输协议HTTP请求；

[0020] 确定所述HTTP请求中包含指定加密标识时，获取相应的指定加密方式；

[0021] 按照所述获取的指定加密方式将所述指定页面对应的页面数据进行加密；

[0022] 将所述加密后的页面数据返回给所述用户设备。

[0023] 在本发明实施方式的第四方面中，提供了另一种页面获取装置，包括：

[0024] 接收模块，用于接收用户设备发送的获取指定页面的超文本传输协议HTTP请求；

[0025] 获取模块，用于确定所述HTTP请求中包含指定加密标识时，获取相应的指定加密方式；

[0026] 加密模块，用于按照所述获取的指定加密方式将所述指定页面对应的页面数据进行加密；

[0027] 发送模块，用于将所述加密后的页面数据返回给所述用户设备。

[0028] 在本发明实施方式的第五方面中，提供了一种页面获取设备，例如，可以包括存储器和处理器，其中，处理器可以用于读取存储器中的程序，执行下列过程：

[0029] 截取用于获取指定页面的超文本传协议HTTP请求；

[0030] 将指定加密标识添加到所述HTTP请求中；

[0031] 将添加指定加密标识的HTTP请求发送给网络侧。

[0032] 在本发明实施方式的第六方面中，提供了另一种页面获取设备，例如，可以包括存储器和处理器，其中，处理器可以用于读取存储器中的程序，执行下列过程：

[0033] 接收用户设备发送的获取指定页面的超文本传输协议HTTP请求；

[0034] 确定所述HTTP请求中包含指定加密标识时，获取相应的指定加密方式；

[0035] 按照所述获取的指定加密方式将所述指定页面对应的页面数据进行加密；

[0036] 将所述加密后的页面数据返回给所述用户设备。

[0037] 在本发明实施方式的第七方面中，提供了一种程序产品，其包括程序代码，当所述程序产品运行时，所述程序代码用于执行以下过程：

[0038] 截取用于获取指定页面的超文本传协议HTTP请求；

[0039] 将指定加密标识添加到所述HTTP请求中；

[0040] 将添加指定加密标识的HTTP请求发送给网络侧。

[0041] 在本发明实施方式的第八方面中，提供了另一种程序产品，其包括程序代码，当所述程序产品运行时，所述程序代码用于执行以下过程：

[0042] 接收用户设备发送的获取指定页面的超文本传输协议HTTP请求；

[0043] 确定所述HTTP请求中包含指定加密标识时，获取相应的指定加密方式；

[0044] 按照所述获取的指定加密方式将所述指定页面对应的页面数据进行加密；

[0045] 将所述加密后的页面数据返回给所述用户设备。

[0046] 根据本发明实施方式的页面获取方法和装置，用户设备在截取的HTTP请求中添加加密标识，并将添加加密标识的HTTP请求发送给网络侧，网络侧将按照HTTP请求中的加密标识对应的加密方式加密后的页面数据返回给用户设备，即，在HTTP协议的基础上，通过HTTP请求，从网络侧获取加密后的页面数据，从而既能够防止用户设备请求获取的页面被篡改，又能够节约成本。

附图说明

[0047] 通过参考附图阅读下文的详细描述，本发明示例性实施方式的上述以及其他目的、特征和优点将变得易于理解。在附图中，以示例性而非限制性的方式示出了本发明的若干实施方式，其中：

[0048] 图1示意性地示出了根据本发明实施方式的应用场景示意图；

[0049] 图2示意性地示出了根据本发明实施方式的页面获取方法一实施例流程示意图；

[0050] 图3示意性地示出了本发明方式中对加密后的页面数据进行解密处理的方法的流程示意图；

[0051] 图4示意性地示出根据本发明实施方式的页面获取方法另一实施例流程示意图；

[0052] 图5示意性地示出了本发明实施方式中确定HTTP请求中包含指定加密标识的流程示意图；

[0053] 图6示意性地示出本发明实施方式中将加载资源白名单返回给用户设备的流程示意图；

[0054] 图7示意性地示出本发明实施方式中将加密后的页面数据返回给用户设备的流程示意图；

[0055] 图8示意性地示出本发明实施方式提供的用户设备与网络侧交互的页面获取方法的一实施例的流程性示意图；

[0056] 图9示意性地示出了根据本发明实施方式提供的用户设备与网络侧交互的页面获取方法的另一实施例的流程示意图。

[0057] 图10示意性地示出了根据本发明一实施例的页面获取装置的结构示意图；

[0058] 图11示意性地示出了根据本发明另一实施例的页面获取装置的结构示意图；

[0059] 图12示意性地示出了根据本发明又一实施例的页面获取装置的结构示意图；

[0060] 图13示意性地示出了根据本发明再一实施例的页面获取装置的结构示意图；

[0061] 图14示意性地示出了根据本发明一实施例的用于用户页面获取方法的程序产品示意图；

[0062] 图15示意性地示出了根据本发明又一实施例的用于页面获取方法的程序产品示意图。

[0063] 在附图中，相同或对应的标号表示相同或对应的部分。

具体实施方式

[0064] 下面将参考若干示例性实施方式来描述本发明的原理和精神。应当理解，给出这些实施方式仅仅是为了使本领域技术人员能够更好地理解进而实现本发明，而并非以任何方式限制本发明的范围。相反，提供这些实施方式是为了使本公开更加透彻和完整，并且能够将本公开的范围完整地传达给本领域的技术人员。

[0065] 本领域技术人员知道，本发明的实施方式可以实现为一种系统、装置、设备、方法或计算机程序产品。因此，本公开可以具体实现为以下形式，即：完全的硬件、完全的软件(包括固件、驻留软件、微代码等)，或者硬件和软件结合的形式。

[0066] 根据本发明的实施方式，提出了一种页面获取方法和装置。

[0067] 在本文中，需要理解的是，附图中的任何元素数量均用于示例而非限制，以及任何

命名都仅用于区分，而不具有任何限制含义。

[0068] 下面参考本发明的若干代表性实施方式，详细阐释本发明的原理和精神。

[0069] 发明概述

[0070] 本发明人发现，现有技术中，为了避免基于HTTP协议的页面获取方式所造成的页面被篡改的问题，将HTTP协议替换为HTTPS协议。但是，将HTTP协议替换为HTTPS协议涉及运维配置修改、代码修改以及网络设备性能优化等操作，需要在网络侧进行的改动较多，成本较高。因此，现有技术中缺乏一种改进的页面获取方法，既能够节约成本又能够防止页面被篡改。

[0071] 为此，本发明提供了一种页面获取方法和装置，其中，基于用户设备侧的页面获取方法可以包括：截取用于获取指定页面的超文本传协议HTTP请求；将指定加密标识添加到所述HTTP请求中；将添加指定加密标识的HTTP请求发送给网络侧；基于网络侧的页面获取方法可以包括：接收用户设备发送的获取指定页面的超文本传输协议HTTP请求；确定所述HTTP请求中包含指定加密标识时，获取相应的指定加密方式；按照所述获取的指定加密方式将所述指定页面对应的页面数据进行加密；将所述加密后的页面数据返回给所述用户设备。

[0072] 在介绍了本发明的基本原理之后，下面具体介绍本发明的各种非限制性实施方式。

[0073] 应用场景总览

[0074] 首先参考图1，如图1所示，为本发明实施例提供的页面获取方法的应用场景示意图，包括用户设备101和服务器102，其中，服务器102位于网络侧，用户设备101中包括浏览器(或者APP中的浏览器组件)和网络中间层。更具体的，当用户设备101的操作系统为安卓操作系统时，可将自定义的组件作为网络中间层，当用户设备101的操作系统为IOS操作系统时，可将IOS系统自带的NSPprotocol作为网络中间层。

[0075] 用户设备中的网络中间层截取浏览器或者浏览器组件发送的用于获取指定页面的超文本传协议HTTP请求；将指定加密标识添加到所述HTTP请求中；将添加指定加密标识的HTTP请求发送给网络侧的服务器102。服务器102接收用户设备发送的获取指定页面的超文本传输协议HTTP请求；确定所述HTTP请求中包含指定加密标识时，获取相应的指定加密方式；按照所述获取的指定加密方式将所述指定页面对应的页面数据进行加密；将所述加密后的页面数据返回给所述用户设备。用户设备101中还可安装有具有浏览页面功能的应用程序，这里不做限定。

[0076] 示例性方法

[0077] 下面结合图1的应用场景，参考图2～图9来描述根据本发明示例性实施方式的页面获取方法。需要注意的是，上述应用场景仅是为了便于理解本发明的精神和原理而示出，本发明的实施方式在此方面不受任何限制。相反，本发明的实施方式可以应用于适用的任何场景。

[0078] 图2为本发明提供的一种页面获取方法一实施例的流程示意图，主要包括用户设备从网络侧获取页面的流程，执行主体可以为应用场景总览中的用户设备101，如图2所示，本发明实施例提供的一种页面获取方法，包括如下步骤：

[0079] 步骤201，截取用于获取指定页面的超文本传协议HTTP请求。

[0080] 具体实施时，监测到浏览器或者浏览器组件基于HTTP协议发出HTTP请求后，截取该HTTP请求，以便对该HTTP请求进行处理。

[0081] 步骤202，将指定加密标识添加到所述HTTP请求中。

[0082] 本步骤中，在截取的HTTP请求中添加加密标识，优选可将指定加密标识添加到所述HTTP请求的头部。其中，用户设备与网络侧预先约定不同加密标识对应的加密方式，用户设备将加密标识添加到HTTP请求中，网络侧接收到添加加密标识的HTTP请求时，根据保存的加密标识与加密方式的对应关系以及HTTP请求中的加密标识，确定加密标识对应的加密方式。其中，具体的加密方式可参考现有的加密算法，同理，相应的解密方式也可参考现有的解密算法，这里不做详述。本发明实施例中的加密标识优选用于表示获取按照该加密标识对应的加密方式进行加密后的页面数据，即如果HTTP请求中携带该标识，则表示获取的页面数据为使用该加密标识所对应的加密方式加密后的页面数据。这只是对针对加密标识的一种优选限定方式，除此之外，本发明实施例中的加密标识还可以用于表示获取未加密的页面数据，或者，用于表示获取使用预先设定的一种默认加密方式进行加密后的页面数据，即，本发明中的加密标识可用于表示请求获取的页面数据是否需要加密、使用预设的一种默认方式加密、或使用预设的多种加密方式中的某一种方式进行加密。

