[19] 中华人民共和国国家知识产权局

[51] Int. Cl.
G06F 21/00 (2006.01)
H04L 29/06 (2006.01)

[12] 发明专利申请公布说明书

[21] 申请号 200810129150.7

[43] 公开日 2008 年 11 月 19 日

[11] 公开号 CN 101308533A

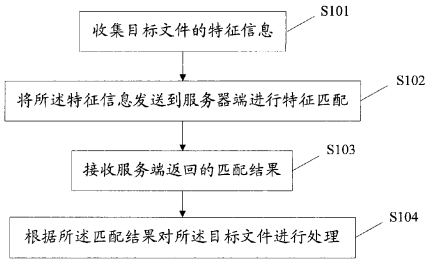
[22] 申请日 2008.6.30
[21] 申请号 200810129150.7
[71] 申请人 华为技术有限公司
地址 518129 广东省深圳市龙岗区坂田华为基地总部办公楼
[72] 发明人 孙灵峰
[74] 专利代理机构 北京中博世达专利商标代理有限公司
代理人 申 健
权利要求书 4 页 说明书 12 页 附图 6 页

[54] 发明名称

病毒查杀的方法、装置和系统

[57] 摘要

本发明实施例公开了一种病毒查杀的方法，在客户端，所述病毒查杀的方法包括：收集目标文件的特征信息；将所述特征信息发送到服务器端进行特征匹配；接收服务端返回的匹配结果；根据所述匹配结果对所述目标文件进行处理。 在服务器端，所述病毒查杀的方法包括：接收客户端发送的目标文件的特征信息；将所述特征信息与特征库中的特征信息进行特征匹配，其中，所述特征库位于服务器端，用于存储带有病毒的目标文件的特征信息；将所述匹配结果发送到客户端，由客户端根据所述匹配结果对所述目标文件进行处理。 本发明实施例还提供一种客户端、服务器端以及病毒查杀的系统，本发明适用于对通信终端进行病毒的查杀，能够节省系统资源。



1、一种病毒查杀的方法，其特征在于，包括:

收集目标文件的特征信息;

将所述特征信息发送到服务器端进行特征匹配;

接收服务端返回的匹配结果;

根据所述匹配结果对所述目标文件进行处理。

2、根据权利要求1所述的病毒查杀的方法，其特征在于，所述收集目标文件的特征信息的步骤包括:

选择需要扫描的目标文件，所述目标文件有唯一的校验值;

提取所述目标文件的特征信息;

存储所述目标文件的特征信息和校验值，所述校验值与所述特征信息为一一对应的关系。

3、根据权利要求1所述的病毒查杀的方法，其特征在于，在所述将所述特征信息发送到服务器端进行特征匹配的步骤之前，还包括:

对所述收集到的特征信息进行加密;

将所述加密后的特征信息转换为支持信息发送的格式的特征信息;

发出将所述特征信息发送到服务器端的指示。

4、根据权利要求1所述的病毒查杀的方法，其特征在于，所述接收服务端返回的匹配结果的步骤包括:

接收所述服务端返回的加密后的匹配结果;

对所述匹配结果进行解密。

5、根据权利要求1所述的病毒查杀的方法，其特征在于，所述根据所述匹配结果对所述目标文件进行处理的步骤包括:

判断所述匹配结果是否正常;

若正常，则提示所述目标文件正常；

若不正常，则提示所述目标文件不正常，并删除所述目标文件。

6、一种病毒查杀的方法，其特征在于，包括：

接收客户端发送的目标文件的特征信息；

将所述特征信息与特征库中的特征信息进行特征匹配，其中，所述特征库位于服务器端，用于存储带有病毒的目标文件的特征信息；

将所述匹配结果发送到客户端，由客户端根据所述匹配结果对所述目标文件进行处理。

7、根据权利要求6所述的病毒查杀的方法，其特征在于，所述接收到的目标文件的特征信息为客户端加密后的特征信息，在所述将所述特征信息与特征库中的特征信息进行特征匹配的步骤之前，还包括：

