

(12) 发明专利申请

(10) 申请公布号 CN 103425927 A

(43) 申请公布日 2013. 12. 04

(21) 申请号 201210151170. 0

(22) 申请日 2012. 05. 16

(71) 申请人 腾讯科技(深圳)有限公司

地址 518044 广东省深圳市福田区振兴路赛  
格科技园 2 栋东 403 室

(72) 发明人 于涛 白子潘

(74) 专利代理机构 上海波拓知识产权代理有限  
公司 31264

代理人 杨波

(51) Int. Cl.

G06F 21/56 (2013. 01)

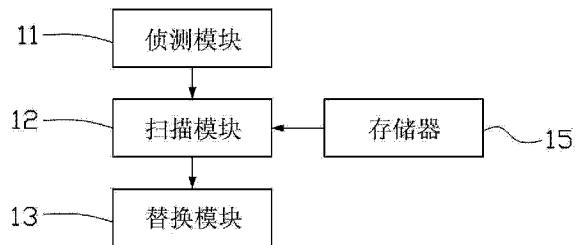
权利要求书1页 说明书4页 附图4页

(54) 发明名称

计算机文档病毒清除装置及清除方法

(57) 摘要

本发明涉及计算机文档病毒清除装置及病毒清除方法，其中计算机文档病毒清除装置包括：存储器、扫描模块以及替换模块；存储器用于预先存储已知病毒特征码；扫描模块用于根据病毒特征码扫描计算机文档中是否具有病毒代码；替换模块用于在扫描模块扫描出病毒代码时将计算机文档中的病毒代码替换为安全代码。本发明通过在扫描模块扫描出病毒代码时将计算机文档中的病毒代码替换为安全代码，因此能提高计算机文档修复成功率，保证计算机装置安全、可靠地运行。



1. 一种计算机文档病毒清除装置,其包括 :

存储器,用于预先存储已知病毒特征码;以及

扫描模块,用于根据所述病毒特征码扫描计算机文档中是否具有病毒代码;

其特征是,所述病毒清除装置还包括 :

替换模块,用于在所述扫描模块扫描出病毒代码时将所述计算机文档中的所述病毒代码替换为安全代码。

2. 根据权利要求 1 所述的病毒清除装置,其特征是 :所述病毒清除装置还包括 :

侦测模块,用于侦测所述计算机文档中有无宿主代码,当所述计算机文档中具有宿主代码时所述扫描模块才扫描所述计算机文档。

3. 根据权利要求 2 所述的病毒清除装置,其特征是 :所述宿主代码为宏代码。

4. 根据权利要求 1 所述的病毒清除装置,其特征是 :所述安全代码为空格字符。

5. 一种计算机文档病毒清除方法,其特征是 :包括步骤 :

根据病毒特征码扫描计算机文档中是否具有病毒代码;以及

在扫描出病毒代码时将所述计算机文档中的所述病毒代码替换为安全代码。

6. 根据权利要求 5 所述的病毒清除方法,其特征是 :在根据所述病毒特征码扫描所述计算机文档中是否具有病毒代码的步骤前还包括步骤 :

侦测所述计算机文档中有无宿主代码,当所述计算机文档中具有宿主代码时才扫描所述计算机文档。

7. 根据权利要求 5 所述的病毒清除方法,其特征是 :所述宿主代码为宏代码。

8. 根据权利要求 5 所述的病毒清除方法,其特征是 :所述安全代码为空格字符。

## 计算机文档病毒清除装置及清除方法

### 技术领域

[0001] 本发明涉及电脑安全技术领域,特别涉及计算机文档病毒清除装置及清除方法。

### 背景技术

[0002] 目前,用户的计算机大都存储大量的文档,例如word文档、excel表格等,这些文档通常保存着用户非常重要的信息。当用户的计算机被破坏性病毒,例如宏病毒感染时,这些文档,例如office文档通常也会被注入宏病毒等恶意脚本。若用户运行被宏病毒感染的office文档时,宏病毒等恶意脚本就会被执行,导致计算机产生不正常的动作,例如使计算机自动登录恶意网站、删除计算机上存储的文档等,从而威胁用户的计算机安全,造成用户精神与财产上巨大的损失。