[0083] 步骤203，将添加指定加密标识的HTTP请求发送给网络侧。

[0084] 本步骤中，用户设备基于HTTP协议将添加指定加密标识的HTTP请求发送给网络侧。

[0085] 图2提供的实施例，在HTTP协议的基础上，将添加加密标识的HTTP请求发送给网络侧，以从网络侧获取所请求的页面对应的加密后的页面数据，从而能够防止用户设备请求的页面被篡改，并且，依然使用HTTP协议进行通信，不需要将HTTP协议替换为HTTPS协议，节约了成本。

[0086] 执行步骤203之后，网络侧针对用户设备发送的HTTP请求会返回用户设备请求的页面对应的页面数据，此时，本发明实施例提供的页面获取方法还包括以下内容：

[0087] 步骤204，截取所述网络侧发送的以指定加密方式加密后的页面数据，所述页面数据为所述指定页面对应的页面数据。

[0088] 其中，所述指定加密方式为所述指定加密标识对应的加密方式。

[0089] 步骤205，按照所述指定加密方式对应的解密方式，对所述加密后的页面数据进行解密处理。

[0090] 步骤206，根据解密处理后的页面数据生成所述指定页面并显示。

[0091] 具体实施时，用户设备向网络侧发送添加指定加密标识的HTTP请求后，网络侧返回已按照相应加密方式(与指定加密标识相对应的指定加密方式)加密后的页面数据。用户设备获取网络侧返回的加密后页面数据，并按照与指定加密标识相对应的指定加密方式对应的解密方式，对网络侧返回的加密后的页面数据进行解密，按照解密后的页面数据生成指定页面并显示。具体的，按照页面数据生成页面的方式可参考现有技术，这里不做详述。

[0092] 本发明实施例，用户设备和网络侧之间传输的页面数据均为加密后的页面数据，能够防止用户设备请求的页面被恶意篡改，用户设备和网络侧之间基于HTTP协议通信，避免了使用HTTPS协议，节约了成本。

[0093] 具体的，网络侧返回指定页面对应的页面数据包括所述指定页面的HTML数据，所

述HTML数据包括文本数据、JS链接地址和资源数据链接地址。其中，HTML的中文全称为超文本标记语言，英文全称为HyperText Markup Language，JS为JavaScript(一种脚本语言)的缩写，本发明实施例中HTML数据中的文本数据为页面中的文本对应的数据，资源数据链接地址为页面中的图片、视频、音频等资源对应的链接地址，JS链接地址为页面中由JS脚本控制的部分对应的JS执行脚本的链接地址，比如页面中的提交按钮对应的JS执行脚本的链接地址。优选地，可利用图3提供的内容，按照所述指定加密方式对应的解密方式，对所述加密后的页面数据进行解密处理：

[0094] 步骤301，按照所述指定加密方式对应的解密方式，对所述加密后的页面数据进行解密，得到所述指定页面的解密后的HTML数据。

[0095] 本步骤中，对加密后页面数据进行解密，得到指定页面对应的解密后的HTML数据。

[0096] 步骤302，根据所述HTML数据中的JS链接地址，从所述网络侧获取所述JS链接地址对应的已按照所述指定加密方式加密后的JS数据。

[0097] 具体实施时，网络侧预先保存JS链接对应的JS数据，并且网络侧预先保存的JS数据为已按照各个加密方式进行加密后的JS数据和未加密的JS数据。用户设备根据HTML数据中的JS链接地址，从网络侧获取JS链接地址对应的已按照指定加密方式加密后的JS数据。其中，针对同一JS数据，按照不同加密方式加密后的该JS数据的JS链接地址不同，未加密的该JS数据的JS链接地址与加密后的该JS数据的JS链接地址也不同，比如：未加密的JS数据的链接地址为a，加密后的该JS数据的链接地址为Xa，其中，X用于表示不同的加密方式，X为1时，加密方式为第一种加密方式，X为2时表示第二种加密方式，以此类推，当然，加密后的JS数据的链接地址的形式也可以为其它形式，这里不做限定。

[0098] 本发明实施例中，网络侧返回给用户设备的JS链接地址即为指定加密方式对应的JS链接地址，用户设备可直接根据该JS链接地址获取已按照指定加密方式加密后的JS数据。

[0099] 步骤303，按照所述指定加密方式对应的解密方式，对所述已按照所述指定加密方式加密后的JS数据进行解密，得到所述指定页面的JS数据。

[0100] 步骤304，根据所述HTML数据中的资源数据链接地址，从所述网络侧获取所述资源数据链接地址对应的资源数据。

[0101] 具体的，根据资源数据链接地址，从网络侧获取资源数据链接地址对应的资源数据。其中，步骤302和步骤304的先后顺序可不做限定，也可先执行步骤304，再执行步骤302，或者步骤302和步骤304同时执行。

[0102] 作为一种优选地实施方式，本发明实施例提供的页面获取方法还截取所述网络侧发送的以指定加密方式加密后的加载资源白名单；按照所述指定加密方式对应的解密方式，对所述加密后的加载资源白名单进行解密处理，得到解密后的加载资源白名单，所述加载资源白名单中包括所述指定页面中受信任的链接地址。其中，加载资源白名单CSP中包含指定页面中受信任的链接地址，即CSP中的链接地址为安全级别较高的链接地址，CSP中的链接地址包括资源数据连接地址。得到解密后的加载资源白名单后，可按照以下方式根据所述HTML数据中的资源数据链接地址，从所述网络侧获取所述资源数据链接地址对应的资源数据：

[0103] 确定所述资源数据链接地址为所述加载资源白名单中的资源数据链接地址时，从

所述服务器获取所述资源数据链接地址对应的资源数据。

[0104] 这种获取资源数据连接地址对应的资源数据的方式，可保证资源数据链接地址的可靠性，进一步提高获取的资源数据的安全性。

[0105] 图4为本发明提供的一种页面获取方法一实施例的流程示意图，主要包括网络侧向用户设备返回页面数据的流程，执行主体可以为应用场景总览中的服务器102，如图4所示，本发明实施例提供的一种页面获取方法，包括如下步骤：

[0106] 步骤401，接收用户设备发送的获取指定页面的超文本传输协议HTTP请求。

[0107] 步骤402，判断所述HTTP请求中是否包含指定加密标识，如果是，执行步骤403，否则，执行步骤406。

[0108] 具体实施时，可判断HTTP请求的头部是否包含指定加密标识。

[0109] 步骤403，获取相应的指定加密方式。

[0110] 本步骤中，当HTTP请求中包含指定加密标识时，确定与该指定加密标识相对应的指定加密方式，其中，网络侧预先存储加密标识与加密方式的对应关系，如果指定加密方式当前的含义为获取未加密的页面数据，则指定步骤406。

[0111] 步骤404，按照所述获取的指定加密方式将所述指定页面对应的页面数据进行加密。

[0112] 本步骤中，按照指定加密方式，对指定页面对应的页面数据进行加密，其中，对页面数据的解释可参考用户设备侧的页面获取方法中对页面数据的解释，这里不做赘述。

[0113] 步骤405，将所述加密后的页面数据返回给所述用户设备。

[0114] 本步骤中，可通过针对用户设备侧发送的HTTP请求的HTTP响应，将加密后的页面数据返回给用户设备。具体可将加密后的页面数据编辑到HTTP响应的头部的后面。

[0115] 步骤406，将所述指定页面对应的未加密的页面数据返回给所述用户设备。

[0116] 本步骤中，HTTP请求中未携带加密标识，可确定用户终端通过HTTP请求获取未加密的页面数据，此时可通过针对用户设备侧发送的HTTP请求的HTTP响应，将未加密的页面数据返回给用户设备。

[0117] 具体实施时，可采用图5提供的内容，确定所述HTTP请求中包含指定加密标识：

[0118] 步骤501，判断所述HTTP请求的头部的指定字段是否为预设值，如果是，执行步骤502，否则，执行步骤503。

[0119] 步骤502，确定所述HTTP请求中包含指定加密标识。

[0120] 步骤503，确定所述HTTP请求中未包含指定加密标识。

[0121] 作为一种优选地实施方式，还可以将针对指定页面的加载资源白名单与加密后的页面数据一起返回给用户设备，具体可按照图6提供的内容，将加载资源白名单返回给用户设备：

[0122] 步骤601，从针对所述HTTP请求的HTTP响应消息的头部获取加载资源白名单。

[0123] 其中，针对加载资源白名单的具体说明，可参考用户设备针对加载资源白名单的说明，这里不做赘述。

[0124] 步骤602，按照所述获取的指定加密方式对加载资源白名单进行加密。

[0125] 其中，获取的指定加密方式即步骤403中所获取的相应的指定加密方式

[0126] 步骤603，将所述加密后的加载资源白名单返回给所述用户设备。

[0127] 现有技术中，网络侧会将加载资源白名单携带在该HTTP响应消息的头部返回给用户设备，但并不会对该加载资源白名单进行加密。本优选实施方式，通过截取加载资源白名单，并对加载资源白名单按照指定加密方式加密后，和页面数据一起返回给用户设备，从而保证加载资源白名单不被恶意攻击。具体实施时，可将加密后的加载资源白名单与页面数据并列添加到HTTP响应的头部的后面，返回给用户设备。

[0128] 可按照图7提供的内容，将所述加密后的页面数据返回给所述用户设备：

[0129] 步骤701，确定所述获取的指定加密方式对应的JS链接地址，其中，所述JS链接地址对应的JS数据为所述指定页面对应的JS数据，并且该JS数据预先按照所述获取的指定加密方式进行加密。

[0130] 具体实施时，网络侧针对同一JS数据，保存了该JS数据经过不同加密方式加密后，所对应的JS链接地址，即，不同加密方式加密后的该JS数据对应的JS链接地址的形式不同。具体的解释可参考针对步骤302的详细说明，这里不做赘述。网络侧预先保存了各个JS数据、加密方式以及JS链接地址的对应关系，可根据用户设备请求获取的指定页面以及用户设备侧指示的指定加密方式，获取该指定加密方式对应的该指定页面的JS数据对应的JS链接地址。