对所述接收到的特征信息进行解密；

将所述解密后的特征信息转换为可以识别的格式的特征信息。

8、根据权利要求6所述的病毒查杀的方法，其特征在于，所述将所述匹配结果发送到客户端的步骤包括：

对所述匹配结果进行加密；

将所述加密后的匹配结果发送到所述客户端。

9、一种客户端，其特征在于，包括：

特征收集模块，用于收集目标文件的特征信息；

第一发送模块，用于将所述特征信息发送到服务器端进行特征匹配；

第一接收模块，用于接收服务器端返回的匹配结果；

处理模块，用于根据所述匹配结果对所述目标文件进行处理。

10、根据权利要求9所述的客户端，其特征在于，所述特征收集模块包括：

选择单元，用于选择需要扫描的目标文件，所述目标文件有唯一的校验值；

提取单元，用于提取所述目标文件的特征信息；

存储单元，用于存储所述目标文件的特征信息和校验值，所述校验值与所述特征信息为一一对应的关系。

11、根据权利要求9所述的客户端，其特征在于，所述客户端还包括：

第一加密模块，用于对所述收集到的特征信息进行加密；

第一转换模块，用于将所述加密后的特征信息转换为支持信息发送的格式的特征信息；

指示模块，用于发出将所述特征信息发送到服务器端的指示。

12、根据权利要求9所述的客户端，其特征在于，所述第一接收模块接收所述服务器端返回的匹配结果为所述服务器端加密后的匹配结果，所述客户端还包括：

第一解密模块，用于对所述匹配结果进行解密。

13、根据权利要求9所述的客户端，其特征在于，所述处理模块包括：

判断模块，用于判断所述解密后的匹配结果是否正常；

提示模块，用于当判断匹配结果为正常时，提示所述目标文件正常；

删除模块，用于当判断匹配结果为不正常时，提示所述目标文件不正常，并删除所述目标文件。

14、一种服务器端，其特征在于，包括：

第二接收模块，用于接收客户端发送的特征信息；

特征库，用于存储带有病毒的目标文件的特征信息；

特征匹配模块，用于将所述第二接收模块接收到的特征信息与所述特征库中的特征信息进行特征匹配；

第二发送模块，用于将所述特征匹配模块的匹配结果发送到客户端。

15、根据权利要求14所述的服务器端，其特征在于，还包括：

第二解密模块，用于对所述第二接收模块接收到的特征信息进行解密；

第二转换模块，用于将所述第二解密模块解密后的特征信息转换为所述特征匹配模块可以识别的格式的特征信息。

16、根据权利要求14所述的服务器端，其特征在于，还包括：

第二加密模块，用于将所述特征匹配模块生成的匹配结果进行加密；

所述第二发送模块发送到客户端的匹配结果为所述第二加密模块加密后的匹配结果。

17、一种病毒查杀的系统，其特征在于，包括：

客户端，用于收集目标文件的特征信息；

服务器端，用于接收所述客户端发送的特征信息，对所述特征信息进行特征匹配，将所述匹配结果返回给所述客户端，其中，所述客户端还用于接收所述服务器端返回的匹配结果，根据所述匹配结果对所述目标文件进行处理。

18、根据权利要求17所述的病毒查杀的系统，其特征在于，所述客户端还用于判断所述匹配结果是否正常，当判断所述匹配结果正常时，提示所述目标文件正常；及当判断所述匹配结果不正常时，提示所述目标文件不正常，并删除所述目标文件。

病毒查杀的方法、装置和系统

技术领域

本发明涉及通信技术领域，尤其涉及一种病毒查杀的方法、装置和系统。

背景技术

目前，随着网络技术的日益发展，网络病毒也正在威胁着网络用户的安全，给网络用户的隐私和利益带来的很大的风险。移动终端也不例外，通常，移动终端采用安装病毒查杀软件，由移动终端自身进行病毒的查杀。

目前的大多数病毒查杀软件采用特征码查毒与人工杀毒相结合的方法。在移动终端中存储有病毒特征库，在查杀病毒时，将程序体与特征库中的特征码进行匹配，查找出病毒，进而由人工编制解毒代码进行杀毒。

在实现本发明的过程中，发明人发现现有技术中至少存在如下问题:

由于目前针对移动终端的恶意代码数量相对较少，因此特征库占用空间较少，而随着病毒数量的增加，移动终端设备的特征库占用的空间也随着增加，但不能无限的增加，因此，移动终端设备的特征库已不能满足病毒数量日益增加的需要；此外，病毒查找过程是移动终端中进行的，其占用了大量的系统资源。

发明内容

本发明的实施例提供一种病毒查杀的方法、装置和系统，能够节省系统资源。

为达到上述目的，本发明的实施例采用如下技术方案:

一种病毒查杀的方法，包括:

收集目标文件的特征信息;

将所述特征信息发送到服务器端进行特征匹配;

接收服务端返回的匹配结果;

根据所述匹配结果对所述目标文件进行处理。

一种病毒查杀的方法，包括:

接收客户端发送的目标文件的特征信息;

将所述特征信息与特征库中的特征信息进行特征匹配，其中，所述特征库位于服务器端，用于存储带有病毒的目标文件的特征信息;

将所述匹配结果发送到客户端，由客户端根据所述匹配结果对所述目标文件进行处理。

一种客户端，包括:

特征收集模块，用于收集目标文件的特征信息;

第一发送模块，用于将所述特征信息发送到服务器端进行特征匹配;

第一接收模块，用于接收服务器端返回的匹配结果;

处理模块，用于根据所述匹配结果对所述目标文件进行处理。

一种服务器端，包括:

第二接收模块，用于接收客户端发送的特征信息;

特征库，用于存储带有病毒的目标文件的特征信息;

特征匹配模块，用于将所述第二接收模块接收到的特征信息与所述特征库中的特征信息进行特征匹配;

第二发送模块，用于将所述特征匹配模块的匹配结果发送到客户端。

一种病毒查杀的系统，包括:

客户端，用于收集目标文件的特征信息;

服务器端，用于接收所述客户端发送的特征信息，对所述特征信息进行特征匹配，将所述匹配结果返回给所述客户端，其中，所述客户端还用于接收所

述服务器端返回的匹配结果，根据所述匹配结果对所述目标文件进行处理。

本发明实施例提供的病毒查杀的方法、装置和系统，客户端提取目标文件的特征信息，将所述特征信息发送给服务器端，由服务器端根据内部的特征库对所述特征信息进行特征匹配，并将匹配结果返回客户端，客户端根据所述匹配结果对所述目标文件进行处理。与现有技术相比，客户端不必存放大量的病毒特征库，此外，特征匹配的过程在服务器端完成，节省了客户端的资源。

附图说明

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性的前提下，还可以根据这些附图获得其他的附图。

图1为本发明提供的客户端病毒查杀的方法实施例一方法流程图；

图2为本发明提供的客户端病毒查杀的方法实施例二方法流程图；

图3为本发明提供的服务器端病毒查杀的方法实施例一方法流程图；

图4为本发明提供的服务器端病毒查杀的方法实施例二方法流程图；

图5为本发明提供的客户端实施例一结构示意图；

图6为本发明提供的客户端实施例二结构示意图；

图7为本发明提供的服务器端实施例一结构示意图；

图8为本发明提供的服务器端实施例二结构示意图；

图9为本发明实施例提供的病毒查杀的系统结构示意图。

具体实施方式

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作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。

本发明的实施例提供一种病毒查杀的方法、装置和系统。

为使本发明技术方案的优点更加清楚，下面结合附图和实施例对本发明作详细说明。

本发明的实施例提供一种病毒查杀的方法，该方法能够节省系统资源。

实施例一

如图1所示，所述病毒查杀的方法包括:

S101、收集目标文件的特征信息;

S102、将所述特征信息发送到服务器端进行特征匹配;

S103、接收服务端返回的匹配结果;

S104、根据所述匹配结果对所述目标文件进行处理。

本发明实施例提供的病毒查杀的方法，客户端提取目标文件的特征信息，将所述特征信息发送给服务器端，由服务器端根据内部的特征库对所述特征信息进行特征匹配，并将匹配结果返回客户端，客户端根据所述匹配结果对所述目标文件进行处理。与现有技术相比，客户端不必存放大量的病毒特征库，此外，特征匹配的过程在服务器端完成，节省了客户端的资源。

实施例二

如图2所示，所述病毒查杀的方法包括:

S201、选择需要扫描的目标文件，所述目标文件有唯一的校验值;

S202、提取所述目标文件的特征信息;

S203、存储所述目标文件的特征信息和校验值，所述校验值与所述特征信息为一一对应的关系;

其中，所述校验值和特征信息都是唯一表示目标文件的一种标识，对于同一个目标文件，其校验值和特征信息存在对应关系。

当扫描一个目标文件并提取该目标文件的特征信息之后，所述目标文件的特征信息将被存储起来，当下次选择扫描同一个目标文件时，则不需要重新对该目标文件进行扫描和特征信息的提取，只需根据该目标文件的校验值，即可查找到该目标文件的特征信息。

S204、对所述收集到的特征信息进行加密；

S205、将所述加密后的特征信息转换为支持信息发送的格式的特征信息；

S206、发出将所述特征信息发送到服务器端的指示；

S207、将所述特征信息发送到服务器端进行特征匹配；

其中，所述服务器端进行的特征匹配包括：

服务器端在内部特征库中查找是否有所述特征信息，所述特征库中包括带有病毒的目标文件的特征信息。

S208、接收所述服务器端返回的加密后的匹配结果；

S209、对所述匹配结果进行解密；

S210、判断所述匹配结果是否正常；

其中，所述匹配结果为服务器端和客户端事先约定好的一种形式，客户端根据服务器端返回的该种形式的匹配结果，即可得知所述匹配结果是否正常。

例如：服务器端和客户端事先约定好，当服务器端在特征库中查找到与所述目标文件的特征信息相匹配的特征信息时，返回1，表明所述匹配结果不正常，所述目标文件带有病毒；当服务器端没有在特征库中查找到与所述目标文件的特征信息相匹配的特征信息时，返回0，表明所述匹配结果正常，所述目标文件没有病毒。

S211、若正常，则提示所述目标文件正常；

如步骤S210中所述，若匹配结果为0，则表明所述匹配结果正常，提示所述目标文件正常。

S212、若不正常，则提示所述目标文件不正常，并删除所述目标文件。

如步骤S210中所述，若匹配结果为1，则表明所述匹配结果不正常，提示所述目标文件不正常，删除所述目标文件。

因而，利用本发明的实施例病毒查杀的方法，能够节省系统资源。

本发明的实施例提供一种病毒查杀的方法，该方法能够节省系统资源。

实施例一

如图3所示，所述病毒查杀的方法包括：

S301、接收客户端发送的目标文件的特征信息；

S302、将所述特征信息与特征库中的特征信息进行特征匹配，其中，所述特征库位于服务器端，用于存储带有病毒的目标文件的特征信息；

S303、将所述匹配结果发送到客户端，由客户端根据所述匹配结果对所述目标文件进行处理。

本发明实施例提供的病毒查杀的方法，服务器端接收客户端发送的特征信息，将所述特征信息与内部特征库中的特征信息进行特征匹配，并将匹配结果返回给客户端，客户端根据所述匹配结果对所述目标文件进行处理。与现有技术相比，客户端不必存放大量的病毒特征库，此外，特征匹配的过程在服务器端完成，节省了客户端的资源。

实施例二

如图4所示，所述病毒查杀的方法包括：

S401、接收客户端发送的加密后的目标文件的特征信息；

S402、对所述接收到的特征信息进行解密;

S403、将所述解密后的特征信息转换为可以识别的格式的特征信息。

S404、将所述特征信息与特征库中的特征信息进行特征匹配，其中，所述特征库位于服务器端，用于存储带有病毒的目标文件的特征信息;

S405、对所述匹配结果进行加密;

S406、将所述加密后的匹配结果发送到客户端，由客户端根据所述匹配结果对所述目标文件进行处理。

因而，利用本发明的实施例病毒查杀的方法，能够节省系统资源。

本发明的实施例还提供一种客户端，能够节省系统资源。

实施例一

如图5所示，所述客户端包括:

特征收集模块501，用于收集目标文件的特征信息;

第一发送模块502，用于将所述特征信息发送给服务器端进行特征匹配;

第一接收模块503，用于接收服务器端返回的匹配结果;

处理模块504，用于根据所述匹配结果对所述目标文件进行处理。

本发明实施例提供的客户端，客户端提取目标文件的特征信息，将所述特征信息发送给服务器端，由服务器端根据内部的特征库对所述特征信息进行特征匹配，并将匹配结果返回客户端，客户端根据所述匹配结果对所述目标文件进行处理。与现有技术相比，客户端不必存放大量的病毒特征库，此外，特征匹配的过程在服务器端完成，节省了客户端的资源。

实施例二

如图6所示，所述客户端包括:

特征收集模块601，用于收集目标文件的特征信息;

第一发送模块602，用于将所述特征信息发送给服务器端进行特征匹配；

第一接收模块603，用于接收服务器端返回的匹配结果；

处理模块604，用于根据所述匹配结果对所述目标文件进行处理。

如图6所示，所述特征收集模块601包括：

选择单元605，用于选择需要扫描的目标文件，所述目标文件有唯一的校验值；

提取单元606，用于提取所述目标文件的特征信息；

存储单元607，用于存储所述目标文件的特征信息和校验值，所述校验值与所述特征信息为一一对应的关系。

当扫描一个目标文件并提取该目标文件的特征信息之后，所述目标文件的特征信息将被存储单元607保存，当下次选择扫描同一个目标文件时，则不需要重新对该目标文件进行扫描和特征信息的提取，只需根据该目标文件的校验值，从所述存储单元607中即可查找到该目标文件的特征信息。