[0003] 为了避免计算机文档感染病毒而遭受重大损失,目前清除此类病毒的方法大都采用将病毒代码进行直接删除。这种清除病毒的方法虽然能够消除病毒带来的危害,但是在清除此类病毒时由于改变了文档原来的结构。所以,在清除病毒后,还需要将整个文档按照原先的格式重新进行编排。这样很可能导致文档编排的不正确,从而导致文档无法打开,进而也会给用户带来损失。

### 发明内容

[0004] 因此,本发明提供计算机文档病毒清除装置及清除方法,以克服现有计算机文档病毒清除技术存在的问题。

[0005] 具体地,本发明实施例提出的一种计算机文档病毒清除装置,包括存储器、扫描模块以及替换模块。其中,存储器用于预先存储已知病毒特征码;扫描模块用于根据病毒特征码扫描计算机文档中是否具有病毒代码;替换模块用于在扫描模块扫描出病毒代码时将计算机文档中的病毒代码替换为安全代码。

[0006] 在本发明实施例中,上述的计算机文档病毒清除装置例如还包括侦测模块,用于侦测计算机文档中有无宿主代码,当计算机文档中具有宿主代码时扫描模块才扫描计算机文档。上述宿主代码例如为宏代码。上述安全代码例如为空格字符。

[0007] 另外,本发明实施例提出的一种计算机文档病毒清除方法,包括步骤:根据病毒特征码扫描计算机文档中是否具有病毒代码;以及在扫描出病毒代码时将计算机文档中的病毒代码替换为安全代码。

[0008] 在本发明实施例中,上述的计算机文档病毒清除方法例如还包括步骤:侦测计算机文档中有无宿主代码,当计算机文档中具有宿主代码时才扫描计算机文档。上述宿主代码例如为宏代码。上述安全代码例如为空格字符

由上述实施例可知,本发明通过在扫描出病毒代码时将计算机文档中的病毒代码替换为安全代码,例如空格字符的方式,以将病毒危害清除干净,能够保证计算机文档100%的修复成功率。同时也符合计算机文档的编排规则,使得用户的计算机文档不会造成任何损害。

[0009] 上述说明仅是本发明技术方案的概述,为了能够更清楚了解本发明的技术手段,而可依照说明书的内容予以实施,并且为了让本发明的上述和其他目的、特征和优点能够更明显易懂,以下特举较佳实施例,并配合附图,详细说明如下。

## 附图说明

- [0010] 图 1 是本发明实施例提出的计算机文档病毒清除装置的主要架构框图。
- [0011] 图 2 是感染了宏病毒的计算机文档中被压缩过的宏代码的示意图。
- [0012] 图 3 是图 2 的计算机文档中的宏代码被清除宏病毒后的示意图。
- [0013] 图 4 是本发明实施例提出的计算机文档病毒清除方法的步骤流程图。
- [0014] 图 5 是本发明另一实施例提出的计算机文档病毒清除方法的步骤流程图。

## 具体实施方式

[0015] 为更进一步阐述本发明为达成预定发明目的所采取的技术手段及功效,以下结合附图及较佳实施例,对依据本发明提出的计算机文档病毒清除装置及清除方法其具体实施方式、结构、特征及功效,详细说明如后。

[0016] 有关本发明的前述及其他技术内容、特点及功效,在以下配合参考图式的较佳实施例详细说明中将可清楚的呈现。通过具体实施方式的说明,当可对本发明为达成预定目的所采取的技术手段及功效得以更加深入且具体的了解,然而所附图式仅是提供参考与说明之用,并非用来对本发明加以限制。

[0017] 图 1 是本发明实施例提出的计算机文档病毒清除装置的主要架构框图。图 2 是感染了宏病毒的计算机文档中被压缩过的宏代码的示意图。图 3 是图 2 的计算机文档中的宏代码被清除宏病毒后的示意图。请共同参阅图 1 至图 3,计算机文档病毒清除装置包括:扫描模块 12、替换模块 13 以及存储器 15。其中,计算机文档病毒清除装置还可以包括侦测模块 11,以整合更多的功能。