[0131] 步骤702，将获取的指定加密方式对应的JS链接地址放置在所述指定页面的HTLM数据中。

[0132] 本步骤中，页面数据包括HTML数据，HTML数据包括JS链接地址。

[0133] 步骤703，将所述指定页面的HTLM数据按照所述获取的指定加密方式加密后返回给所述用户设备。

[0134] 其中，针对任一JS数据，使用不同的加密方式加密后的所述任一JS数据对应的JS链接地址不同，未加密的所述任一JS数据以及预先按照各个加密方式进行加密后的所述任一JS数据预先存储在备份服务器CND中。网络侧包括原服务器和多个备份服务器，且每个备份服务器中预先备份了原服务器中的页面数据，具体实施时，用户设备优选与距离其最近的一个服务器(原服务器或备份服务器)进行通信，以从该服务器获取用户设备请求的页面对应的页面数据。

[0135] 图8为本发明提供的基于用户设备与网络侧交互的页面获取方法一实施例的流程示意图，主要包括网络侧与用户设备之间交互的流程，包括如下步骤：

[0136] 步骤801，用户设备截取用于获取指定页面的超文本传协议HTTP请求。

[0137] 步骤802，用户设备将指定加密标识添加到所述HTTP请求中。

[0138] 本步骤中，将指定加密标识添加到所述HTTP请求的头部。

[0139] 步骤803，用户设备将添加指定加密标识的HTTP请求发送给网络侧。

[0140] 步骤804，网络侧接收用户设备发送的获取指定页面的超文本传输协议HTTP请求。

[0141] 步骤805，网络侧确定所述HTTP请求中包含指定加密标识时，获取相应的指定加密方式。

[0142] 本步骤中，采用如下方式确定所述HTTP请求中包含指定加密标识：

[0143] 判断所述HTTP请求的头部的指定字段是否为预设值；如果是，确定所述HTTP请求中包含指定加密标识。

[0144] 步骤806，网络侧按照所述获取的指定加密方式将所述指定页面对应的页面数据

进行加密。

[0145] 步骤807，网络侧将所述加密后的页面数据返回给所述用户设备。

[0146] 具体实施时，可按照以下方式将所述加密后的页面数据返回给所述用户设备：确定所述获取的指定加密方式对应的JS链接地址，其中，所述JS链接地址对应的JS数据为所述指定页面对应的JS数据，并且该JS数据预先按照所述获取的指定加密方式进行加密；将获取的指定加密方式对应的JS链接地址放置在所述指定页面的HTLM数据中；将所述指定页面的HTLM数据按照所述获取的指定加密方式加密后返回给所述用户设备；其中，针对任一JS数据，使用不同的加密方式加密后的所述任一JS数据对应的JS链接地址不同，未加密的所述任一JS数据以及预先按照各个加密方式进行加密后的所述任一JS数据预先存储在备份服务器中。

[0147] 步骤808，用户设备截取所述网络侧发送的以指定加密方式加密后的页面数据，所述页面数据为所述指定页面对应的页面数据。

[0148] 步骤809，用户设备按照所述指定加密方式对应的解密方式，对所述加密后的页面数据进行解密处理。

[0149] 优选地，按照以下方式实施步骤809：

[0150] 按照所述指定加密方式对应的解密方式，对所述加密后的页面数据进行解密，得到所述指定页面的解密后的HTML数据；根据所述HTML数据中的JS链接地址，从所述网络侧获取所述JS链接地址对应的已按照所述指定加密方式加密后的JS数据；按照所述指定加密方式对应的解密方式，对所述已按照所述指定加密方式加密后的JS数据进行解密，得到所述指定页面的JS数据；并，根据所述HTML数据中的资源数据链接地址，从所述网络侧获取所述资源数据链接地址对应的资源数据。

[0151] 步骤810，用户设备根据解密处理后的页面数据生成所述指定页面并显示。

[0152] 图8提供的实施例中的页面数据包括所述指定页面的超文本标记语言HTML数据，所述HTML数据包括文本数据、JS链接地址和资源数据链接地址。

[0153] 图9为本发明提供的用户设备与网络侧交互的页面获取方法另一实施例的流程示意图，主要包括网络侧与用户设备之间交互的流程，包括如下步骤：

[0154] 步骤901，用户设备截取用于获取指定页面的超文本传协议HTTP请求。

[0155] 步骤902，用户设备将指定加密标识添加到所述HTTP请求的头部。

[0156] 步骤903，用户设备将添加指定加密标识的HTTP请求发送给网络侧。

[0157] 步骤904，网络侧接收用户设备发送的获取指定页面的超文本传输协议HTTP请求。

[0158] 步骤905，网络侧确定所述HTTP请求的头部包含指定加密标识时，获取相应的指定加密方式。

[0159] 步骤906，网络侧按照所述获取的指定加密方式将所述指定页面对应的页面数据进行加密。

[0160] 步骤907，网络侧从针对所述HTTP请求的HTTP响应消息的头部获取加载资源白名单。

[0161] 其中，所述加载资源白名单中包括所述指定页面中受信任的链接地址。

[0162] 步骤908，按照所述获取的指定加密方式对加载资源白名单进行加密。

[0163] 步骤909，网络侧将所述加密后的页面数据以及所述加密后的加载资源白名单编

辑到针对所述HTTP请求的HTTP响应消息的头部的后面，并将编辑后的HTTP响应消息返回给所述用户设备。

[0164] 步骤910，用户设备截取HTTP响应消息，并从该HTTP响应消息的头部的后面获取以指定加密方式加密后的页面数据以及加密后的加载资源白名单。

[0165] 步骤911，用户设备按照所述指定加密方式对应的解密方式，对所述加密后的页面数据以及加密后的加载资源白名单进行解密处理。

[0166] 优选地，按照以下方式实施步骤911：

[0167] 按照所述指定加密方式对应的解密方式，对所述加密后的页面数据进行解密，得到所述指定页面的解密后的HTML数据；根据所述HTML数据中的JS链接地址，从所述网络侧获取所述JS链接地址对应的已按照所述指定加密方式加密后的JS数据；按照所述指定加密方式对应的解密方式，对所述已按照所述指定加密方式加密后的JS数据进行解密，得到所述指定页面的JS数据；并，确定所述资源数据链接地址为所述加载资源白名单中的资源数据链接地址时，从所述服务器获取所述资源数据链接地址对应的资源数据。

[0168] 步骤912，用户设备根据解密处理后的页面数据以及加载资源白名单，生成所述指定页面并显示。

[0169] 示例性设备

[0170] 在介绍了本发明示例性实施方式的页面获取方法之后，接下来，参考图10～图11描述本发明示例性实施方式的页面获取装置。

[0171] 图10为本发明实施例提供的设置于用户设备中的一种页面获取装置的结构示意图，如图10所示，可以包括如下模块：

[0172] 第一截取模块1001，用于截取用于获取指定页面的超文本传协议HTTP请求；

[0173] 添加模块1002，用于将指定加密标识添加到所述HTTP请求中；

[0174] 发送模块1003，用于将添加指定加密标识的HTTP请求发送给网络侧。

[0175] 优选地，本发明实施例提供的页面获取装置还包括：

[0176] 第二截取模块1004，用于截取所述网络侧发送的以指定加密方式加密后的页面数据，所述页面数据为所述指定页面对应的页面数据；

[0177] 解密模块1005，用于按照所述指定加密方式对应的解密方式，对所述加密后的页面数据进行解密处理；

[0178] 显示模块1006，用于根据解密处理后的页面数据生成所述指定页面并显示，其中所述指定加密方式为所述指定加密标识对应的加密方式。

[0179] 优选地，本发明实施例提供的页面获取装置中，所述页面数据包括所述指定页面的超文本标记语言HTML数据，所述HTML数据包括文本数据、JS链接地址和资源数据链接地址。

[0180] 优选地，所述解密模块1005包括：

[0181] 第一解密单元10051，用于按照所述指定加密方式对应的解密方式，对所述加密后的页面数据进行解密，得到所述指定页面的解密后的HTML数据；

[0182] 第一获取单元10052，用于根据所述HTML数据中的JS链接地址，从所述网络侧获取所述JS链接地址对应的已按照所述指定加密方式加密后的JS数据；

[0183] 第二解密单元10053，用于按照所述指定加密方式对应的解密方式，对所述已按照

所述指定加密方式加密后的JS数据进行解密，得到所述指定页面的JS数据；

[0184] 第二获取单元10054，用于根据所述HTML数据中的资源数据链接地址，从所述网络侧获取所述资源数据链接地址对应的资源数据。

[0185] 优选地，所述第二截取模块1004还用于，截取所述网络侧发送的以指定加密方式加密后的加载资源白名单；

[0186] 所述解密模块1005还用于，按照所述指定加密方式对应的解密方式，对所述加密后的加载资源白名单进行解密处理，所述加载资源白名单中包括所述指定页面中受信任的链接地址。

[0187] 优选地，第二获取单元10054具体用于，确定所述资源数据链接地址为所述加载资源白名单中的资源数据链接地址时，从所述服务器获取所述资源数据链接地址对应的资源数据。

[0188] 优选地，所述添加模块1002具体用于，将指定加密标识添加到所述HTTP请求的头部。

[0189] 图11为本发明实施例提供的设置于网络侧的一种页面获取装置的结构示意图，如图11所示，可以包括如下模块：

[0190] 接收模块1101，用于接收用户设备发送的获取指定页面的超文本传输协议HTTP请求；

[0191] 获取模块1102，用于确定所述HTTP请求中包含指定加密标识时，获取相应的指定加密方式；

[0192] 加密模块1103，用于按照所述获取的指定加密方式将所述指定页面对应的页面数据进行加密；

[0193] 发送模块1104，用于将所述加密后的页面数据返回给所述用户设备。

[0194] 优选地，所述获取模块1102包括：

[0195] 判断单元11021，用于判断所述HTTP请求的头部的指定字段是否为预设值；

[0196] 确定单元11022，用于在判断单元11021判断是情况下，确定所述HTTP请求中包含指定加密标识。

[0197] 优选地，所述获取模块1102还用于，从针对所述HTTP请求的HTTP响应消息的头部获取加载资源白名单；

[0198] 所述加密模块1103还用于，按照所述获取的指定加密方式对加载资源白名单进行加密；

[0199] 所述发送模块1104还用于，将所述加密后的加载资源白名单返回给所述用户设备。

[0200] 优选地，所述发送模块1104包括：

[0201] 确定单元11041，用于确定所述获取的指定加密方式对应的JS链接地址，其中，所述JS链接地址对应的JS数据为所述指定页面对应的JS数据，并且该JS数据预先按照所述获取的指定加密方式进行加密；