如图6所示，所述客户端还包括：

第一加密模块608，用于对所述收集到的特征信息进行加密；

第一转换模块609，用于将所述加密后的特征信息转换为支持信息发送的格式的特征信息；

指示模块610，用于发出将所述特征信息发送到服务器端的指示。

如图6所示，所述第一接收模块603接收所述服务器端返回的匹配结果为所述服务器端加密后的匹配结果，所述客户端还包括：

第一解密模块611，用于对所述匹配结果进行解密。

如图6所示，所述处理模块604包括：

判断模块612，用于判断所述解密后的匹配结果是否正常；

提示模块613，用于当判断匹配结果为正常时，提示所述目标文件正常；

删除模块614，用于当判断匹配结果为不正常时，提示所述目标文件不正常，并删除所述目标文件。

其中，所述匹配结果为服务器端和客户端事先约定好的一种形式，客户端根据服务器端返回的该种形式的匹配结果，即可得知所述匹配结果是否正常。

例如：服务器端和客户端事先约定好，当服务器端在特征库中查找到与所述目标文件的特征信息相匹配的特征信息时，返回1，表明所述匹配结果不正常，所述目标文件带有病毒，删除模块614提示所述目标文件不正常，并删除所述目标文件；当服务器端没有在特征库中查找到与所述目标文件的特征信息相匹配的特征信息时，返回0，表明所述匹配结果正常，所述目标文件没有病毒，提示模块613提示所述目标文件正常。

因而，利用本发明的实施例客户端，能够节省系统资源。

其中，所述客户端包括但不仅限于手机、笔记本、PDA等通信终端设备。

本发明的实施例还提供一种服务器端，能够节省系统资源。

实施例一

如图7所示，所述服务器端包括：

第二接收模块701，用于接收客户端发送的特征信息；

特征库702，用于存储带有病毒的目标文件的特征信息；

特征匹配模块703，用于将所述第二接收模块701接收到的特征信息与所述特征库702中的特征信息进行特征匹配；

第二发送模块704，用于将所述特征匹配模块703的匹配结果发送到客户端。

本发明实施例提供的服务器端，服务器端接收客户端发送的特征信息，将所述特征信息与内部特征库中的特征信息进行特征匹配，并将匹配结果返回给

客户端，客户端根据所述匹配结果对所述目标文件进行处理。与现有技术相比，客户端不必存放大量的病毒特征库，此外，特征匹配的过程在服务器端完成，节省了客户端的资源。

实施例二

如图8所示，所述服务器端包括:

第二接收模块801，用于接收客户端发送的特征信息;

特征库802，用于存储带有病毒的目标文件的特征信息;

特征匹配模块803，用于将所述第二接收模块801接收到的特征信息与所述特征库802中的特征信息进行特征匹配;

第二发送模块804，用于将所述特征匹配模块803的匹配结果发送到客户端。

其中，所述匹配结果为服务器端和客户端事先约定好的一种形式，客户端根据服务器端返回的该种形式的匹配结果，即可得知所述匹配结果是否正常。

例如：服务器端和客户端事先约定好，当服务器端在特征库802中查找到与所述目标文件的特征信息相匹配的特征信息时，返回1，表明所述匹配结果不正常，所述目标文件带有病毒；当服务器端没有在特征库802中查找到与所述目标文件的特征信息相匹配的特征信息时，返回0，表明所述匹配结果正常，所述目标文件没有病毒。

如图8所示，所述服务器端还包括:

第二解密模块805，用于对所述第二接收模块801接收到的特征信息进行解密;

第二转换模块806，用于将所述第二解密模块805解密后的特征信息转换为所述特征匹配模块803可以识别的格式的特征信息。

如图8所示，所述服务器端还包括:

第二加密模块807，用于将所述特征匹配模块803生成的匹配结果进行加密；

所述第二发送模块804发送到客户端的匹配结果为所述第二加密模块807加密后的匹配结果。

因而，利用本发明的实施例服务器端，能够节省系统资源。

其中，所述服务器端为可以接收信息的类似网关的设备，该设备有充足的存储空间和良好的兼容性，而且具有信息收发的功能。

本发明的实施例还提供一种病毒查杀的系统，能够节省系统资源。

如图9所示，所述系统包括客户端901及服务器端902；

客户端901用于收集目标文件的特征信息；

服务器端902用于接收所述客户端901发送的特征信息，对所述特征信息进行特征匹配，将所述匹配结果返回给所述客户端901，其中，所述客户端901还用于接收所述服务器端902返回的匹配结果，根据所述匹配结果对所述目标文件进行处理。

本发明实施例提供的病毒查杀的系统，客户端901提取目标文件的特征信息，将所述特征信息发送给服务器端902，由服务器端902根据内部的特征库对所述特征信息进行特征匹配，并将匹配结果返回客户端901，客户端901根据所述匹配结果对所述目标文件进行处理。与现有技术相比，客户端901不必存放大量的病毒特征库，此外，特征匹配的过程在服务器端902完成，节省了客户端901的资源。

其中，所述客户端901还用于判断所述匹配结果是否正常，当判断所述匹配结果正常时，提示所述目标文件正常；及当判断所述匹配结果不正常时，提示所述目标文件不正常，并删除所述目标文件。