[0018] 更具体地,存储器 15 用于预先存储已知病毒特征码,例如宏病毒的部分或者全部特征码。

[0019] 侦测模块 11 用于通过侦测计算机文档,例如如图 2 所示的计算机文档中是否具有宿主代码。上述宿主代码例如是保存在计算机文档内的可执行代码,只有当具有宿主代码时,才有可能被写入宏病毒。因此,当具有宿主代码时,即可将其视为可疑代码,即有可能带有病毒如宏病毒的代码。如果计算机文档为 office 文档,上述宿主代码为宏代码,那么若侦测模块 11 侦测到 office 文档中有宏代码,则判断为此宏代码为可疑代码,即此宏代码有可能带有宏病毒。反之,若侦测模块 11 侦测到 office 文档中无宏代码,则判断为 office 文件中无宏病毒。在其它实施方式中,也可以实际需要省去侦测模块 11。

[0020] 扫描模块 12 用于根据病毒特征码扫描计算机文档中是否具有病毒代码,例如当计算机文档中具有宿主代码时,可以通过扫描计算机文档中的宿主代码,例如宏代码,并将此宏代码与预先存储于存储器 15 中的已知病毒特征码进行比较,若此宏代码与病毒特征码中有相同的代码,则判断为此代码为病毒代码,即计算机文档感染了病毒。反之,若此宏代码与任意的病毒特征码均不相同,则判断为此代码不是病毒代码,即计算机文档未感染病毒。

[0021] 若计算机文档病毒清除装置未设置侦测模块 11 时，则扫描模块 12 用于扫描计算机文档中的代码，并将此代码与预先存储于存储器 15 中的已知病毒特征码进行比较，若此代码与病毒特征码中有相同的代码，则表示计算机文档感染了病毒。反之，若此代码与任意的病毒特征码均不相同，则表示计算机文档未感染病毒。

[0022] 替换模块 13 在扫描模块 12 扫描出病毒代码时将计算机文档，例如 office 文档中的病毒代码替换为安全代码，上述的安全代码例如是采用安全字符经 office 文档的压缩格式压缩转换后得到，这样安全代码仍符合 office 文档的压缩算法规则。上述的安全字符例如可以是任意 ASC 字符，一般来说，比较常见的，可以采用空格、空字符、星号 \* 等。对应地，其 ASC 码值分别为 32、0 与 42，十六进制码分别为 0x20、0x00 与 0x2A。此外，还可以采用各安全字符的组合。

[0023] 如图 3 所示，是图 2 的 office 文档中的宏代码被清除宏病毒代码后的示意图。图 3 显示了清除宏病毒后，office 文档的二进制数据（以十六进制方式显示），可见在原来是宏病毒代码均被替换成空格，可以理解的是，空格的 ASC 码值为 32，以十六进制方式显示为 20。上述方式未改动 office 文档的原来结构，与清楚病毒之前的差异仅在于解码后的病毒代码被空格所替换。

[0024] 在此，在解压清除病毒后的代码后，原先带有病毒的代码都被安全代码，例如空格字符所替换，这样宏病毒的威胁就被彻底消除。另外，仅将原压缩的病毒代码全部替换成空格字符，这样也符合计算机文档的编排规则，例如 office 文档的压缩算法规则，未改变计算机文档原来的结构，不会对原有的 office 文档格式造成影响，保证了计算机文档的修复成功率为 100%。

[0025] 请一并参阅图 1 至图 4，其中图 4 是本发明实施例提出的计算机文档病毒清除方法的步骤流程图。具体地，本发明实施例的计算机文档病毒清除方法可大致包括以下步骤 S202-S209。

[0026] 步骤 S202：侦测模块 11 侦测计算机文档，例如如图 2 所示的 office 文件中被压缩过的宏代码中有无宿主代码，例如宏代码而判断 office 文件中是否存在可疑代码，即有可能带有病毒的代码，例如宏病毒代码。如果计算机文档为 office 文件，宿主代码为宏代码，那么若侦测模块 11 侦测到 office 文件中有宏代码，则进行步骤 S203，若侦测模块 11 侦测到 office 文件中无宏代码，则进行步骤 S205。

