[19] 中华人民共和国国家知识产权局

[51] Int. Cl[7]
G06F 15/16
G06F 9/06 G06F 13/00
G06F 17/00

[12] 发明专利申请公开说明书

[21] 申请号 03159313.5

[43] 公开日 2004 年 4 月 21 日

[11] 公开号 CN 1490736A

[22] 申请日 2003.9.3 [21] 申请号 03159313.5

[30] 优先权

[32] 2002. 9. 4 [33] US [31] 10/235，587

[71] 申请人 微软公司

地址 美国华盛顿州

[72] 发明人 D·阿登特 C·韦斯特

P·杜布里什 C·P·斯特罗姆

B·D·克赖茨

[74] 专利代理机构 上海专利商标事务所

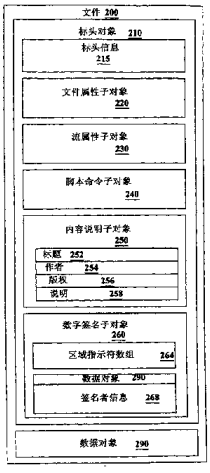
代理人 李家麟

权利要求书 8 页 说明书 10 页 附图 5 页

[54] 发明名称 数据流标头对象保护

[57] 摘要

数据文件的标头对象由子对象组成，子对象指定了数据流的属性并且包含适当验证并解译数据对象内的信息所需的信息。 为了允许保护任意子对象组而不要求子对象遵从任意特定的排列，引入新的子对象，它包括标识子对象内的区域以及那些区域的验证信息。 这个标头对象内新的子对象允许修改非保护区域并重新组织标头内的子对象而不使验证信息失效。



ISSN1008-4274

1．一种与包括至少一个子对象的数字对象结合使用的方法，所述方法为至少一个区域提供数字签名，其中所述至少一个区域的每一个都由所述至少一个子对象之一的全部或部分组成，且其中所述子对象可以在对象内被重排而不使数字签名失效，该方法的特征在于包括：

为所述至少一个区域的每一个创建一个数组，包含标识该区域的区域指示符；

根据包含每个区域的数据和所述数组的数据产生数字签名；以及

把包含所述数组和所述数字签名的签名子对象加入数字对象。

2．如权利要求 1 所述的方法，其特征在于，所述至少一个区域的每一个包括来自所述至少一个子对象中的一个子对象。

3．如权利要求 1 所述的方法，其特征在于，所述区域指示符的每一个都包括按照校验和算法计算的校验和。

4．如权利要求 3 所述的方法，其特征在于，所述校验和为该区域而计算。

5．如权利要求 3 所述的方法，其特征在于，所述校验和为包含该区域的子对象而计算。

6．如权利要求 3 所述的方法，其特征在于，所述签名子对象包含标识所使用校验和算法的校验和算法标识符。

7．如权利要求 3 所述的方法，其特征在于，所述区域标识符的每一个都包括校验和长度。

8．如权利要求 1 所述的方法，其特征在于，所述签名子对象包括一个签名算法标识符，它标识为所述数字签名的产生而使用的签名算法。

9．如权利要求 1 所述的方法，其特征在于，所述签名子对象包括签名者标识

符，标识用于验证所述数字签名的签名者。

10. 如权利要求 9 所述的方法，其特征在于，所述签名者标识符包括数字证书，用于安全地标识并验证所述签名者的公钥。

11. 如权利要求 1 所述的方法，其特征在于，所述区域指示符的每一个都包括一个区域偏移，标识子对象中相应区域的起始位置。

12. 如权利要求 1 所述的方法，其特征在于，所述区域指示符的每一个都包括一个区域大小，标识子对象中相应区域的大小。

13. 如权利要求 1 所述的方法，其特征在于，所述对象是 ASF 文件的标头对象。

14. 如权利要求 13 所述的方法，其特征在于，所述新对象还包括 GUID。

15. 一种与包括至少一个子对象的数字对象结合使用的方法，所述方法为至少一个区域确认数字签名，其中所述至少一个区域的每一个都由所述至少一个子对象之一的全部或部分所组成，其中数组包括所述至少一个区域的每一个的区域指示符，该方法的特征在于包括：

标识相应于每一个所述区域指示符的区域；

创建一个数据对象，包含所述数组，以及用于每一个所述区域指示符的与所述区域指示符对应的所述区域；以及

确认在所述数据对象上使用的所述数字签名。

16. 如权利要求 15 所述的方法，其特征在于，所述对象是 ASF 文件的标头文件。

17. 一种与包括至少一个子对象的数字对象结合使用的方法，所述方法为至少一个区域确认数字签名，其中所述至少一个区域的每一个都由所述至少一个子对象之一的全部或部分所组成，其中数组包括所述至少一个区域的每一个的区域指示

符，该方法的特征在于包括：

确定所述数字对象中存在的数字签名数目；

确认每一个所述数字签名。

18．如权利要求 17 所述的方法，其特征在于还包括：

如果所述数字对象内存在的数字签名数目为零则返回错误值。

19．一种与包括至少一个子对象的数字对象结合使用的系统，所述系统为至少一个区域提供数字签名，其中所述至少一个区域的每一个都由所述至少一个子对象之一的全部或部分所组成，且其中所述子对象可能在对象内被重排而不会使数字签名失效，该系统的特征在于包括：

数组创建装置，用于为所述至少一个区域的每一个创建一个数组，包含标识该区域的区域指示符；

签字装置，用于根据包含每个区域的数据和所述数组产生数字签名；以及

签名子对象添加装置，用于把包含所述数组和所述数字签名的签名子对象添加至数字对象。

20．如权利要求 19 所述的系统，其特征在于，所述至少一个区域的每一个包括来自所述至少一个子对象的一个子对象。

21．如权利要求 19 所述的系统，其特征在于，所述至少一个区域的每一个包括按照校验和算法计算的校验和。

22．如权利要求 21 所述的系统，其特征在于，所述校验和为该区域而计算。

23．如权利要求 21 所述的系统，其特征在于，所述校验和为包含该区域的子对象而计算。

24．如权利要求 21 所述的系统，其特征在于，所述签名子对象包含标识所使用校验和算法的校验和算法标识符。

25. 如权利要求 21 所述的系统，其特征在于，所述区域标识符的每一个都包括校验和长度。

26. 如权利要求 19 所述的系统，其特征在于，所述签名子对象包括一个签名算法标识符，它标识为所述数字签名的产生而使用的签名算法。

27. 如权利要求 19 所述的系统，其特征在于，所述签名子对象包括签名者标识符，标识用于验证所述数字签名的签名者。

28. 如权利要求 27 所述的系统，其特征在于，所述签名者标识符包括数字证书，用于安全地标识并验证所述签名者的公钥。

29. 如权利要求 19 所述的系统，其特征在于，所述区域指示符的每一个都包括一个区域偏移，标识子对象中相应区域的起始位置。

30. 如权利要求 19 所述的系统，其特征在于，所述区域指示符的每一个都包括一个区域大小，标识子对象中相应区域的大小。

31. 如权利要求 19 所述的系统，其特征在于，所述对象是 ASF 文件的标头对象。

32. 如权利要求 31 所述的系统，其特征在于，所述新对象还包括 GUID。

33. 一种与包括至少一个子对象的数字对象结合使用的系统，所述系统为至少一个区域确认数字签名，其中所述至少一个区域的每一个都由所述至少一个子对象之一的全部或部分所组成，其中数组包括所述至少一个区域的每一个的区域指示符，该系统的特征在于包括：