[0202] 放置单元11042，用于将获取的指定加密方式对应的JS链接地址放置在所述指定页面的HTLM数据中；

[0203] 返回单元11043，用于将所述指定页面的HTLM数据按照所述获取的指定加密方式

加密后返回给所述用户设备;其中,针对任一JS数据,使用不同的加密方式加密后的所述任一JS数据对应的JS链接地址不同,未加密的所述任一JS数据以及预先按照各个加密方式进行加密后的所述任一JS数据预先存储在备份服务器中。

[0204] 示例性设备

[0205] 在介绍了本发明示例性实施方式的页面获取方法和装置之后,接下来,介绍根据本发明的另一示例性实施方式的页面获取装置,该页面获取装置位于用户设备侧。

[0206] 所属技术领域的技术人员能够理解,本发明的各个方面可以实现为系统、方法或程序产品。因此,本发明的各个方面可以具体实现为以下形式,即:完全的硬件实施方式、完全的软件实施方式(包括固件、微代码等),或硬件和软件方面结合的实施方式,这里可以统称为“电路”、“模块”或“系统”。

[0207] 在一些可能的实施方式中,根据本发明的页面获取装置可以至少包括至少一个处理单元、以及至少一个存储单元。其中,所述存储单元存储有程序代码,当所述程序代码被所述处理单元执行时,使得所述处理单元执行本说明书上述“示例性方法”部分中描述的根据本发明基于用户终端侧的各种示例性实施方式的页面获取方法中的步骤。例如,所述处理单元可以执行如图2中所示的步骤201,截取用于获取指定页面的超文本传协议HTTP请求,步骤202,将指定加密标识添加到所述HTTP请求中,步骤203,将添加指定加密标识的HTTP请求发送给网络侧。

[0208] 下面参照图12来描述根据本发明的这种实施方式的页面获取装置120。图12显示的页面获取装置120仅仅是一个示例,不应对本发明实施例的功能和使用范围带来任何限制。

[0209] 如图12所示,页面获取装置120以通用计算设备的形式表现。页面获取装置120的组件可以包括但不限于:上述至少一个处理单元1201、上述至少一个存储单元1202、连接不同系统组件(包括处理单元1201和存储单元1202)的总线1203。

[0210] 总线1203表示几类总线结构中的一种或多种,包括存储器总线或者存储器控制器、外围总线、处理器或者使用多种总线结构中的任意总线结构的局域总线。

[0211] 存储单元1202可以包括易失性存储器形式的可读介质,例如随机存取存储器(RAM)12021和/或高速缓存存储器12022,还可以进一步包括只读存储器(ROM)12023。

[0212] 存储单元1202还可以包括具有一组(至少一个)程序模块12024的程序/实用工具12025,这样的程序模块12024包括但不限于:操作系统、一个或者多个应用程序、其它程序模块以及程序数据,这些示例中的每一个或某种组合中可能包括网络环境的实现。

[0213] 页面获取装置120也可以与一个或多个外部设备1204(例如键盘、指向设备等)通信,还可与一个或者多个使得用户能与页面获取装置120交互的设备通信,和/或与使得该页面获取装置120能与一个或多个其它计算设备进行通信的任何设备(例如路由器、调制解调器等等)通信。这种通信可以通过输入/输出(I/O)接口1205进行。并且,页面获取装置120还可以通过网络适配器1206与一个或者多个网络(例如局域网(LAN),广域网(WAN)和/或公共网络,例如因特网)通信。如图12所示,网络适配器1206通过总线1203与用于页面获取装置120的其它模块通信。应当理解,尽管图中未示出,可以结合页面获取装置120使用其它硬件和/或软件模块,包括但不限于:微代码、设备驱动器、冗余处理单元、外部磁盘驱动阵列、RAID系统、磁带驱动器以及数据备份存储系统等。

[0214] 接下来，介绍根据本发明的又一示例性实施方式的页面获取装置，该页面获取装置位于网络侧。

[0215] 所属技术领域的技术人员能够理解，本发明的各个方面可以实现为系统、方法或程序产品。因此，本发明的各个方面可以具体实现为以下形式，即：完全的硬件实施方式、完全的软件实施方式(包括固件、微代码等)，或硬件和软件方面结合的实施方式，这里可以统称为“电路”、“模块”或“系统”。

[0216] 在一些可能的实施方式中，根据本发明的页面获取装置可以至少包括至少一个处理单元、以及至少一个存储单元。其中，所述存储单元存储有程序代码，当所述程序代码被所述处理单元执行时，使得所述处理单元执行本说明书上述“示例性方法”部分中描述的根据本发明网络侧的各种示例性实施方式的页面获取方法中的步骤。例如，所述处理单元可以执行如图4中所示的步骤401，接收用户设备发送的获取指定页面的超文本传输协议HTTP请求，步骤402，判断所述HTTP请求中是否包含指定加密标识，如果是，执行步骤403，否则，执行步骤406，步骤403，获取相应的指定加密方式，步骤404，按照所述获取的指定加密方式将所述指定页面对应的页面数据进行加密，步骤405，将所述加密后的页面数据返回给所述用户设备，步骤406，将所述指定页面对应的未加密的页面数据返回给所述用户设备。

[0217] 下面参照图13来描述根据本发明的这种实施方式的页面获取装置130。图13显示的页面获取装置130仅仅是一个示例，不应对本发明实施例的功能和使用范围带来任何限制。

[0218] 如图13所示，页面获取装置130以通用计算设备的形式表现。页面获取装置130的组件可以包括但不限于：上述至少一个处理单元1301、上述至少一个存储单元1302、连接不同系统组件(包括处理单元1301和存储单元1302)的总线1303。

[0219] 总线1303表示几类总线结构中的一种或多种，包括存储器总线或者存储器控制器、外围总线、处理器或者使用多种总线结构中的任意总线结构的局域总线。

[0220] 存储单元1302可以包括易失性存储器形式的可读介质，例如随机存取存储器(RAM)13021和/或高速缓存存储器13022，还可以进一步包括只读存储器(ROM)13023。

[0221] 存储单元1302还可以包括具有一组(至少一个)程序模块13024的程序/实用工具13025，这样的程序模块13024包括但不限于：操作系统、一个或者多个应用程序、其它程序模块以及程序数据，这些示例中的每一个或某种组合中可能包括网络环境的实现。

[0222] 页面获取装置130也可以与一个或多个外部设备1304(例如键盘、指向设备等)通信，还可与一个或者多个使得用户能与页面获取装置130交互的设备通信，和/或与使得该页面获取装置130能与一个或多个其它计算设备进行通信的任何设备(例如路由器、调制解调器等等)通信。这种通信可以通过输入/输出(I/O)接口1305进行。并且，页面获取装置130还可以通过网络适配器1306与一个或者多个网络(例如局域网(LAN)，广域网(WAN)和/或公共网络，例如因特网)通信。如图13所示，网络适配器1306通过总线1303与用于页面获取装置130的其它模块通信。应当理解，尽管图中未示出，可以结合页面获取装置130使用其它硬件和/或软件模块，包括但不限于：微代码、设备驱动器、冗余处理单元、外部磁盘驱动阵列、RAID系统、磁带驱动器以及数据备份存储系统等。

[0223] 示例性程序产品

[0224] 在一些可能的实施方式中，本发明提供的页面获取方法的各个方面还可以实现为

一种程序产品的形式，其包括程序代码，当所述程序产品在计算机设备上运行时，所述程序代码用于使所述计算机设备执行本说明书上述“示例性方法”部分中描述的根据本发明基于用户设备侧的各种示例性实施方式的页面获取方法中的步骤，例如，所述计算机设备可以执行如图2中所示的步骤201，截取用于获取指定页面的超文本传协议HTTP请求，步骤202，将指定加密标识添加到所述HTTP请求中，步骤203，将添加指定加密标识的HTTP请求发送给网络侧。

[0225] 上述程序产品可以采用一个或多个可读介质的任意组合。可读介质可以是可读信号介质或者可读存储介质。可读存储介质例如可以是——但不限于——电、磁、光、电磁、红外线、或半导体的系统、装置或器件，或者任意以上的组合。可读存储介质的更具体的例子(非穷举的列表)包括：具有一个或多个导线的电连接、便携式盘、硬盘、随机存取存储器(RAM)、只读存储器(ROM)、可擦式可编程只读存储器(EPROM或闪存)、光纤、便携式紧凑盘只读存储器(CD-ROM)、光存储器件、磁存储器件、或者上述的任意合适的组合。

[0226] 如图14所示，描述了根据本发明的实施方式的用于页面获取的程序产品140，其可以采用便携式紧凑盘只读存储器(CD-ROM)并包括程序代码，并可以在终端设备上运行。然而，本发明的程序产品不限于此，在本文件中，可读存储介质可以是任何包含或存储程序的有形介质，该程序可以被指令执行系统、装置或者器件使用或者与其结合使用。

[0227] 可读信号介质可以包括在基带中或者作为载波一部分传播的数据信号，其中承载了可读程序代码。这种传播的数据信号可以采用多种形式，包括——但不限于——电磁信号、光信号或上述的任意合适的组合。可读信号介质还可以是可读存储介质以外的任何可读介质，该可读介质可以发送、传播或者传输用于由指令执行系统、装置或者器件使用或者与其结合使用的程序。

[0228] 可读介质上包含的程序代码可以用任何适当的介质传输，包括——但不限于——无线、有线、光缆、RF等等，或者上述的任意合适的组合。

[0229] 可以以一种或多种程序设计语言的任意组合来编写用于执行本发明操作的程序代码，所述程序设计语言包括面向对象的程序设计语言—诸如Java、C++等，还包括常规的过程式程序设计语言—诸如“C”语言或类似的程序设计语言。程序代码可以完全地在用户计算设备上执行、部分地在用户设备上执行、作为一个独立的软件包执行、部分在用户计算设备上部分在远程计算设备上执行、或者完全在远程计算设备或服务器上执行。在涉及远程计算设备的情形中，远程计算设备可以通过任意种类的网络——包括局域网(LAN)或广域网(WAN)—连接到用户计算设备，或者，可以连接到外部计算设备(例如利用因特网服务提供商来通过因特网连接)。