其中，所述客户端包括但不仅限于手机、笔记本、PDA等通信终端设备。

其中，所述服务器端为可以接收信息的类似网关的设备，该设备有充足的存储空间和良好的兼容性，而且具有信息收发的功能。

本领域普通技术人员可以理解实现上述实施例方法中的全部或部分流程，是可以通过计算机程序来指令相关的硬件来完成，所述的程序可存储于一计算机可读取存储介质中，该程序在执行时，可包括如上述各方法的实施例的流程。其中，所述的存储介质可为磁碟、光盘、只读存储记忆体（Read-Only Memory，ROM）或随机存储记忆体（Random Access Memory，RAM）等。

以上所述，仅为本发明实施例的具体实施方式，但本发明实施例的保护范围并不局限于此，任何熟悉本技术领域的技术人员在本发明揭露的技术范围内，可轻易想到的变化或替换，都应涵盖在本发明的保护范围之内。因此，本发明实施例的保护范围应该以权利要求的保护范围为准。

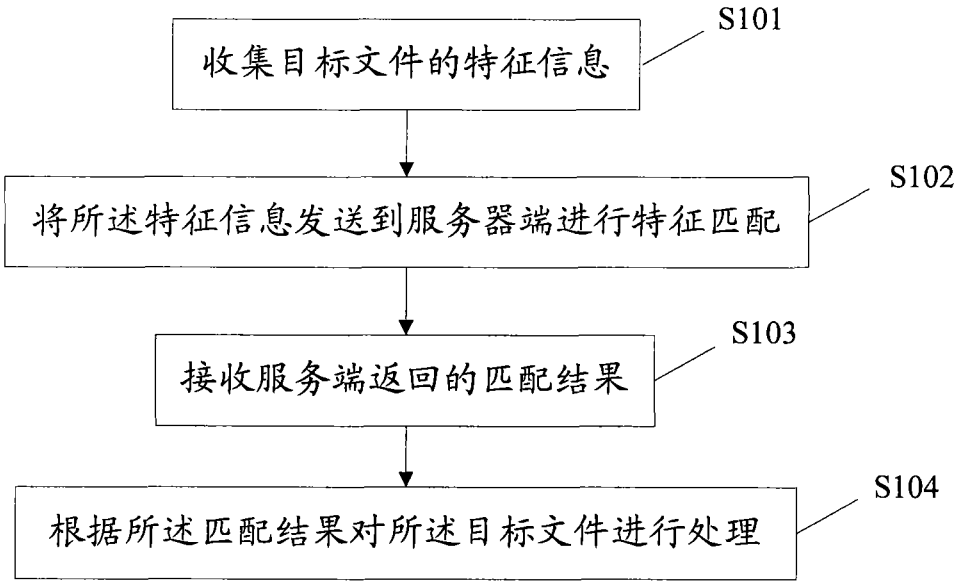

S101
收集目标文件的特征信息
S102
将所述特征信息发送到服务器端进行特征匹配
S103
接收服务端返回的匹配结果
S104
根据所述匹配结果对所述目标文件进行处理