区域标识装置，标识相应于每一个所述区域指示符的区域；

数据对象创建装置，用于创建一个数据对象，包含所述数组，以及用于每一个所述区域指示符的与所述区域指示符对应所述区域；以及

确认装置，确认所述数据对象上使用的所述数字签名。

34．如权利要求33所述的系统，其特征在于，所述对象是ASF文件的标头文件。

35．一种与包括至少一个子对象的数字对象结合使用的系统，所述系统为至少一个区域确认数字签名，其中所述至少一个区域的每一个都由所述至少一个子对象之一的全部或部分所组成，其中数组包括所述至少一个区域的每一个的区域指示符，该系统的特征在于包括：

计数装置，用于确定所述数字对象中存在的数字签名数目；

确认装置，用于确认每一个所述数字签名。

36．如权利要求35所述的方法，其特征在于还包括：

错误返回装置，如果所述数字对象内存在的数字签名数目为零则返回错误值。

37．一种与包括至少一个子对象的数字对象结合使用的计算机可读媒质，所述计算机可读媒质为至少一个区域提供数字签名，其中所述至少一个区域的每一个都由所述至少一个子对象之一的全部或部分所组成，且其中所述子对象可能在对象内被重排而不会使数字签名失效，具有指令来执行操作的计算机可读媒质的特征在于包括：

为所述至少一个区域的每一个创建一个数组，该数组包含标识该区域的区域指示符；

根据包含每个区域的数据和所述数组产生数字签名；以及

把包含所述数组和所述数字签名的签名子对象添加至数字对象。

38．如权利要求37所述的计算机可读媒质，其特征在于，所述至少一个区域的每一个包括来自所述至少一个子对象的一个子对象。

39．如权利要求37所述的计算机可读媒质，其特征在于，所述区域指示符包括按照校验和算法计算的校验和。

40．如权利要求39所述的计算机可读媒质，其特征在于，所述校验和为该区

域而计算。

41．如权利要求39所述的计算机可读媒质，其特征在于，所述校验和为包含该区域的子对象而计算。

42．如权利要求39所述的计算机可读媒质，其特征在于，所述签名子对象包含标识所使用的校验和算法的校验和算法标识符。

43．如权利要求39所述的计算机可读媒质，其特征在于，所述区域标识符的每一个都包括校验和长度。

44．如权利要求37所述的计算机可读媒质，其特征在于，所述签名子对象包括一个签名算法标识符，它标识为所述数字签名的产生而使用的签名算法。

45．如权利要求37所述的计算机可读媒质，其特征在于，所述签名子对象包括签名者标识符，标识用于验证所述数字签名的签名者。

46．如权利要求45所述的计算机可读媒质，其特征在于，所述签名者标识符包括数字证书，用于安全地标识并验证所述签名者的公钥。

47．如权利要求37所述的计算机可读媒质，其特征在于，所述区域指示符的每一个都包括一个区域偏移，标识子对象中相应区域的起始位置。

48．如权利要求37所述的计算机可读媒质，其特征在于，所述区域指示符的每一个都包括一个区域大小，标识子对象中相应区域的大小。

49．如权利要求37所述的计算机可读媒质，其特征在于，所述对象是ASF文件的标头对象。

50．如权利要求49所述的计算机可读媒质，其特征在于，所述新对象还包括GUID。

51．一种与包括至少一个子对象的数字对象结合使用的计算机可读媒质，所述计算机可读媒质为至少一个区域确认数字签名，其中所述至少一个区域的每一个都由所述至少一个子对象之一的全部或部分所组成，其中数组包括所述至少一个区域的每一个的区域指示符，该计算机可读媒质的特征在于包括：

标识相应于每一个所述区域指示符的区域；

创建一个数据对象，包含所述数组，以及用于每一个所述区域指示符创的与所述区域指示符对应的所述区域；以及

确认所述数据对象上使用的所述数字签名。

52．如权利要求51所述的计算机可读媒质，其特征在于，所述对象是ASF文件的标头文件。

53．一种与包括至少一个子对象的数字对象结合使用的计算机可读媒质，所述计算机可读媒质为至少一个区域确认数字签名，其中所述至少一个区域的每一个都由所述至少一个子对象之一的全部或部分所组成，其中数组包括所述至少一个区域的每一个的区域指示符，该计算机可读媒质的特征在于包括：

确定所述数字对象中存在的数字签名数目；

确认每一个所述数字签名。

54．如权利要求53所述的计算机可读媒质，其特征在于还包括：

如果所述数字对象内存在的数字签名数目为零则返回错误值。

55．一种用于存储数据的存储器，由包含存储在所述存储器内的数据结构的应用程序来访问，所述数据结构适用于存储由至少一个子对象组成的对象的确认信息，而允许所述子对象顺序的变化，该存储器的特征在于包括：

包含至少一个区域指示符的区域指示符数组，每个这种区域指示符都指定一个区域，它包含所述子对象之一的全部或部分；以及

包含所述区域和所述区域指示符数组的每一个的数据的数字签名。

56．如权利要求55所述的存储器，其特征在于，所述数据结构还包括下列的

一个或多个：

所述数据结构的全局唯一的标识符（GUID）；

数据结构的大小；

所述区域指示符数组内的区域数目；

校验和算法标识符；

签名算法标识符，标识用于产生所述数字签名的算法；

所述数字签名的签名长度；以及

用于验证所述数字签名的签名者信息。

数据流标头对象保护

(1)技术领域

本发明一般涉及数据验证，尤其涉及数据文件的标头对象。

(2)背景技术

通常，某些数据文件和数据流格式包括标头对象。标头对象包括用于标识并使用包括在数据文件或数据流内的内容数据的“元内容”信息。

例如，一个数据流格式是高级流格式（ASF），它是为存储同等多媒体数据而设计的可扩展文件格式。目前该格式的规范可从www.microsoft.com得到。ASF 支持大范围网络和协议上的数据传递，而允许本地回放。