[0230] 在另一些可能的实施方式中，本发明提供的页面获取方法的各个方面还可以实现为一种程序产品的形式，其包括程序代码，当所述程序产品在计算机设备上运行时，所述程序代码用于使所述计算机设备执行本说明书上述“示例性方法”部分中描述的根据本发明网络侧的各种示例性实施方式的页面获取方法中的步骤，例如，所述计算机设备可以执行如图4中所示的步骤401，接收用户设备发送的获取指定页面的超文本传输协议HTTP请求，步骤402，判断所述HTTP请求中是否包含指定加密标识，如果是，执行步骤403，否则，执行步骤406，步骤403，获取相应的指定加密方式，步骤404，按照所述获取的指定加密方式将所述指定页面对应的页面数据进行加密，步骤405，将所述加密后的页面数据返回给所述用户设

备，步骤406，将所述指定页面对应的未加密的页面数据返回给所述用户设备。

[0231] 上述程序产品可以采用一个或多个可读介质的任意组合。可读介质可以是可读信号介质或者可读存储介质。可读存储介质例如可以是——但不限于——电、磁、光、电磁、红外线、或半导体的系统、装置或器件，或者任意以上的组合。可读存储介质的更具体的例子(非穷举的列表)包括：具有一个或多个导线的电连接、便携式盘、硬盘、随机存取存储器(RAM)、只读存储器(ROM)、可擦式可编程只读存储器(EPROM或闪存)、光纤、便携式紧凑盘只读存储器(CD-ROM)、光存储器件、磁存储器件、或者上述的任意合适的组合。

[0232] 如图15所示，描述了根据本发明的实施方式的用于页面获取的程序产品150，其可以采用便携式紧凑盘只读存储器(CD-ROM)并包括程序代码，并可以在终端设备上运行。然而，本发明的程序产品不限于此，在本文件中，可读存储介质可以是任何包含或存储程序的有形介质，该程序可以被指令执行系统、装置或者器件使用或者与其结合使用。

[0233] 可读信号介质可以包括在基带中或者作为载波一部分传播的数据信号，其中承载了可读程序代码。这种传播的数据信号可以采用多种形式，包括——但不限于——电磁信号、光信号或上述的任意合适的组合。可读信号介质还可以是可读存储介质以外的任何可读介质，该可读介质可以发送、传播或者传输用于由指令执行系统、装置或者器件使用或者与其结合使用的程序。

[0234] 可读介质上包含的程序代码可以用任何适当的介质传输，包括——但不限于——无线、有线、光缆、RF等等，或者上述的任意合适的组合。

[0235] 可以以一种或多种程序设计语言的任意组合来编写用于执行本发明操作的程序代码，所述程序设计语言包括面向对象的程序设计语言—诸如Java、C++等，还包括常规的过程式程序设计语言—诸如“C”语言或类似的程序设计语言。程序代码可以完全地在用户计算设备上执行、部分地在用户设备上执行、作为一个独立的软件包执行、部分在用户计算设备上部分在远程计算设备上执行、或者完全在远程计算设备或服务器上执行。在涉及远程计算设备的情形中，远程计算设备可以通过任意种类的网络——包括局域网(LAN)或广域网(WAN)—连接到用户计算设备，或者，可以连接到外部计算设备(例如利用因特网服务提供商来通过因特网连接)。

[0236] 应当注意，尽管在上文详细描述中提及了装置的若干模块，但是这种划分仅仅是示例性的并非强制性的。实际上，根据本发明的实施方式，上文描述的两个或更多模块的特征和功能可以在一个模块中具体化。反之，上文描述的一个模块的特征和功能可以进一步划分为由多个模块来具体化。

[0237] 此外，尽管在附图中以特定顺序描述了本发明方法的操作，但是，这并非要求或者暗示必须按照该特定顺序来执行这些操作，或是必须执行全部所示的操作才能实现期望的结果。附加地或备选地，可以省略某些步骤，将多个步骤合并为一个步骤执行，和/或将一个步骤分解为多个步骤执行。

[0238] 虽然已经参考若干具体实施方式描述了本发明的精神和原理，但是应该理解，本发明并不限于所公开的具体实施方式，对各方面的划分也不意味着这些方面中的特征不能组合以进行受益，这种划分仅是为了表述的方便。本发明旨在涵盖所附权利要求的精神和范围内所包括的各种修改和等同布置。

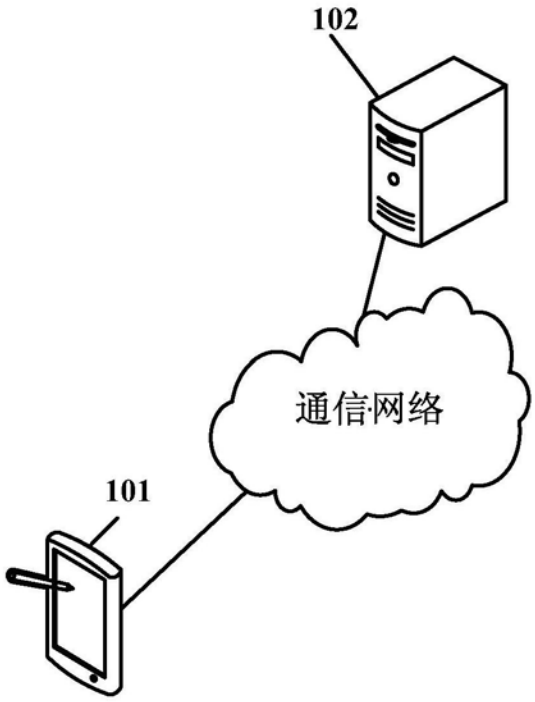


图1

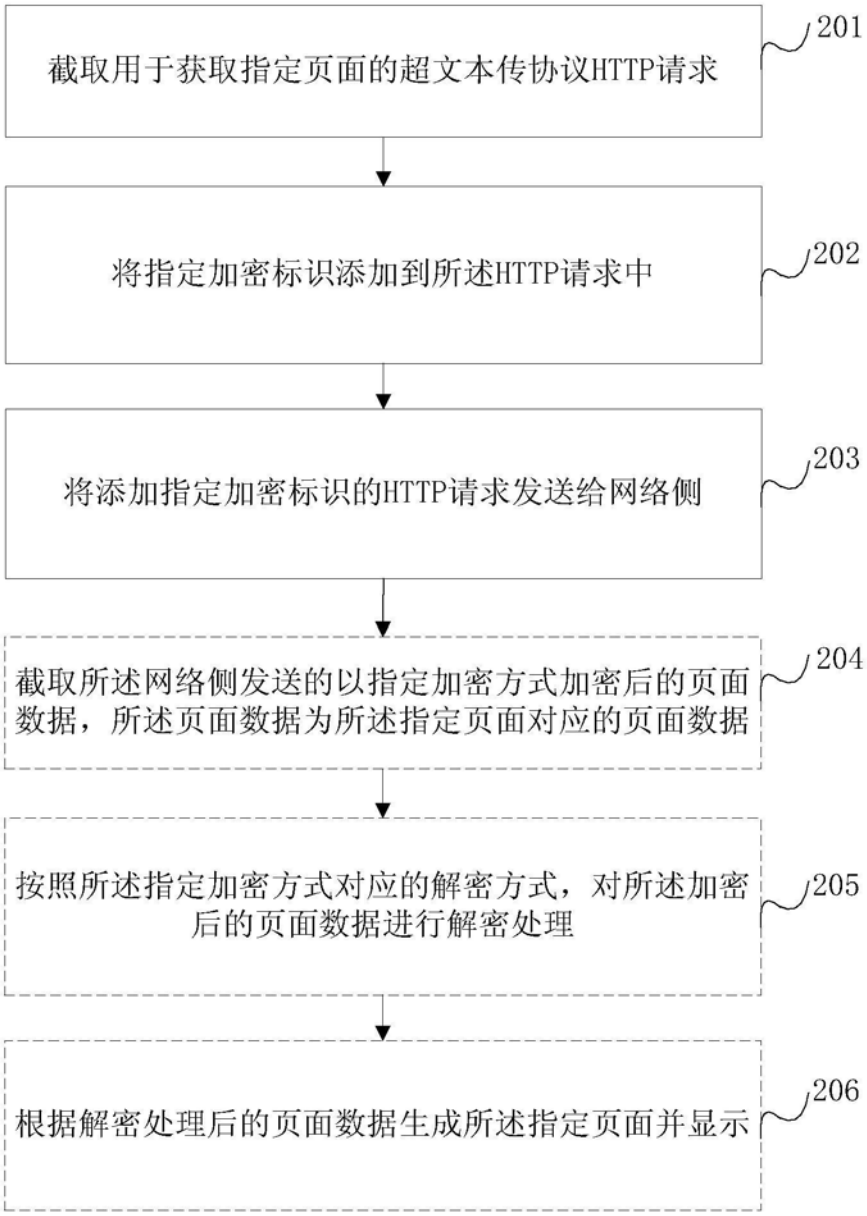

截取用于获取指定页面的超文本传协议HTTP请求
201
将指定加密标识添加到所述HTTP请求中
202
将添加指定加密标识的HTTP请求发送给网络侧
203
截取所述网络侧发送的以指定加密方式加密后的页面数据，所述页面数据为所述指定页面对应的页面数据
204
按照所述指定加密方式对应的解密方式，对所述加密后的页面数据进行解密处理
205
根据解密处理后的页面数据生成所述指定页面并显示
206