[0027] 步骤 S203：侦测模块 11 判断为此宿主代码，例如宏代码为可疑代码，即此宏代码有可能带有病毒，例如宏病毒，进行步骤 S206。

[0028] 步骤 S205：侦测模块 11 判断为计算机文档，例如 office 文件中无病毒，结束。

[0029] 步骤 S206：扫描模块 12 扫描计算机文档中的宿主代码，例如宏代码，并将此宏代码与预先存储于存储器 15 中的已知病毒特征码进行比较，若此宏代码与病毒特征码中有相同的代码，则进行步骤 S207，若此宏代码与任意的病毒特征码均不相同，则进行步骤 S208。

[0030] 步骤 S207：扫描模块 12 判断为此代码为病毒代码，即计算机文档感染了病毒，进行步骤 S209。

[0031] 步骤 S208：扫描模块 12 判断为判断为此代码不是病毒代码，即计算机文档未感染病毒，结束。

[0032] 步骤 S209 :替换模块 13 将计算机文档中的病毒代码替换为安全代码,例如空格字符。

[0033] 在其它实施方式中,当本发明实施例的计算机文档病毒清除装置未设置侦测模块 11 的情形下,相应地可省去步骤 S202。

[0034] 请一并参阅图 1 至图 5,其中图 5 是本发明另一实施例提出的计算机文档病毒清除方法的步骤流程图。图 5 与图 4 的区别在于图 5 是计算机文档病毒清除装置未设置侦测模块 11 的情形。具体地,本发明实施例的计算机文档病毒清除方法可大致包括以下步骤 S306-S309。

[0035] 步骤 S306 :扫描模块 12 扫描计算机文档中的代码,并将此代码与预先存储于存储器 15 中的已知病毒特征码进行比较以判断此代码是否为病毒代码,若此代码与病毒特征码中有相同的代码,则进行步骤 S307,若此代码与任意的病毒特征码均不相同,则进行步骤 S308。

[0036] 步骤 S307 :扫描模块 12 判断为此代码为病毒代码,即计算机文档感染了病毒,进行步骤 S309。

[0037] 步骤 S308 :扫描模块 12 判断为此代码不是病毒代码,即计算机文档未感染病毒,结束。

[0038] 步骤 S309 :替换模块 13 将计算机文档中的病毒代码替换为安全代码,例如空格字符。

[0039] 综上所述,本发明通过扫描模块 12 将计算机文档中的代码与预先存储于存储器 15 中的已知病毒特征码进行比较,再通过替换模块 13 将计算机文档中的病毒代码替换为安全代码,例如空格字符的方式,以将病毒危害清除干净,能够保证计算机文档 100% 的修复成功率。同时也符合计算机文档的编排规则,例如计算机文档的压缩算法规则,使得用户的计算机文档不会造成任何损害,从而实现了计算机文档病毒的自动识别、自动清除和计算机文档的自动修复,有效地阻止了计算机文档病毒的进一步传染和破坏作用,提高了计算机文档的修复成功率,能够保证计算机装置安全、可靠地运行。

[0040] 以上所述,仅是本发明的较佳实施例而已,并非对本发明作任何形式上的限制,虽然本发明已以较佳实施例揭露如上,然而并非用以限定本发明,任何熟悉本专业的技术人员,在不脱离本发明技术方案范围内,当可利用上述揭示的技术内容作出些许更动或修饰为等同变化的等效实施例,但凡是未脱离本发明技术方案内容,依据本发明的技术实质对以上实施例所作的任何简单修改、等同变化与修饰,均仍属于本发明技术方案的范围内。