每个 ASF 文件都由一个或多个媒体流组成。标头对象执行整个文件的属性，以及流专有的属性。在 ASF 中，每个文件必需具有一个标头对象。标头对象在 ASF 文件的开始处（标头对象 GUID（全局唯一的标识符））提供了一个公知字节序列并且包含适当解译多媒体数据所需的全部信息。标头对象可能被视作包含标头对象信息以及标头子对象组合的容器。标头对象信息包括标头对象（“ASF_Header_Object”）的 GUID、标头对象的大小、及标头对象内所包含的标头子对象的数目。每个标头对象都从 GUID 开始。

标头子对象包括：

- 文件属性子对象，它定义了文件中多媒体数据的全局特性；
- 流属性子对象，它定义了媒体流的特定属性和特性；
- 标头扩展子对象，它允许对 ASF 文件添加附加功能而保持向后兼容性，并且是包含扩展的标头子对象的容器；
- 编解码器列表子对象，它提供与对 ASF 文件中找到的内容进行编码所用的编解码器和格式有关的用户友好信息；
- 脚本命令子对象，它提供了 Unicode 字符串的类型/参数对的一个列表，它们与 ASF 文件的时间线同步；
- 标记子对象，它包含小的、特殊的索引，用于提供文件内命名的跳跃点以允许内容作者把内容分成逻辑部分，譬如整个 CD 中的歌曲边界或者长演讲的话题

变换，并且用于为文件的每个部分分配可由用户使用的人类可读名称；

• 比特率互斥子对象，它标识了彼此具有互斥关系的视频流（换言之，这种关系中只有一个流可以流出，并忽略其它）；

• 纠错子对象，它定义了纠错方法并提供用于恢复的纠错引擎所需的信息；

• 内容描述子对象，它允许作者记录描述文件及其内容的公知数据，包括题目、作者、版权、说明和价目信息；

• 扩展内容描述子对象，它允许作者记录描述文件及其内容的数据，该数据在诸如题目、作者、版权、说明或价目信息等标准书目信息之外；

• 内容加密子对象，它标识该内容是否得到数字权利管理（DRM）系统的保护。该子对象包括 DRM 许可证－获得 URL、DRM 密钥 ID、及其它 DRM 有关的元数据；

• 流比特率属性子对象，它定义了多媒体数据中每个媒体流的平均比特率；以及

• 填充子对象，它是用于填充标头对象大小的虚拟子对象。

首先创建数据流文件的实体以及对它起作用的任何随后实体都可能添加或改变标头文件的元素。例如，内容创建实体可能创建一个数据流文件，并且包括与内容有关的内容说明对象中的信息。第二实体可能创建数据内的标记，并且希望用跟踪信息添加标记对象。而第三实体分发数据流文件，它可能添加包含脚本的行为或数据的脚本命令对象。例如，脚本命令对象可能包含把 Web 浏览器窗口打开为指定 URL（统一资源定位符）的信息。

由于许多实体可能对 ASF 文件起作用，因此不可能确定哪个实体已创建了标头对象的哪个部分。此外，不能识别由攻击者作出的信息变化。

(3)发明内容

本发明针对验证标头对象内子对象的系统、方法和数据结构。本发明允许用一个实体验证标头对象内的一个或多个子对象，而仍然允许排列要改变的子对象。新的子对象随后还能由另一实体创建并验证。可以组合由一个可信实体对两个或多个子对象的验证，使得攻击者不能移动或改变数据，而使一个子对象像已由可信实体签字那样可被验证，而另一子对象不可被验证。

下面的说明中提出了本发明的其它特征和优点。

(4)附图说明

图 1 是计算机系统总览图。

图 2 是说明按照本发明的文件的框图。

图 3 说明了按照本发明创建数字签名子对象的过程。

图 4 说明了按照本发明验证数字签名子对象的过程。

图 5 说明了按照本发明的数字签名子对象。

(5)具体实施方式

综述

为了允许标头对象中的子对象的签名信息及子对象区域，可以创建一个或多个数字签名子对象并将它们放置在数据文件的标头对象中。如果数字签名子对象存在并有效，则可以检测到关于已签名子对象的任意编辑或篡改。子对象的排列不需要被保存。

数字签名子对象包含一个区域指示符数组。每个区域指示符都标识了子对象内的一个特定区域。区域指示符可能还标识一个完整的子对象。

数字签名子对象还包含一个签名。该签名是区域指示符数组中所列的区域的数字签名。该签名可以用于验证区域指示符中所列的区域尚未被篡改。

示例性计算环境

图 1 说明了适当的计算系统环境 100 的一例，其中可能实现本发明。计算系统环境 100 仅是适当的计算环境的一例并且并非意图限制本发明的使用范围或功能。计算环境 100 不应被解释为具有与示例性操作环境 100 中所述的组件的任一或组合有关的从属性或要求。

本领域的技术人员可以理解，计算机或其它客户机或服务器设备可以作为部分计算机网络而采用，或者用于分布式计算环境中。在这点上，本发明属于具有任意数量存储器或存储单元的任意计算机系统，以及发生在任意数量存储单元或容量上的任意数量的应用程序和过程，它们可以与本发明一起使用。本发明可以应用于在网络环境或分布式计算环境中采用服务器计算机和客户机计算机的环境。本发明还可以用于独立计算设备，具有编程语言功能、以及与远程或本地服务一起产生、接收和发射信息的解译和执行能力。

本发明可以用多种其它通用或专用计算系统环境或配置来操作。可能适合与本发明一起使用的公知计算系统、环境和/或配置的示例包括、但不限于：个人计

算机、服务器计算机、手提或便携式设备、多处理器系统、基于微处理器的系统、机顶盒、可编程用户电子设备、网络 PC、小型计算机、大型计算机、包括任一上述系统的分布式计算环境、及其它。

本发明可以用计算机可执行指令的一般上下文来描述，譬如由计算机执行的程序模块。一般而言，程序模块包括例程、程序、对象、组件、数据结构等，它们执行特定任务或实现特定的抽象数据类型。本发明还可以实际用于分布式计算环境中，其中由通过通信网络或其它数据传输媒质连接的远程处理设备来执行任务。在分布式计算环境中，程序模块及其它数据可能位于本地和远程存储媒质中，包括存储器存储设备。分布式计算通过计算设备和系统间的直接交换便于共享计算机资源和服务。这些资源和服务包括信息、高速缓存、及文件磁盘存储的交换。分布式计算利用网络连接性，允许用户机发挥它们的集体功效来有利于整个公司。在这点上，多种设备可能具有应用程序、对象或资源，它们可能利用本发明的技术。