图 1

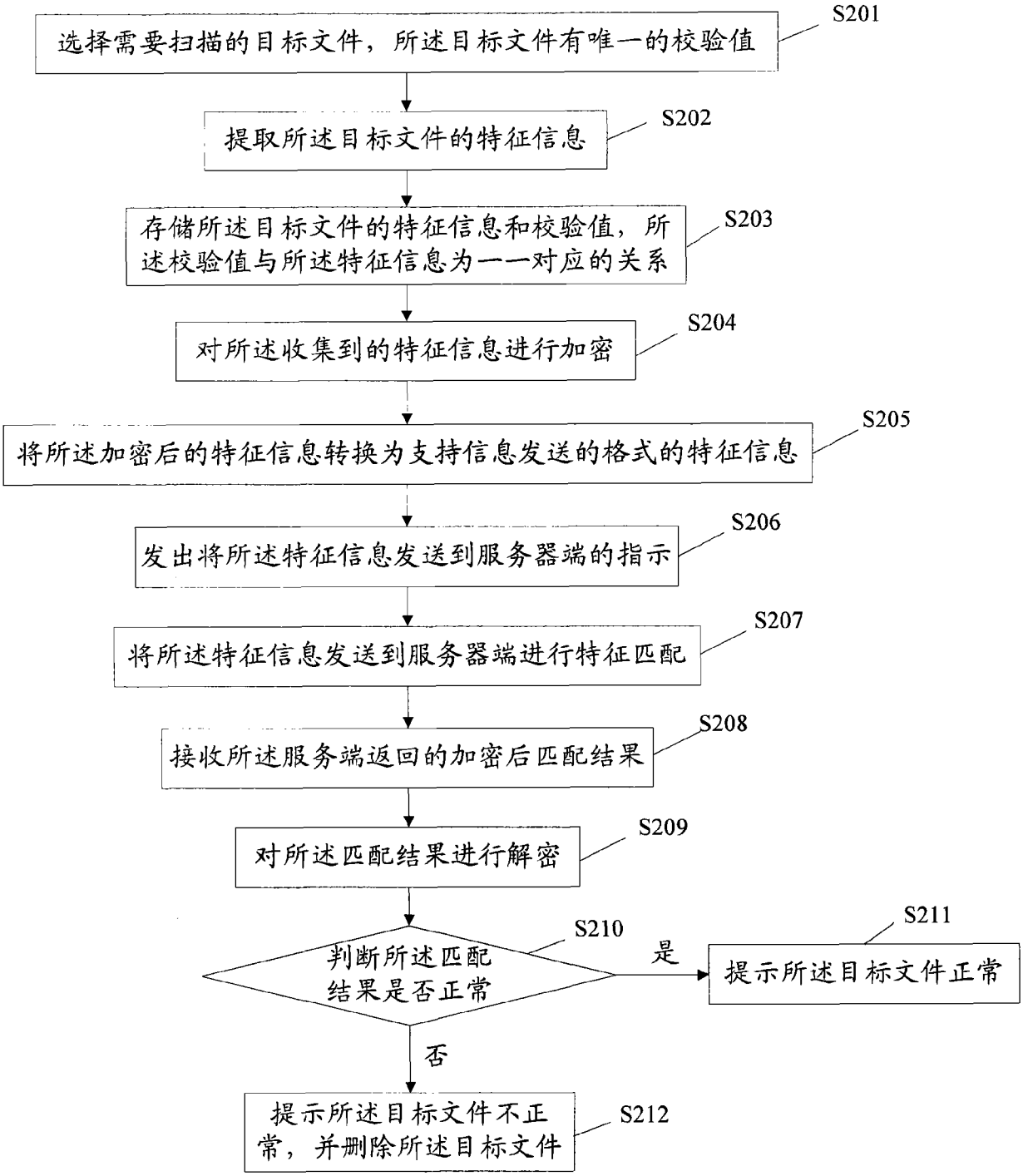

选择需要扫描的目标文件，所述目标文件有唯一的校验值
S201
提取所述目标文件的特征信息
S202
存储所述目标文件的特征信息和校验值，所述校验值与所述特征信息为一一对应的关系
S203
对所述收集到的特征信息进行加密
S204
将所述加密后的特征信息转换为支持信息发送的格式的特征信息
S205
发出将所述特征信息发送到服务器端的指示
S206
将所述特征信息发送到服务器端进行特征匹配
S207
接收所述服务端返回的加密后匹配结果
S208
对所述匹配结果进行解密
S209
判断所述匹配结果是否正常
S210
是
S211
提示所述目标文件正常
否
提示所述目标文件不正常，并删除所述目标文件
S212

图 2

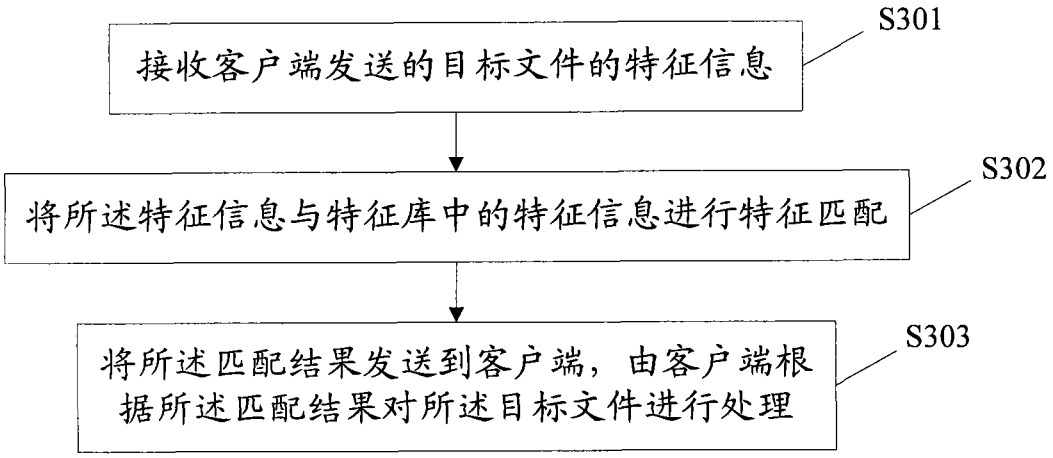

S301
接收客户端发送的目标文件的特征信息
S302
将所述特征信息与特征库中的特征信息进行特征匹配
S303
将所述匹配结果发送到客户端，由客户端根据所述匹配结果对所述目标文件进行处理