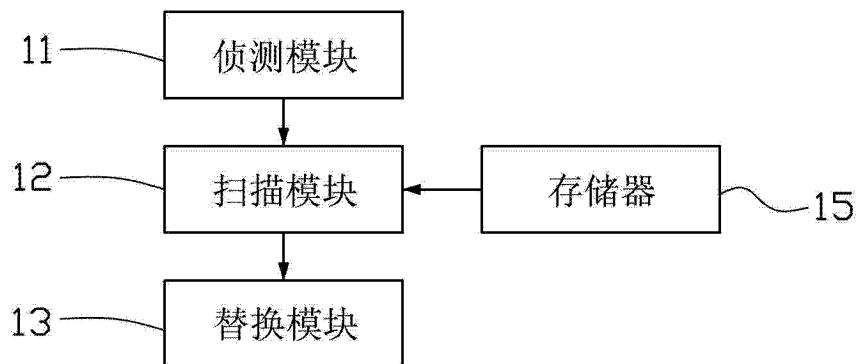


图 1

```

00007ab0h: FF FF 00 00 01 42 B5 00 41 74 74 72 69 62 75 74 ; ...B?Attribut
00007ac0h: 00 65 20 56 42 5F 4E 61 6D 00 65 20 3D 20 22 4D ; .e VB_Nam.e = "M
00007ad0h: 6F 64 00 75 6C 65 31 22 0D 0A 50 10 72 69 76 61 ; cd.ule1" ..P.riva
00007ae0h: 00 70 53 75 62 10 20 63 72 65 00 28 63 61 62 00 ; .pSub. cre.(cab.
00007af0h: 66 69 6C 65 28 29 0D 0A 00 44 69 6D 20 63 68 20 ; file()...Dim ch
00007b00h: 41 00 73 20 42 79 74 65 0D 0A 00 4F 6E 20 45 72 ; A.s Byte...On Ex
00007b10h: 72 6F 72 20 20 52 65 73 75 00 92 4E 65 00 78 74 ; ror Resu.抓e.xr
00007b20h: 0D 0A 53 65 74 20 28 66 73 6F 00 AE 43 02 80 4F ; ..
00007b30h: 62 00 6A 65 63 74 28 22 73 63 00 72 69 70 74 69 ; b.ject("sc.ripti
00007b40h: 6E 67 2E 01 01 4F 73 79 73 74 65 6D 6F AD 02 1B ; ng...Osystemo?.
00007b50h: 22 00 5B 01 35 77 0E 33 77 03 34 40 2E 73 68 65 ; ".[.5w.3w.4@.she
00007b60h: 6C 6C 01 26 6D 80 79 66 6F 6C 64 65 72 00 29 00 ; ll.&mEyfolder.).
00007b70h: 77 2E 53 70 65 63 69 61 04 6C 46 02 11 73 28 22 ; w.Specia.1F..s("
00007b80h: 54 65 08 6D 70 6C 00 B2 73 22 29 20 00 26 20 22 ; Te.mpl.显") .&
00007b90h: SC 53 6F 66 74 20 77 61 72 65 SC 00 D8 49 66 28 ; \Soft ware\.\移f(
00007ba0h: 20 4E 6F 02 98 2E 83 20 65 78 20 69 73 74 73 28 ; No.??ex ists!
00007bb0h: 05 28 29 20 40 54 68 65 6E 0D 0A 80 5C 2E 07 03 ; .() @Then..@\
00007bc0h: 7C 04 34 05 10 0D 0A 45 6E 64 40 20 49 66 0D 0A ; |.4....End@ If..
00007bd0h: 46 80 78 69 01 00 40 31 20 54 6F 20 57 6F 00 72 ; FExi..@1 To Wo.r
00007be0h: 6B 62 6F 6F 6B 73 2E 70 43 6F 75 6E 00 7F 00 34 ; xbooks.pCoun. .4
00007bf0h: 86 09 28 08 69 29 2E 85 B1 6E 6F 72 6D 80 61 6C ; ?(.i).搬norm@al
00007c00h: 2E 78 6C 6D 22 04 35 61 0A 13 43 6C 6F 73 00 A9 ; .xlm".5a..Clos.?
00007c10h: 01 3F 64 20 65 6C 65 74 65 01 92 20 41 00 70 70 ; .?d elete.?A.pp
00007c20h: 6C 69 63 61 74 69 00 6F 6E 2E 53 74 61 72 74 C0 ; licati.on.Start?

```

图 2

301

) .B?