参考图 1，用于实现本发明的示例性系统包括形式为计算机 110 的通用计算设备。计算机 110 的组件可能包括、但不限于：处理单元 120、系统存储器 130、及把包括系统存储器在内的各种系统组件耦合至处理单元 120 的系统总线 121。系统总线 121 可能是多种类型总线结构的任一种，包括存储器总线或存储器控制器、外围设备总线、及使用任一多种总线结构的本地总线。通过示例但非限制，这种结构包括工业标准结构（ISA）总线、微通道结构（MCA）总线、增强型 ISA（EISA）总线、视频电子标准联盟（VESA）本地总线、及外围组件互连（PCI）总线（也称为 Mezzanine 总线）。

计算机 110 一般包括各种计算机可读媒质。计算机可读媒质可以是能由计算机 110 访问的任何可用媒质并包括易失性和非易失性的媒质、可移动和不可移动媒质。通过示例但非限制，计算机可读媒质可能包括计算机存储媒质和通信媒质。计算机存储媒质包括易失性和非易失性、可移动和不可移动媒质，它们以用于存储诸如计算机可读指令、数据结构、程序模块或其它数据这样的信息的任意方法或技术来实现。计算机存储媒质包括、但不限于：RAM、ROM、EEPROM、闪存或其它存储技术、CDROM、数字化通用光盘（DVD）或其它光盘存储器、磁带盒、磁带、磁盘存储器或其它磁性存储设备、或用于存储期望信息并能由计算机 110 访问的任意其它媒质。通信媒质一般在诸如载波或其它传输机制这样的已调数据信号中包含计算机可读指令、数据结构、程序模块或其它数据，并且包括任意信息传递媒质。术语“已调数据信号”意指其一个或多个特性以对信号内信息进行编码的方式被设置或改变

的信号。通过示例但非限制，通信媒质包括诸如有线网络或直接线连接这样的有线媒质、以及诸如声音、RF、红外这样的无线媒质及其它无线媒质。上述的任意组合应该包含在计算机可读媒质的范围内。

系统存储器130包括计算机存储媒质，其形式为易失性和/或非易失性存储器，譬如只读存储器（ROM）131和随机存取存储器（RAM）132。基本输入/输出系统133（BIOS）一般存储在ROM 131内，它包含例如启动期间帮助在计算机110内的组件间传输信息的基本例程。RAM 132 一般包含数据和/或程序模块，它们可以立即访问并且/或者当前由处理单元120在其上操作。通过示例但非限制，图1说明了操作系统134、应用程序135、其它程序模块136和程序数据137。

计算机 110 可能还包括其它可移动/不可移动、易失性/非易失性计算机存储媒质。仅仅通过示例，图1说明了对不可移动、非易失性磁性媒质进行读写的硬盘驱动器140、对可移动、非易失性磁盘152进行读写的磁盘驱动器151、以及对可移动、非易失性光盘156进行读写的光盘驱动器155，譬如CD RAM或其它光学媒质。示例性操作环境中可用的其它可移动/不可移动、易失性/非易失性计算存储媒质包括、但不限于：磁带盒、闪存卡、数字通用盘、数字视频磁带、固态RAM、固态ROM、及其它。硬盘驱动器141一般通过如接口140这样的不可移动存储器接口与系统总线121相连，且磁盘驱动器151和光盘驱动器155一般用如接口150这样的可移动存储器接口与系统总线121相连。

上面讨论并在图 1 中说明的驱动器和它们的相关计算机存储媒质为计算机110提供了计算机可读指令、数据结构、程序模块和其它数据的存储。在图1中，例如，所述硬盘驱动器141存储操作系统144、应用程序145、其它程序模块146和程序数据147。注意到这些组件或者可与操作系统134、应用程序135、其它程序模块136和程序数据137相同，或者与它们不同。这里为操作系统144、应用程序145、其它程序模块146和程序数据147给出不同数字以说明它们至少是不同的复制物。用户可能通过诸如键盘162和指示设备161这样的输入设备把命令和信息输入到计算机20中，输入设备通常称为鼠标、轨迹球或触板。其它输入设备（未示出）可能包括麦克风、游戏杆、游戏板、卫星式转盘、扫描仪及类似物。这些和其它输入设备经常通过与系统总线耦合的用户输入接口160与处理单元120相连，但也可能用其它接口和总线结构连接，譬如并行端口、游戏端口或通用串行总线（USB）。监视器191或其它类型的显示设备也通过诸如视频接口190这样的接口与系统总线121相连。除了监视器之外，计算机可能还包括其它外部设备，如扬声

器 197 和打印机 196，它们可能通过输出外设接口 190 连接。

计算机 110 可能工作在网络化环境中，该环境使用与诸如远程计算机 180 这样的一个或多个远程计算机之间的逻辑连接。远程计算机 180 可能是个人计算机、服务器、路由器、网络 PC、对等设备或其它公共网络节点，并且一般包括上述与计算机 110 有关的许多或全部元件，尽管图 1 中仅说明了存储器存储设备 181。图 1 所述的逻辑连接包括局域网（LAN）171 和广域网（WAN）173，但可能还包括其它网络。这种网络环境在办公室、企业范围计算机网络、企业内部网和互联网中是常见的。

当用于 LAN 网络环境中时，计算机 110 通过网络接口或适配器 170 与 LAN 171 相连。当用于 WAN 网络环境中时，计算机 110 一般包括用于在诸如因特网这样的 WAN 173 上建立通信的调制解调器 172 或其它装置。调制解调器 172 可能是内部或外部的，它可能通过用户输入接口 160 或其它适当机制与系统总线 121 相连。在网络化环境中，关于计算机 110 所述的程序模块或其部分可能存储在远程存储器存储设备中。通过示例但非限制，图 1 说明了驻留在存储器设备 181 上的远程应用程序 185。可以理解，所示网络连接是示例性的，也可能使用在计算机间建立通信连接的其它装置。

数字签名子对象

按照本发明，在标头对象包括要被保护的子对象的子对象和区域时，为了能验证已签名的子对象和区域尚未受到干扰，则可能向标头添加数字签名子对象。该数字签名子对象可能基于任何数字签名算法，算法取得某些数据作为输入并产生稍后能被验证的签名。在一个实施例中，所用算法是 RSA 算法。在另一实施例中，使用椭圆曲线算法。其它实施例可能使用其它签名算法。