图 3

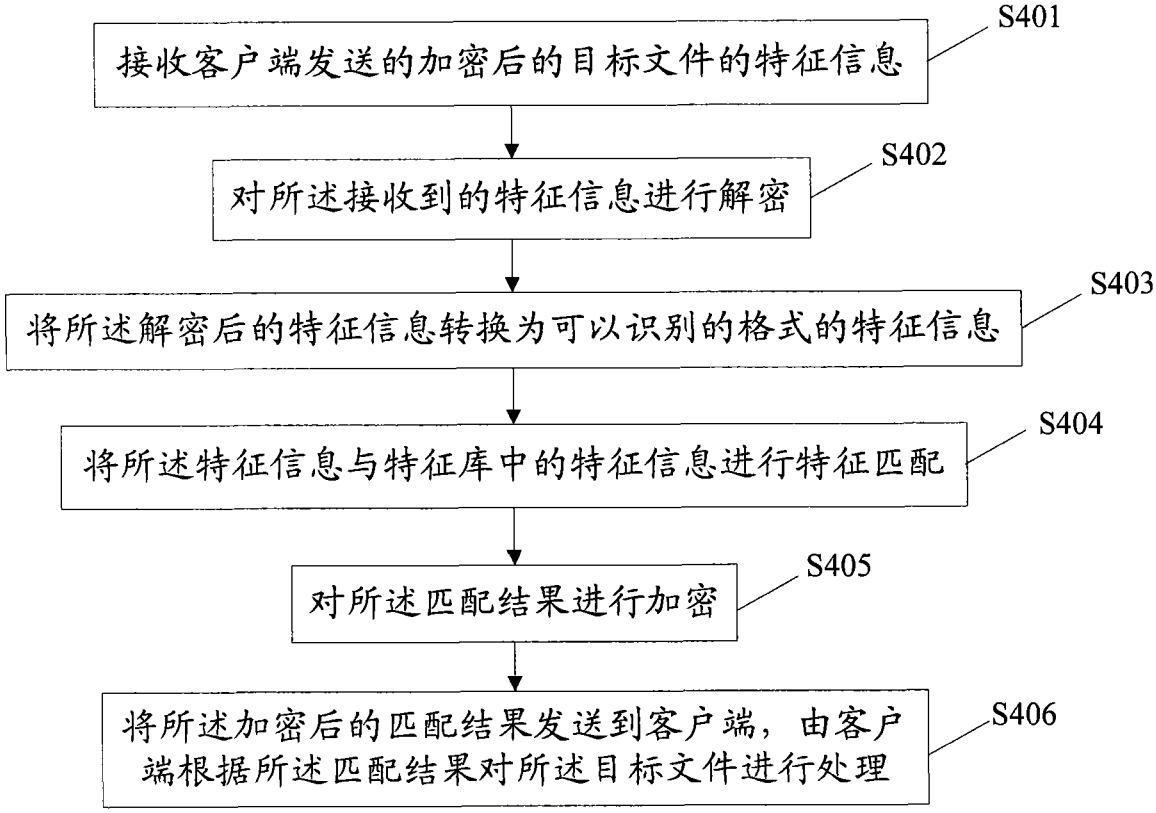

S401
接收客户端发送的加密后的目标文件的特征信息
S402
对所述接收到的特征信息进行解密
S403
将所述解密后的特征信息转换为可以识别的格式的特征信息
S404
将所述特征信息与特征库中的特征信息进行特征匹配
S405
对所述匹配结果进行加密
S406
将所述加密后的匹配结果发送到客户端，由客户端根据所述匹配结果对所述目标文件进行处理

图 4

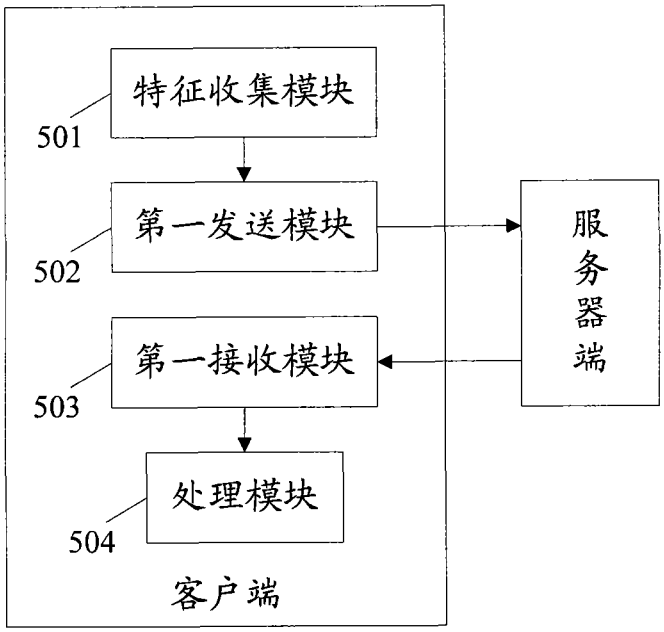

特征收集模块
501
第一发送模块
502
第一接收模块
503
处理模块
504
客户端
服务器端

图 5

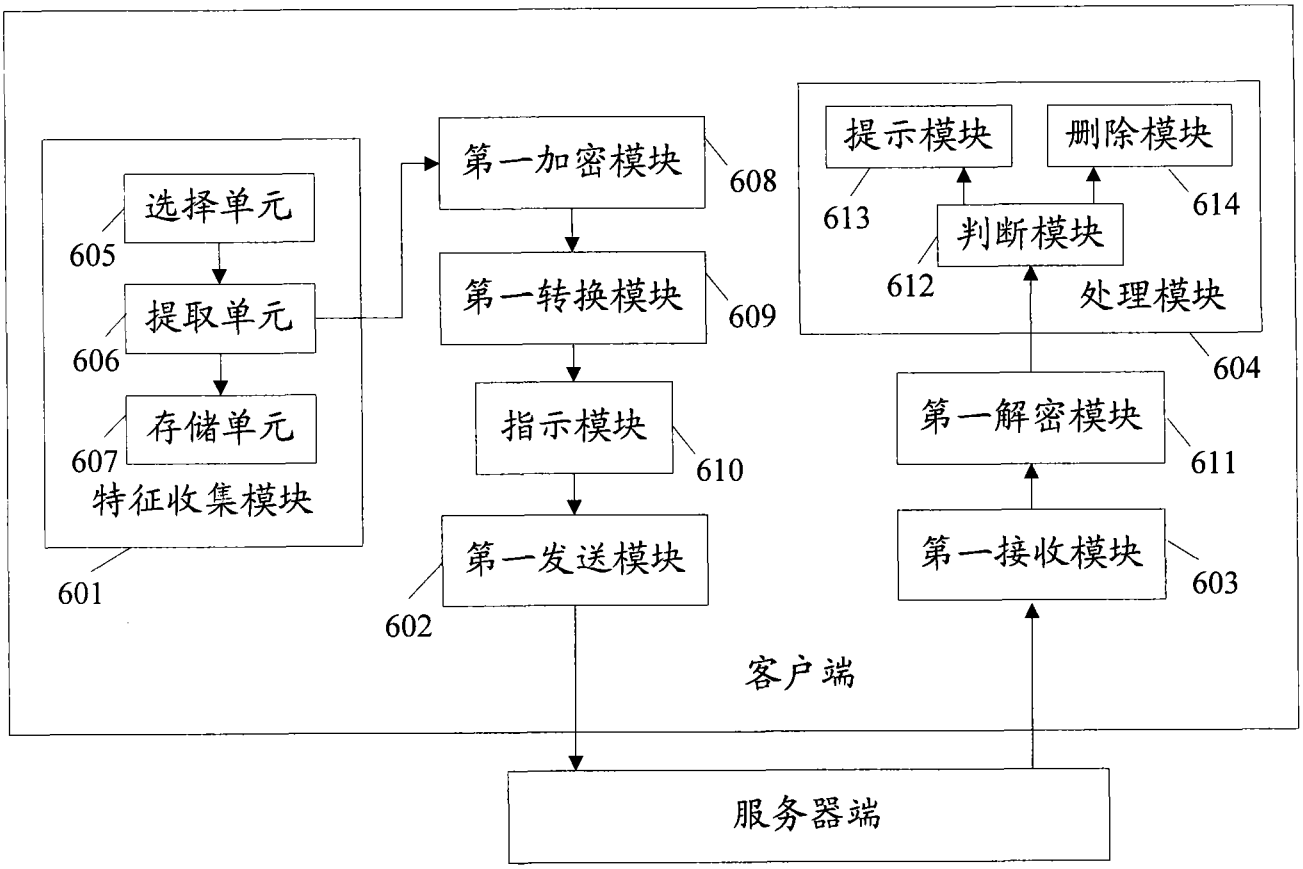

选择单元
605
提取单元
606
存储单元
607
特征收集模块
601
第一加密模块
608
第一转换模块
609
指示模块
610
第一发送模块
602
提示模块
613
删除模块
614
判断模块
612
处理模块
604
第一解密模块
611
第一接收模块
603
客户端
服务器端