图2

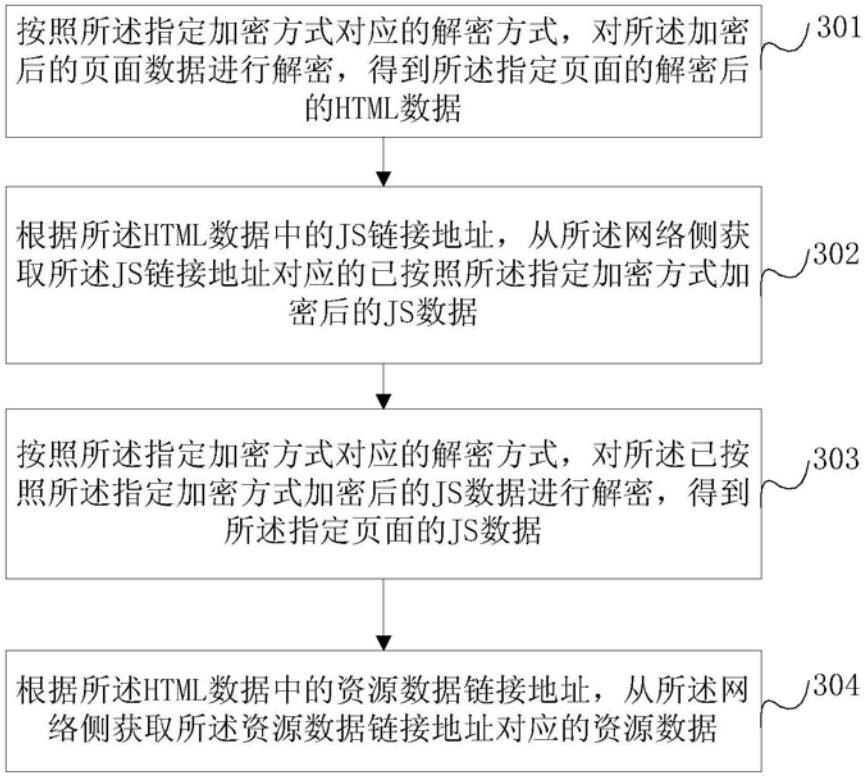

按照所述指定加密方式对应的解密方式，对所述加密后的页面数据进行解密，得到所述指定页面的解密后的HTML数据
301
根据所述HTML数据中的JS链接地址，从所述网络侧获取所述JS链接地址对应的已按照所述指定加密方式加密后的JS数据
302
按照所述指定加密方式对应的解密方式，对所述已按照所述指定加密方式加密后的JS数据进行解密，得到所述指定页面的JS数据
303
根据所述HTML数据中的资源数据链接地址，从所述网络侧获取所述资源数据链接地址对应的资源数据
304

图3

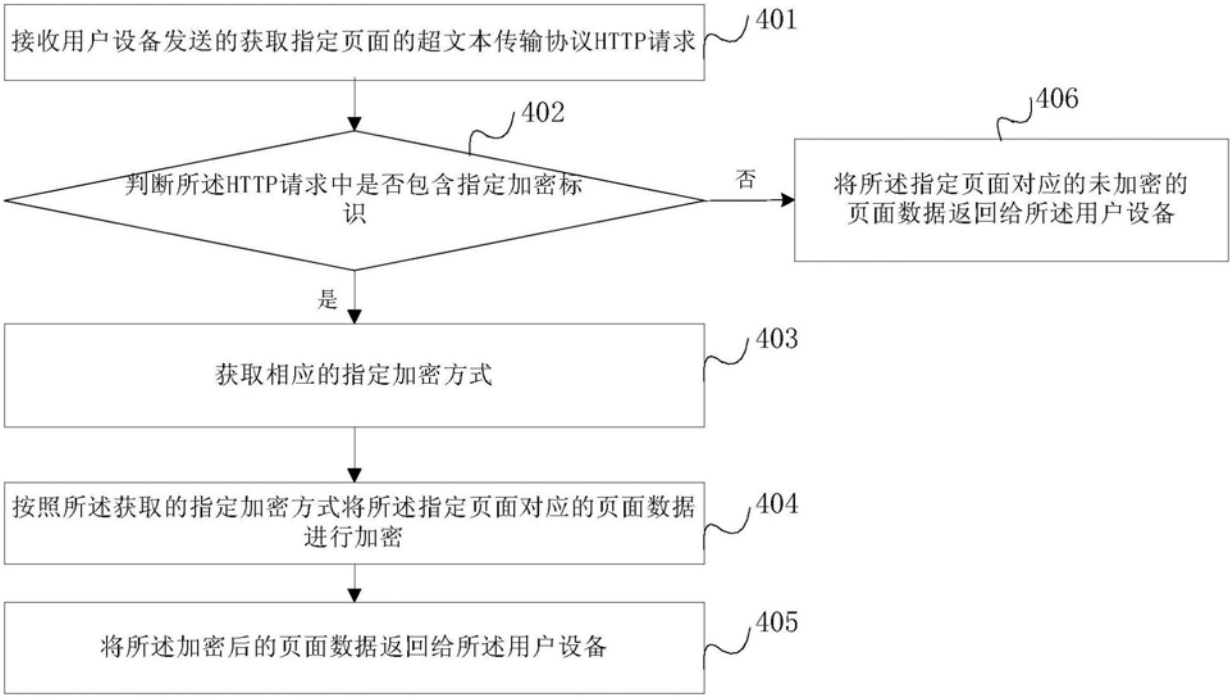

接收用户设备发送的获取指定页面的超文本传输协议HTTP请求
401
判断所述HTTP请求中是否包含指定加密标识
402
否
将所述指定页面对应的未加密的页面数据返回给所述用户设备
406
是
获取相应的指定加密方式
403
按照所述获取的指定加密方式将所述指定页面对应的页面数据进行加密
404
将所述加密后的页面数据返回给所述用户设备
405

图4

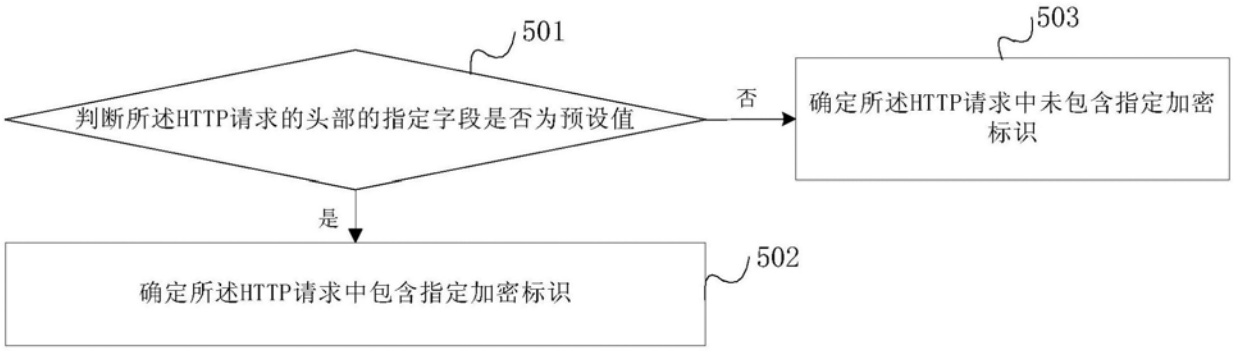

501
判断所述HTTP请求的头部的指定字段是否为预设值
否
503
确定所述HTTP请求中未包含指定加密标识
是
502
确定所述HTTP请求中包含指定加密标识

图5

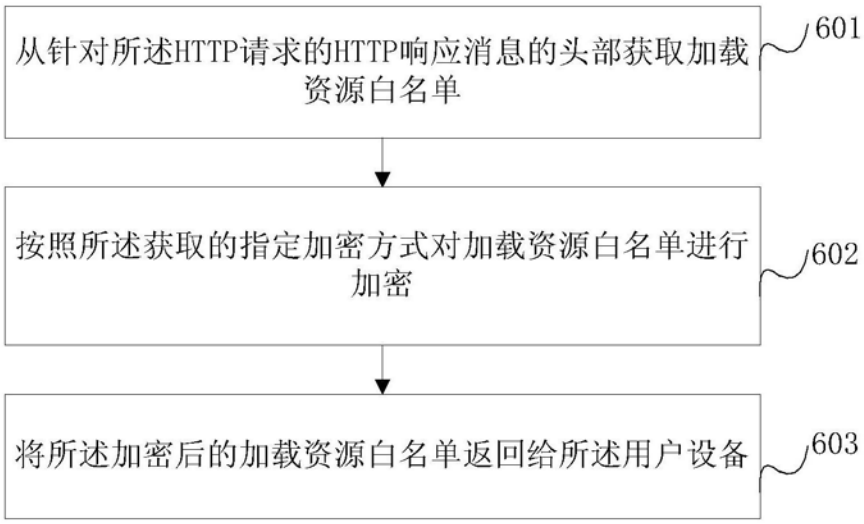

从针对所述HTTP请求的HTTP响应消息的头部获取加载资源白名单
601
按照所述获取的指定加密方式对加载资源白名单进行加密
602
将所述加密后的加载资源白名单返回给所述用户设备
603

图6

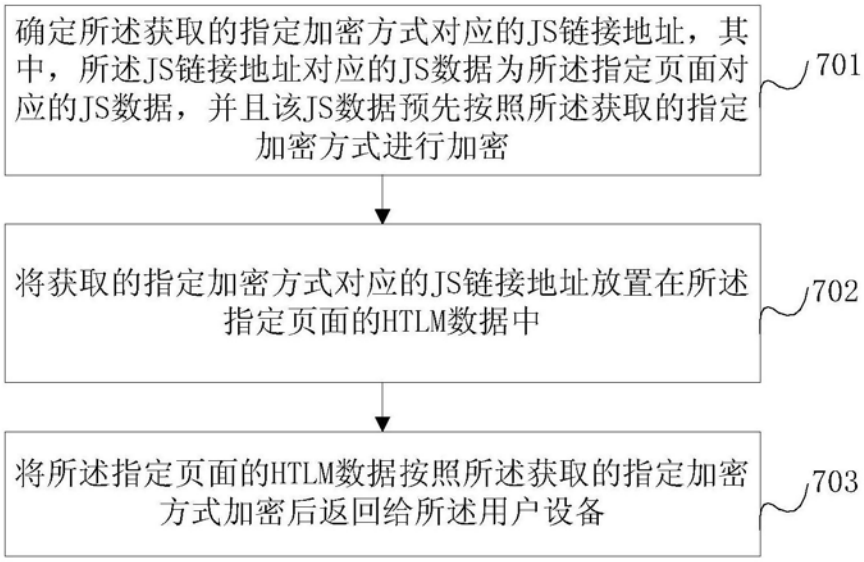

确定所述获取的指定加密方式对应的JS链接地址，其中，所述JS链接地址对应的JS数据为所述指定页面对应的JS数据，并且该JS数据预先按照所述获取的指定加密方式进行加密
701
将获取的指定加密方式对应的JS链接地址放置在所述指定页面的HTLM数据中
702
将所述指定页面的HTLM数据按照所述获取的指定加密方式加密后返回给所述用户设备
703