参考图 2，文件 200 包含标头对象 210。除了标头信息 215 之外，标头对象 210 包含文件属性子对象 220、流属性子对象 230、脚本命令子对象 240、及内容说明子对象 250。内容说明子对象 250 包含与内容的标题 252、作者 254、版权 256 和说明 258 有关的信息。。脚本命令子对象 240 包含 URL245。文件 200 还包含数据对象 290。该签名是示例性的，并且可以认识到除了所示那些子对象之外，标头对象中可能还存在其它子对象的组合。

实体可能通过添加数字签名子对象 260 而防止窜改部分标头对象 210。数字签名子对象 260 包含区域指示符数组 264 和签名 266。在一个实施例中，数字签名子

对象 260 还包含签名者信息 268。在一个实施例中，签名者信息 268 包含可用于安全验证签名 266 的一个或多个证书。

图 3 示出用于创建数字签名子对象 260 的过程。如步骤 310 所示，实体决定要签署哪一个或多个标头子对象，并确定这些区域的区域指示符。例如，参考图 2，要被签署的区域可能包括脚本命令子对象 230 以及内容说明子对象 250 的标题、作者和版权部分。再次参考图 3，在步骤 320 中，创建了区域指示符数组 264（从图 2）。在步骤 330 中，区域指示符数组 264 内指定的区域与区域指示符数组 264 串接（以它们在区域指示符数组 264 内被指定的顺序）。该区域然后被签名 340 以产生签名 266（从图 2）。

当包含标头对象的文件被修改时，其中标头对象包括数字签名子对象，子对象的顺序可能被改变并且可能插入附加的子对象。如果附加区域或子对象要被验证，则可能添加新的数字签名子对象。

参考图 2，为了检查标头对象 210 的验证而使用了数字签名子对象 260 和区域指示符数组 264 中指定的区域。如图 4 所示，在步骤 410 中标识了区域指示符数组 264（来自图 2）中指定的标头子对象区域。在步骤 420 中，这些区域与区域指示符数组 264 串接（以它们在区域指示符数组 264 内被指定的顺序）在一起。在步骤 430 中，检查签名 266（来自图 2）以确定它是否是用于串接的有效签名。

在本发明的一个实施例中，可能用数字签名子对象签署子对象的区域和完整的子对象。在另一实施例中，可能仅签署完整的子对象。在本发明的一个实施例中，在一个数字签名子对象中可能签署来自单独子对象的不止一个区域。在本发明的一个实施例中，被签署的一个子对象的区域可能重叠。

在发明的一个实施例中，每个标头对象必需包含至少一个数字签名子对象。如果标头对象在期望数字签名子对象时并不包含它，则可以假定该标头对象已受到窜改。如果标头对象包含一个未正确验证或者不是来自可信源的数字签名子对象，则在一种实现中，例如，接收包含标头子对象的文件的实体可能通过不使用该文件而作出相应行动。按照该实施例，进行检查来看是否存在任意数字签名子对象。如果不存在，则验证失败。如果存在子对象，则每一个都被检查以产生验证结果。

在一个实施例中，可能按照本发明签署作为对象 $O_1, O_2, \ldots O_n$ 的集合的任意文件 F。创建新的对象 O_{DS}，它包括一区域指示符数组，指示已签名对象的对象或区域以及那些对象和数组的签名。

示例性 ASF 实现

在一个实施例中，文件是 ASF 文件。图 5 示出一个实施例中 ASF 文件的数字签名子对象的组成。数字签名子对象包括 GUID 510。ASF 文件内的每个对象和子对象都以 GUID 开始。GUID 用于唯一标识 ASF 文件内的所有对象类型。每种 ASF 对象类型具有其自身唯一的 GUID。然而，一般而言，GUID 不能用于唯一标识 ASF 标头对象内的子对象，这是由于 ASF 标头对象内的多个子对象可能具有相同的对象类型，并从而具有相同的 GUID。

示例性 ASF 数字签名子对象 500 中的下一元素是子对象大小 520。同样，所有 ASF 对象和子对象一般包括对象和子对象的大小。如上所述，区域指示符数组 540 之前是区域指示符数组 530 中包含的已签名区域数目。校验和算法标识符 550 和签名算法标识符 560 标识了数字签名子对象中所用的校验和及签名算法。区域和区域指示符数组的签名 580 之前是签名长度 570。签名者信息 590 包含验证或获得关于签名者的信息所需的信息。签名者信息 590 可能包括签名者的身份。在一个实施例中，签名者信息 590 包含证书链，它可用来验证该签名者的公钥是来自可信源的。

在示例性 ASF 实现中，每个区域指示符都包含子对象区域偏移、子对象区域大小、校验和长度、及子对象校验和。区域偏移标识该区域在子对象中何处开始，而区域大小标识了区域的大小。对象校验和对应于所指定区域的校验和。在优选实施例中，该校验和算法是安全哈希算法（SHA-1）算法。该算法在联邦信息处理标准出版物 180－1 中可见，该出版物在互联网上 http://www.itl.nist.gov/fipspubs/fip180-1.htm可见。在另一实施例中，可以使用具有低冲突概率的任意哈希算法。在还有一个实施例中，对象校验和对应于包含所指定区域的子对象的校验和。

当签名被校验时，为了确定该区域位于哪个子对象中（如在图 4 的步骤 410 中），标头子对象被检查。对于每个被检查的子对象而言，按照校验和算法标识符 550 中指定的算法计算校验和。在其中在区域上计算校验和的实施例中，为包含在该子对象内的数据计算校验和，该子对象在给定的子对象区域偏移处开始并且扩展为给定的子对象区域大小。在其中在整个子对象上计算校验和的实施例中，为该子对象计算校验和。当所计算的校验和与区域指示符内的校验和相匹配时，则已标识了该区域指示符的正确子对象。当已经标识了相应于每个区域指示符的子对象时，签名可以被检查。

在这种实现中，为了指定要被签署的整个子对象，区域指示符内的偏移将为

零，且区域大小会等于子对象的长度。在另一实施例中，为整个子对象计算校验和而非为所指定区域而计算。

在这种实施例中，为了允许在具有不同区域的子对象一起被验证、以及具有不同实体来验证子对象方面的灵活性，对象内可能包括不止一个数字签名子对象。

在其它实施例中，可以用其它方法来标识区域。在一个实施例中，能唯一标识子对象的数据连同区域偏移和大小数据一起包含在区域指示符内。

在其它实施例中，可能仅签署整个子对象。在一个实施例中，区域指示符包括整个子对象上的校验和。在另一实施例中，还包括了校验和的长度。在还有一个实施例中，区域指示符中使用可以标识子对象的其它数据。