00007ab0h: FF FF 00 00 01 42 B5 00 20 20 20 20 20 20 20 20 ;  
00007ac0h: 00 20 20 20 20 20 20 20 20 00 20 20 20 20 20 20 ;  
00007ad0h: 20 20 00 20 20 20 20 20 20 20 00 20 20 20 20 20 ;  
00007ae0h: 20 20 20 20 00 20 20 20 20 20 20 00 20 20 20 20 ;  
00007af0h: 20 20 20 20 20 00 20 20 20 20 20 20 20 20 20 00 ;  
00007b00h: 20 20 20 20 20 20 20 20 20 00 20 20 20 20 20 20 ;  
00007b10h: 20 00 20 20 20 20 20 20 20 20 00 20 20 20 20 20 ;  
00007b20h: 20 20 20 00 20 20 20 20 20 20 20 00 20 20 20 20 ;  
00007b30h: 20 20 20 20 00 20 20 20 20 20 20 20 20 20 00 20 ;  
00007b40h: 20 20 20 20 20 00 20 20 20 20 20 20 20 20 20 20 ;  
00007b50h: 00 20 20 20 20 20 20 20 00 20 20 20 20 20 20 20 ;  
00007b60h: 20 20 00 20 20 20 20 20 20 20 00 20 20 20 20 20 ;  
00007b70h: 20 20 20 00 20 20 20 20 20 20 20 00 20 20 20 20 ;  
00007b80h: 20 20 20 20 20 00 20 20 20 20 20 20 20 20 20 00 ;  
00007b90h: 20 20 20 20 20 20 00 20 20 20 20 20 20 20 20 20 ;  
00007ba0h: 20 00 20 20 20 20 20 20 20 20 00 20 20 20 20 20 ;  
00007bb0h: 20 20 20 00 20 20 20 20 20 20 20 00 20 20 20 20 ;  
00007bc0h: 20 20 20 20 00 20 20 20 20 20 20 20 20 20 00 20 ;  
00007bd0h: 20 20 20 20 20 00 20 20 20 20 20 20 20 20 20 20 ;  
00007be0h: 00 20 20 20 20 20 20 20 00 20 20 20 20 20 20 20 ;  
00007bf0h: 20 20 00 20 20 20 20 20 20 20 00 20 20 20 20 20 ;  
00007c00h: 20 20 20 00 20 20 20 20 20 20 20 20 00 20 20 20 ;  
00007c10h: 20 20 20 20 20 00 20 20 20 20 20 20 20 20 20 00 ;  
00007c20h: 20 20 20 20 20 20 00 20 20 20 20 20 20 20 20 20 ;