图7

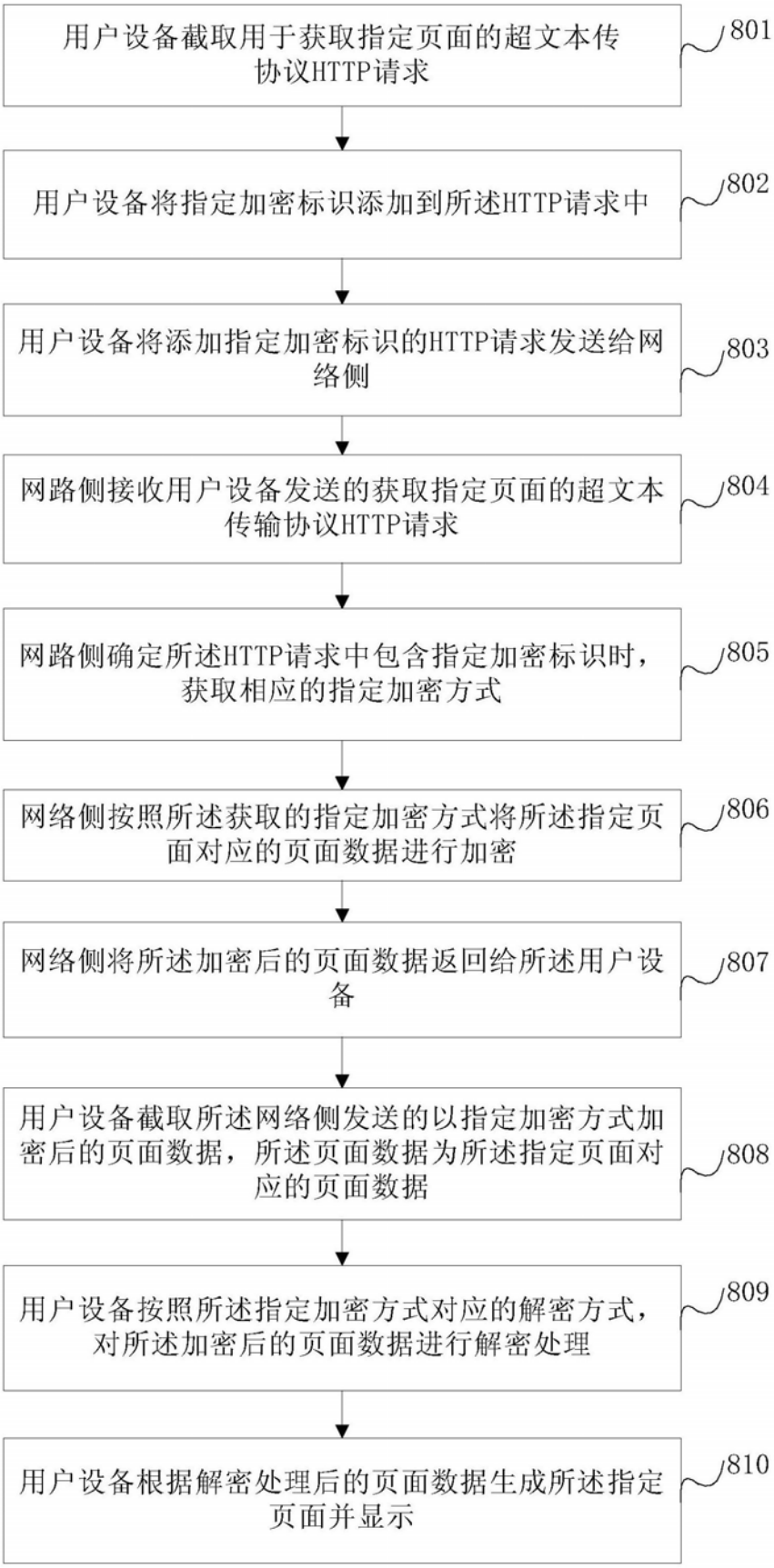

用户设备截取用于获取指定页面的超文本传协议HTTP请求
801
用户设备将指定加密标识添加到所述HTTP请求中
802
用户设备将添加指定加密标识的HTTP请求发送给网络侧
803
网路侧接收用户设备发送的获取指定页面的超文本传输协议HTTP请求
804
网路侧确定所述HTTP请求中包含指定加密标识时，获取相应的指定加密方式
805
网络侧按照所述获取的指定加密方式将所述指定页面对应的页面数据进行加密
806
网络侧将所述加密后的页面数据返回给所述用户设备
807
用户设备截取所述网络侧发送的以指定加密方式加密后的页面数据，所述页面数据为所述指定页面对应的页面数据
808
用户设备按照所述指定加密方式对应的解密方式，对所述加密后的页面数据进行解密处理
809
用户设备根据解密处理后的页面数据生成所述指定页面并显示
810

图8

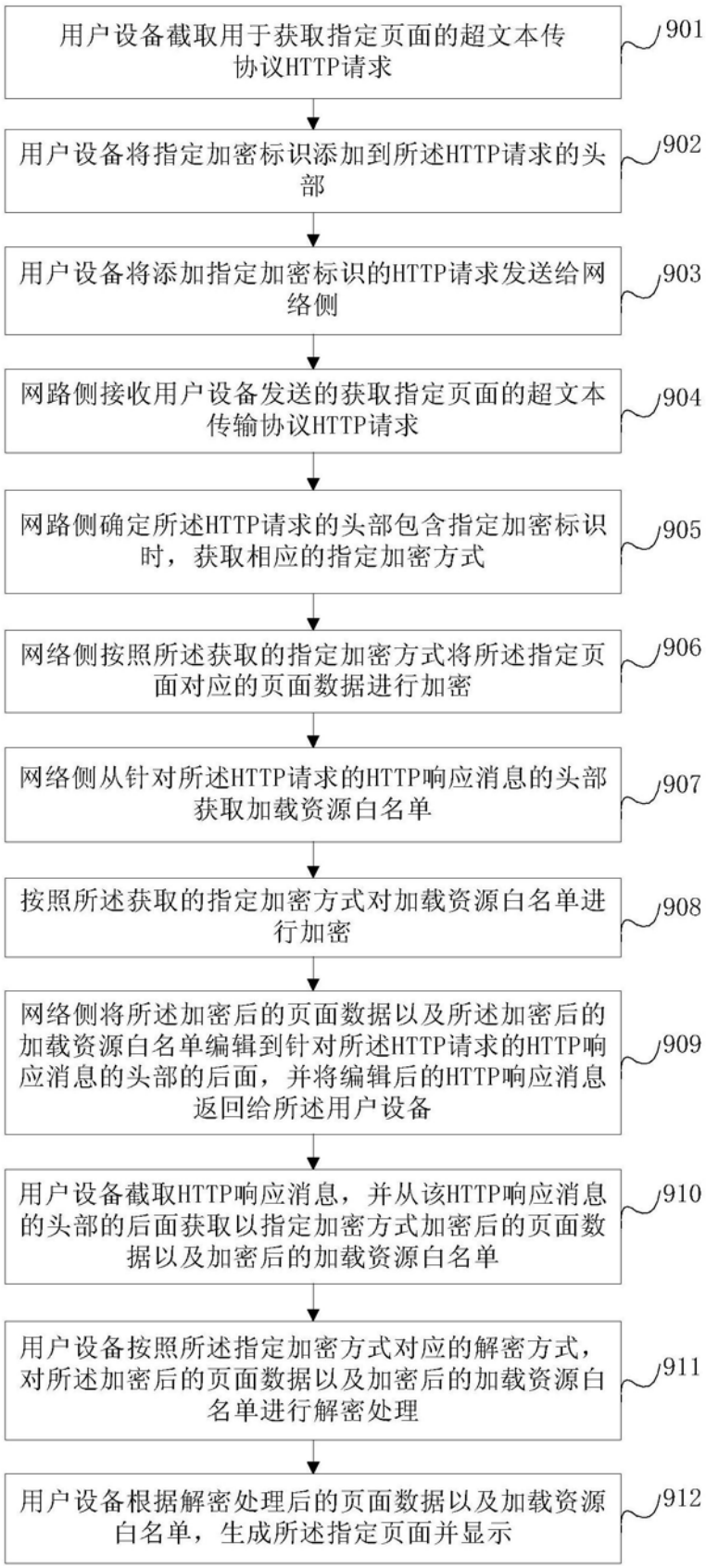

用户设备截取用于获取指定页面的超文本传协议HTTP请求
901
用户设备将指定加密标识添加到所述HTTP请求的头部
902
用户设备将添加指定加密标识的HTTP请求发送给网络侧
903
网路侧接收用户设备发送的获取指定页面的超文本传输协议HTTP请求
904
网路侧确定所述HTTP请求的头部包含指定加密标识时，获取相应的指定加密方式
905
网络侧按照所述获取的指定加密方式将所述指定页面对应的页面数据进行加密
906
网络侧从针对所述HTTP请求的HTTP响应消息的头部获取加载资源白名单
907
按照所述获取的指定加密方式对加载资源白名单进行加密
908
网络侧将所述加密后的页面数据以及所述加密后的加载资源白名单编辑到针对所述HTTP请求的HTTP响应消息的头部的后面，并将编辑后的HTTP响应消息返回给所述用户设备
909
用户设备截取HTTP响应消息，并从该HTTP响应消息的头部的后面获取以指定加密方式加密后的页面数据以及加密后的加载资源白名单
910
用户设备按照所述指定加密方式对应的解密方式，对所述加密后的页面数据以及加密后的加载资源白名单进行解密处理
911
用户设备根据解密处理后的页面数据以及加载资源白名单，生成所述指定页面并显示
912