结论

这是一种用于数据流标头对象保护的系统和方法。如上所述，虽然已经结合各种计算设备和网络结构描述了本发明的示例性实施例，然而所基于的概念可以应用于任何计算设备或系统中，其中提供数据流标头对象保护是理想的。这样，按照本发明用于提供数据流标头对象保护的技术可以应用于多种应用和设备中。例如，本发明的技术可以应用于计算设备的操作系统中，它作为设备上的独立对象、作为另一对象的一部分、作为可从服务器下载的对象、作为设备或对象和网络间的“中间人”、作为分布式对象、等等。虽然这里把示例性名称和示例选作为各种选择的代表，然而这些名称和示例并非限制性的。

这里所述的各种技术可以结合硬件或软件或它们的组合而实现。这样，本发明的方法和装置、或它们的某些方面或部分可能采取有形媒质中含有的程序代码（即，指令）形式，有形媒质有：软盘、CD-ROM、硬盘驱动器、或任意其它机器可读的存储媒质，其中，当程序代码被载入并由如计算机这样的机器执行时，机器，例如计算机，则变成实现本发明的装置。在可编程计算机上执行程序代码的情况下，计算设备一般会包括处理器、可由处理器读取的存储媒质（包括易失性和非易失性存储器和/或存储元件）、至少一个输入设备、以及至少一个输出设备。一个或多个程序可能通过使用数据处理 API 及其它来使用本发明的技术，为了与计算机系统进行通信，这些程序最好用高级程序或面向对象的编程语言来实现。然而，程序可以根据需要以汇编或机器语言来实现。在任何情况下，语言可能是编译的或解释的语言，并且与硬件实现结合。

本发明的方法和装置也可以通过以程序代码形式包含的通信来实现，其中程

序代码在某些传输媒质上被发出，譬如在电线或电缆上、通过光纤、或通过任意形式的传输，其中，当程序代码被接收并被载入并由诸如 EPROM、门阵列、可编程逻辑器件（PLD）、客户端计算机、录像机及其它、或具有如上面示例性实施例所述的有信号处理能力的接收机并由机器执行时会成为实现本发明的装置。当在通用处理器上实现时，程序代码与处理器结合，以提供唯一装置，它工作以调用本发明的功能。此外，结合本发明使用的任意存储技术可能总是硬件和软件的组合。

虽然已经结合各图的优选实施例描述了本发明，然而可以理解，可以使用其它类似实施例，或者可以对所述实施例作出修改和添加来执行与本发明相同的功能并且不背离本发明。例如，虽然以诸如对等网络环境这样的网络化环境的上下文描述了本发明的示例性网络环境，然而本领域的技术人员可以认识到本发明并不限于此，且本申请中所述的方法可以应用于任何计算设备或环境中，譬如游戏控制台、手持计算机、便携式计算机等等，无论有线或无线，或者可以应用于通过通信网络连接的任意数量的这种计算设备中，并且在网络上交互动作。此外，应该强调，尤其随着无线网络化设备的数目继续增加，构想了包括手持设备操作系统和其它应用专用的操作系统的多种计算机平台。更进一步的是，本发明可以在多个处理芯片或器件中间或上面实现，且存储器可能相似地在多个器件上实施。因此，本发明不应限于任意单独实施例，而应该在按照所附实权利要求的宽度和范围内作解释。