图 3

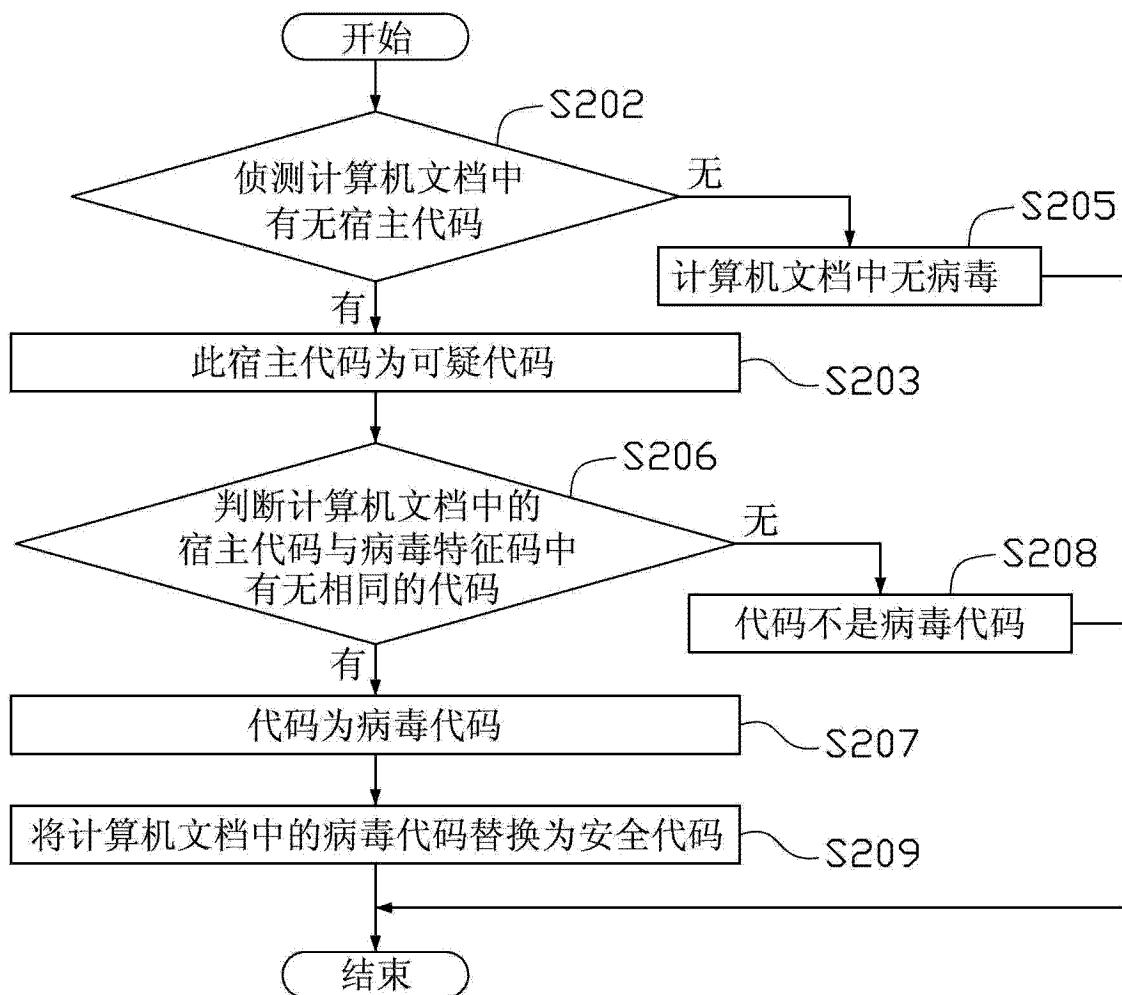


图 4

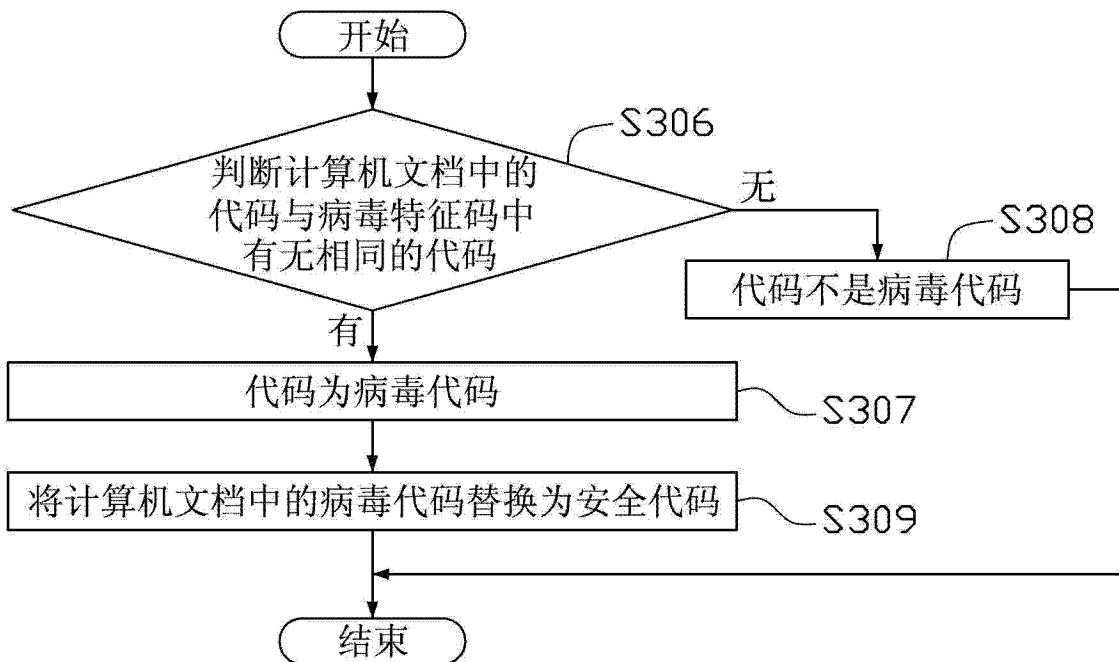


图 5