图 6

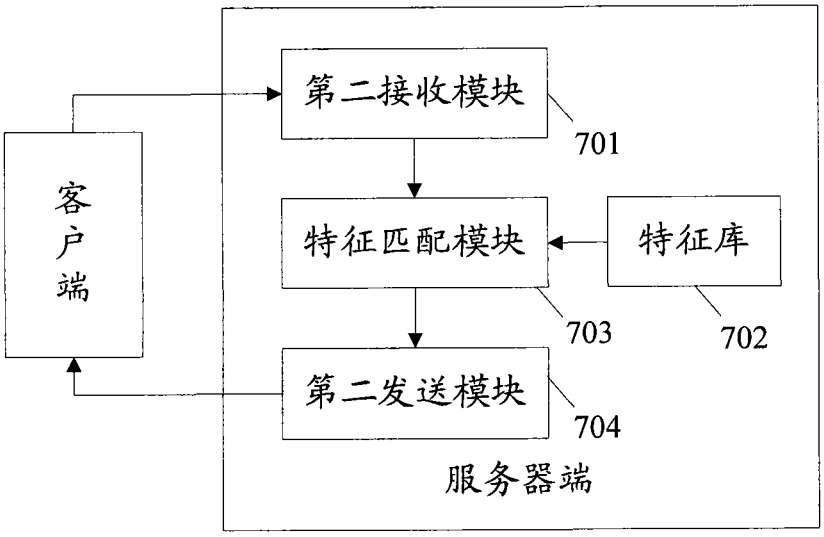

第二接收模块
701
客户端
特征匹配模块
特征库
703
702
第二发送模块
704
服务器端

图 7

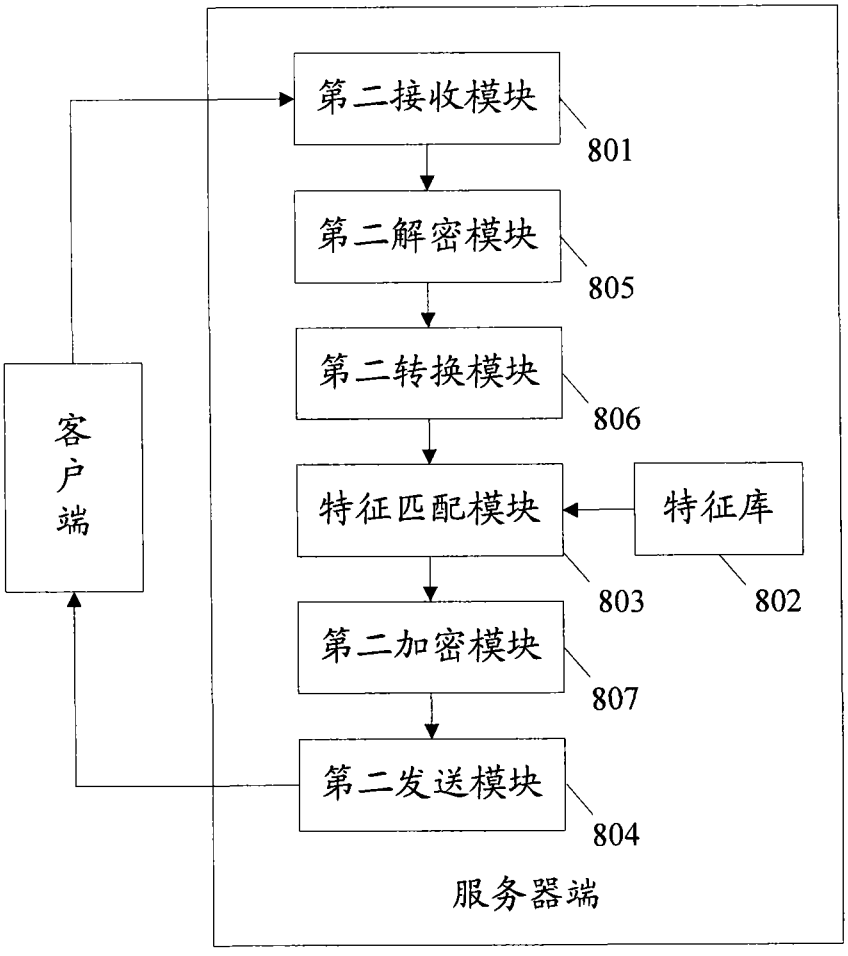

第二接收模块
801
第二解密模块
805
第二转换模块
806
客户端
特征匹配模块
特征库
803
802
第二加密模块
807
第二发送模块
804
服务器端

图 8

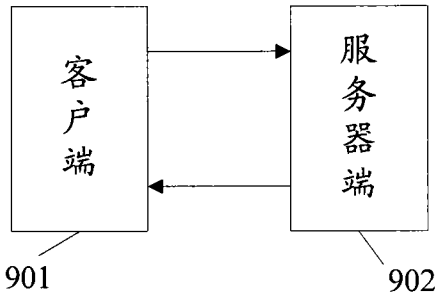


图 9