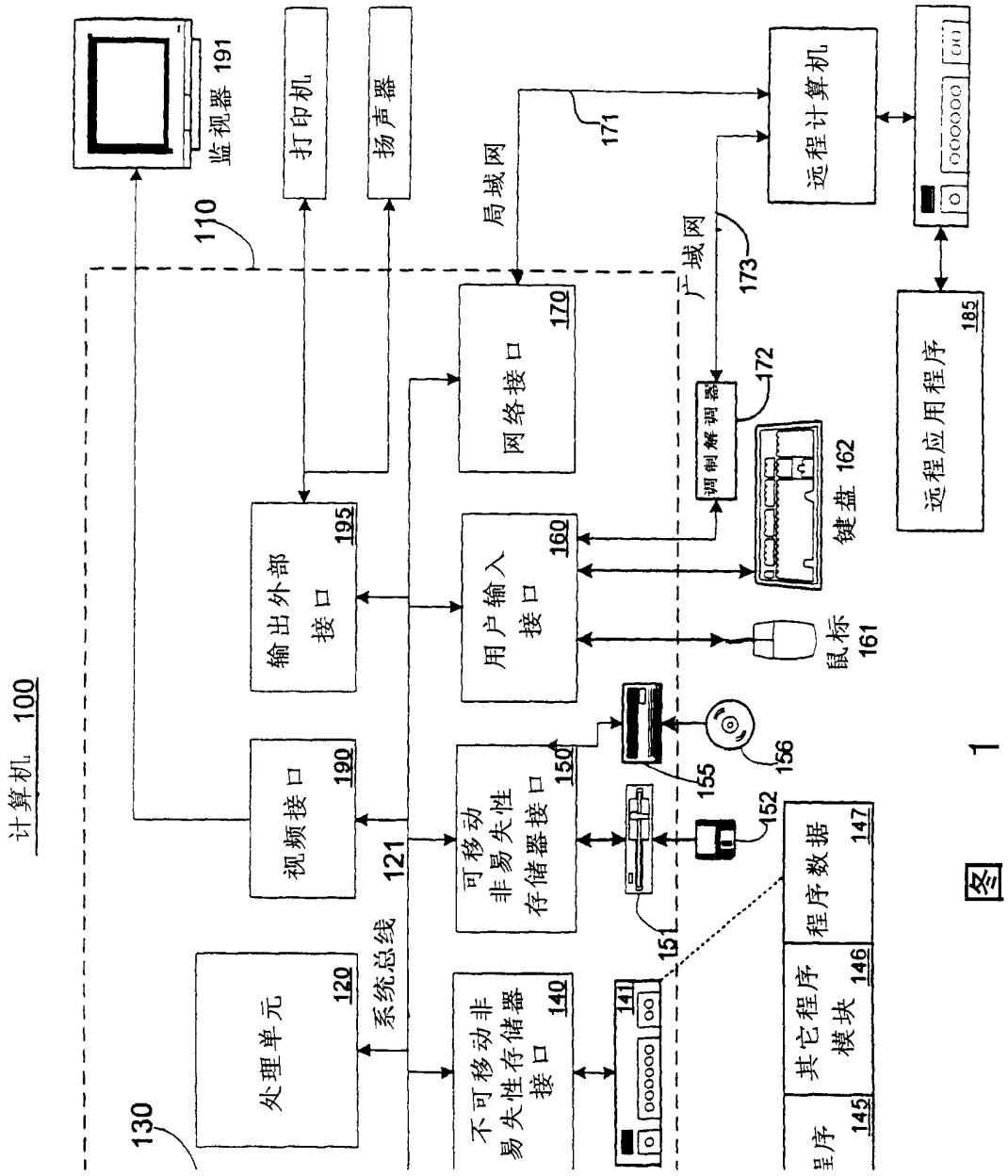

计算机 100
监视器 191
打印机
扬声器
局域网
171
远程计算机
110
广域网
173
网络接口 170
调制解调器 172
远程应用程序 185
输出外部接口 195
用户输入接口 160
键盘 162
鼠标 161
视频接口 190
可移动非易失性存储器接口 150
155
156
152
121
系统总线
处理单元 120
不可移动非易失性存储器接口 140
151
141
130
程序数据 147
其它程序模块 146
呈序 145

图 1

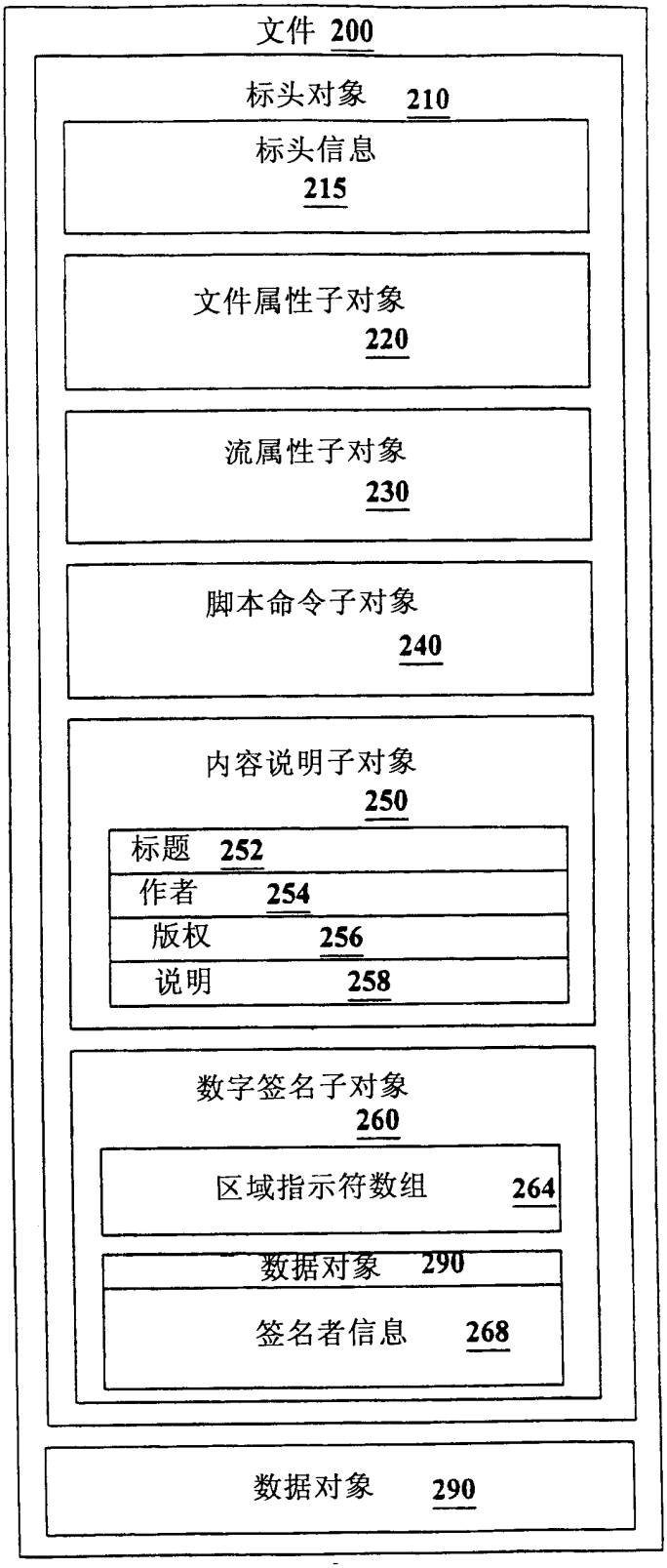

文件 200
标头对象 210
标头信息 215
文件属性子对象 220
流属性子对象 230
脚本命令子对象 240
内容说明子对象 250
标题 252
作者 254
版权 256
说明 258
数字签名子对象 260
区域指示符数组 264
数据对象 290
签名者信息 268
数据对象 290