图9

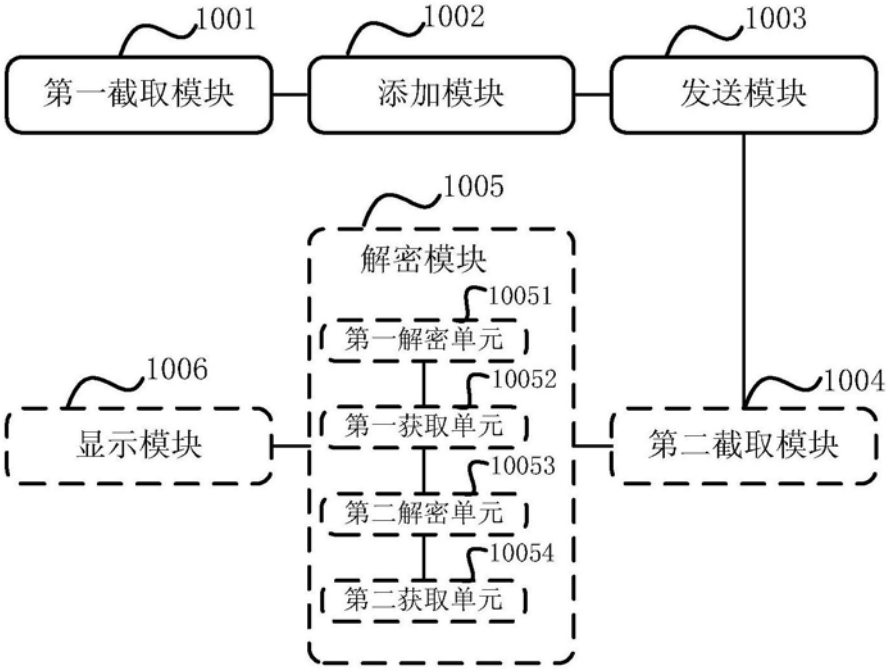

1001
第一截取模块
1002
添加模块
1003
发送模块
1005
解密模块
10051
第一解密单元
10052
第一获取单元
10053
第二解密单元
10054
第二获取单元
1006
显示模块
1004
第二截取模块

图10

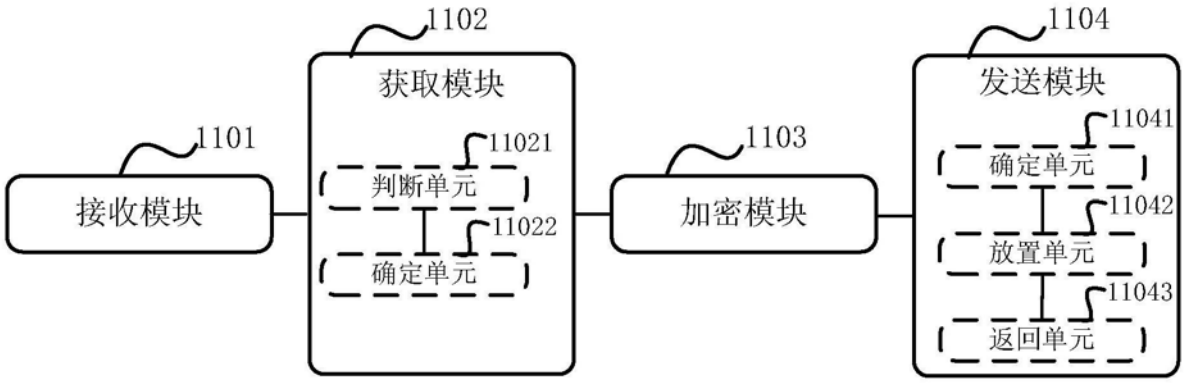

1102
获取模块
11021
判断单元
11022
确定单元
1101
接收模块
1103
加密模块
1104
发送模块
11041
确定单元
11042
放置单元
11043
返回单元

图11

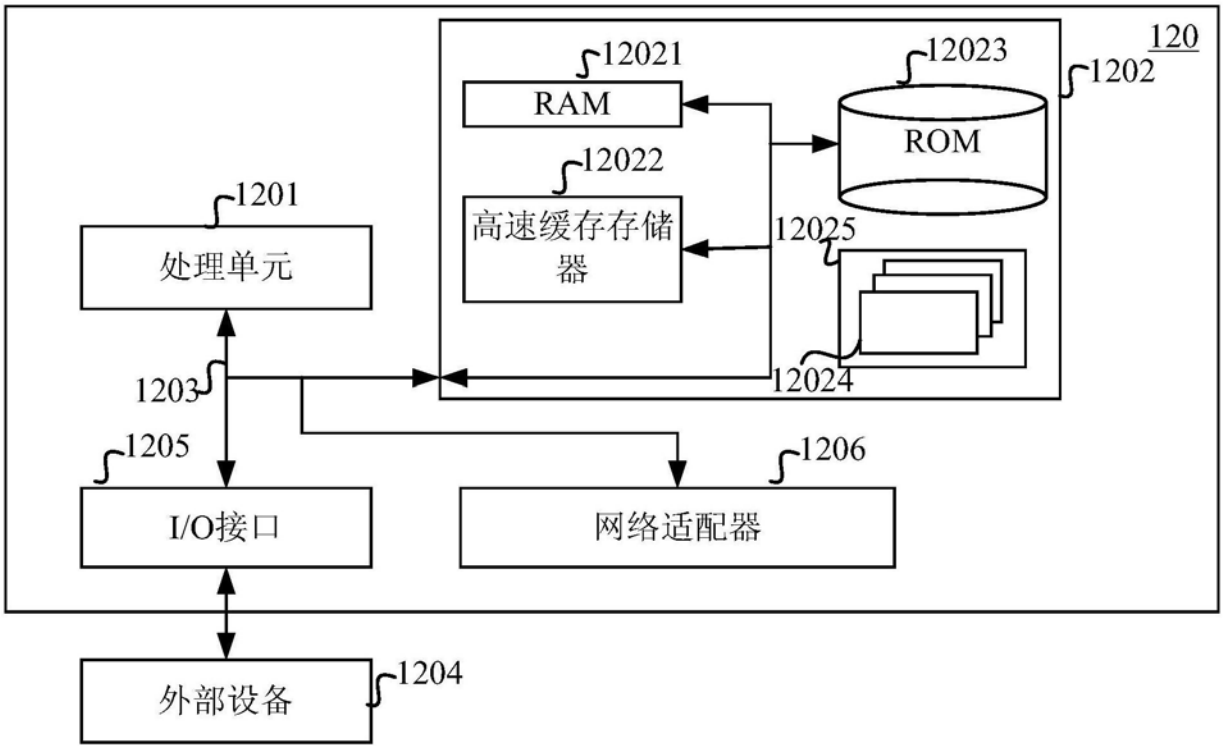

120
12021
RAM
12023
ROM
1202
12022
高速缓存存储器
12025
1201
处理单元
1203
12024
1205
1206
I/O接口
网络适配器
外部设备
1204

图12

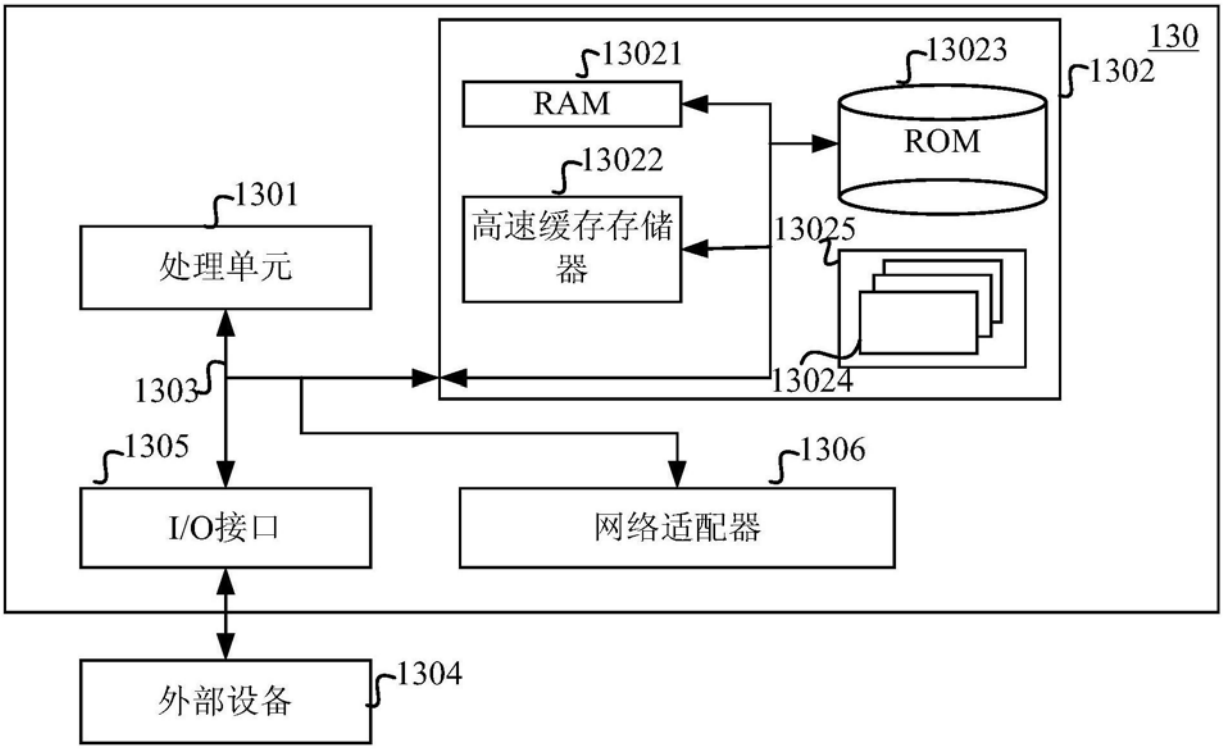

130
13021
RAM
13023
ROM
1302
13022
高速缓存存储器
13025
1301
处理单元
1303
13024
1305
1306
I/O接口
网络适配器
外部设备
1304

图13

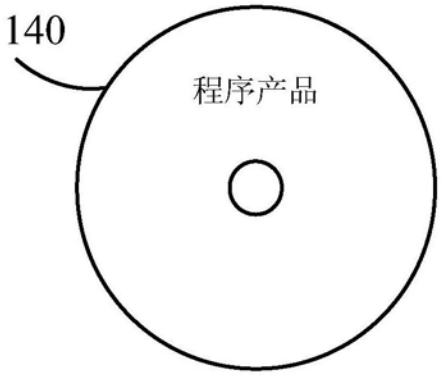


图14

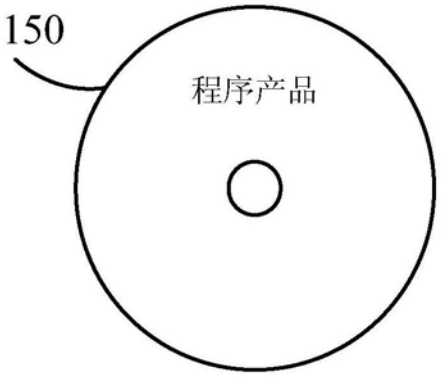


图15