图 2

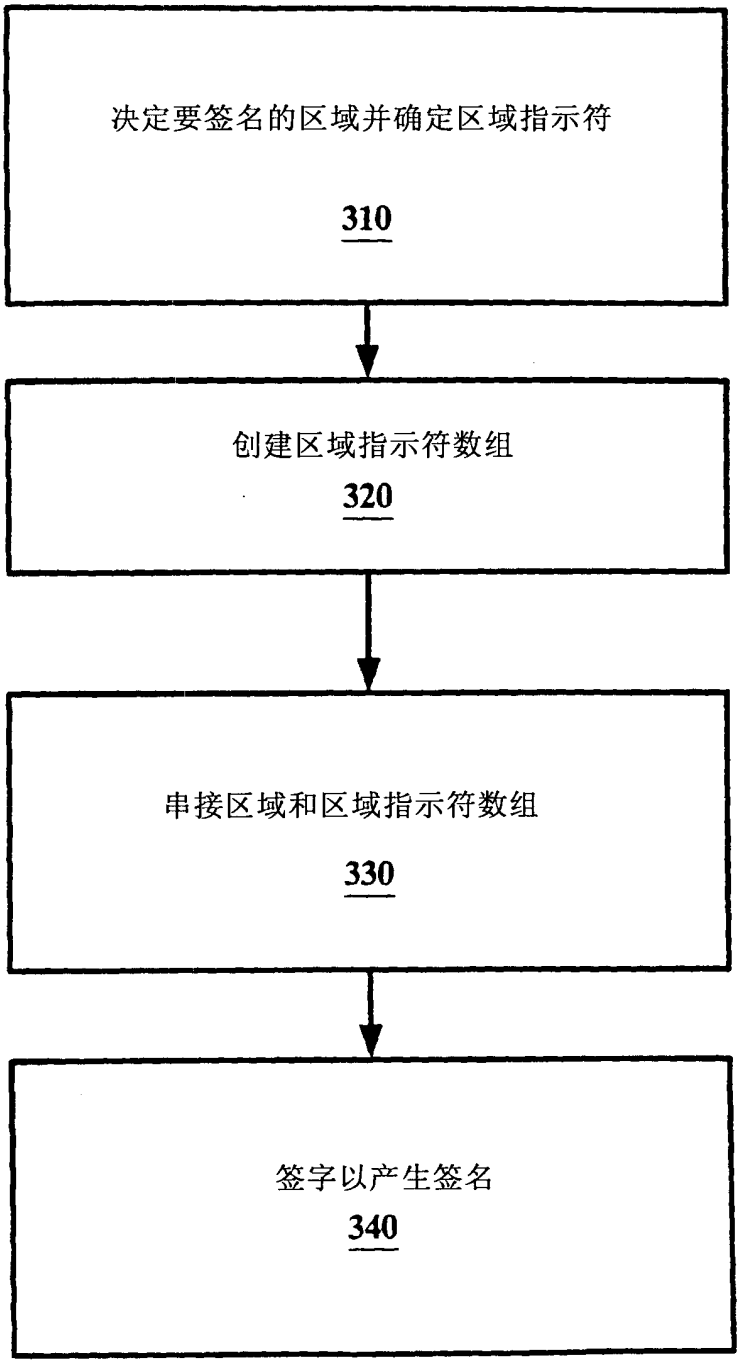

决定要签名的区域并确定区域指示符
310
创建区域指示符数组
320
串接区域和区域指示符数组
330
签字以产生签名
340

图 3

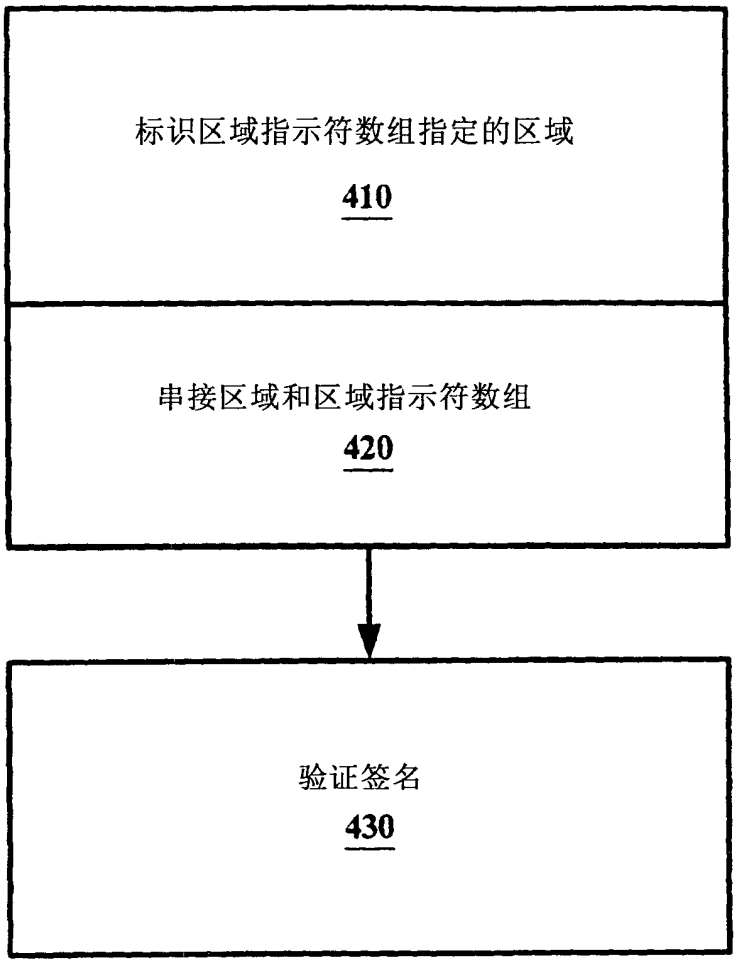


图 4

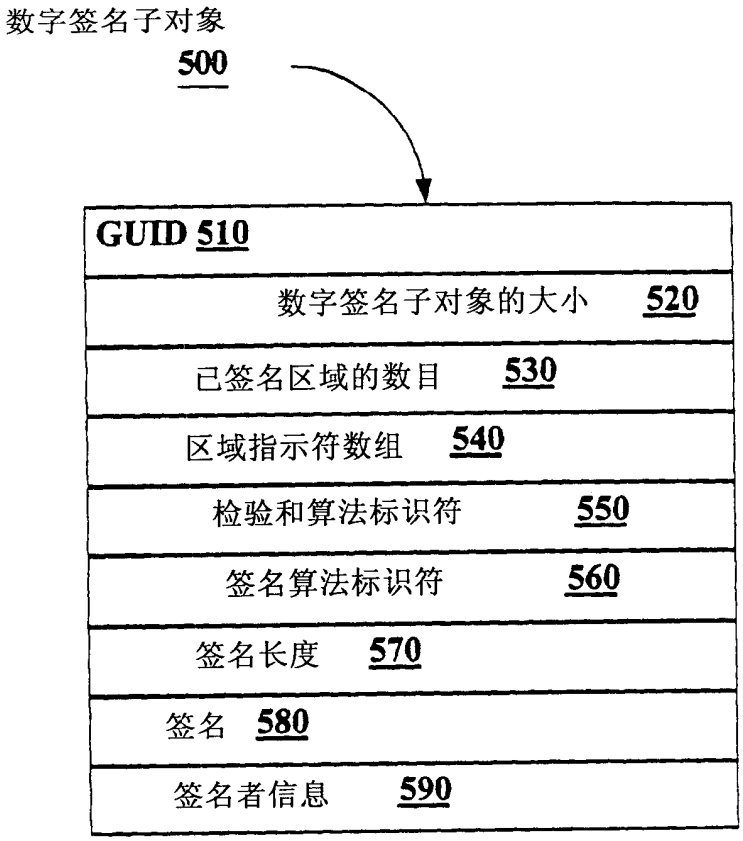

数字签名子对象
500
GUID 510
数字签名子对象的大小 520
已签名区域的数目 530
区域指示符数组 540
检验和算法标识符 550
签名算法标识符 560
签名长度 570
签名 580
签名者信息 590

图 5