



[12] 发 明 专 利 说 明 书

[21] ZL 专利号 97114585.7

[43] 授权公告日 2003 年 3 月 19 日

[11] 授权公告号 CN 1103470C

[22] 申请日 1997.7.7 [21] 申请号 97114585.7

[30] 优先权

[32] 1996. 7. 29 [33] CA [31] 2182254

[71] 专利权人 国际商业机器公司

地址 美国纽约

[72] 发明人 维东·考

[56] 参考文献

US5132900 1992.07.21 G06F15/38

US5369702 1994.11.29 H04L9/00

US5479509 1995.12.26 H04K1/00

审查员 刘 静

[74] 专利代理机构 中国国际贸易促进委员会专利
商标事务所

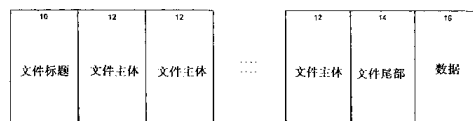
代理人 李德山

权利要求书 2 页 说明书 8 页 附图 9 页

[54] 发明名称 准备安全文件包装的方法

[57] 摘要

一种解决与安全存储及安全交换有关的问题的类安全文件格式。这种文件格式允许把多个文件包装成一个用于存储或传送交换的单个实体。每个文件可以具有不同于其它文件的安全要求。以这种安全文件格式在单个包装体下可以交换不同的文件类型。该安全文件格式还允许把一个文件分成多个节并把这些节包装为单个文件。该文件的每个节具有自己的安全保护。这样允许仅保护敏感信息。而其它节可具有较少的安全保护或者不具有安全保护。



1.一个准备安全文件包装的方法，包括：

- 标识要包装到一起的文件成分；
- 为每个所述文件成分规定安全要求；
- 规定安全文件包装的安全要求；

-为每个所述文件成分获得用于安全要求的参数，调用与每个文件成分有关的安全要求所相关的安全函数并对每个文件成分进行处理；-为安全文件包装获得用于安全要求的参数并且调用与安全文件包装有关的安全要求所相关的安全函数；以及

-创建一个安全包装文件，其特征在于，所述创建步骤进一步包括如下步骤：

-对用于所述安全包装文件的文件标题进行格式化，其中所述标题标识所述安全包装文件的起点和长度；

-重定所述文件成分的格式以提供（a）至少一个数据文件，其包含在所述安全包装文件中的所述处理的文件成分，其中所述数据文件的一部分采用保密形式，以及（b）在所述安全包装文件中用于每个所述处理的文件成分的文件主体，其中每个所述文件主体包含指向所述数据文件中的所述处理的文件成分的指针以及用于所述处理的文件成分的安全保护；以及

-对用于所述安全包装文件的文件尾部格式化，其中所述尾部对所述安全包装文件提供安全保护。

2.按照权利要求 1 的方法，其特征在于：

-对每个所述文件成分规定安全要求的步骤包括确定每个文件成分所需的安全保护以及确定和所述安全保护相关的安全算法；以及

-对每个所述文件成分获得用于安全要求的参数的步骤包括获得用于安全算法的参数。

3.按照权利要求 2 的方法其特征在于，对每个所述文件成分规定

安全要求的步骤进而包括规定算法的操作方式，所使用的字符集和输出文件名。

4.按照权利要求 1 的方法其特征在于，文件成分是单独的文件。

5.按照权利要求 1 的方法其特征在于，文件成分是复合文件中的节。

6.一种准备安全文件包装体的方法，包括：

-选择要在包装体中包装的文件成分；

-重定文件成分的格式以提供（a）一个用于每个文件成分的文件主体，其中所述每个文件主体包含着指向文件数据的指针和所述文件数据的安全保护，以及（b）至少一个含有所述文件数据的数据文件，其中所述文件数据的一部分采用保密形式；

-处理规定着包装体的起点和长度的包装体的文件标题；以及

-处理为包装体提供安全保护的文件尾部。

7.按照权利要求 6 的方法，其特征在于进而包括按如下次序处理包装体的步骤：（i）文件标题；（ii）所有的文件主体；（iii）文件尾部；以及（iv）所述至少一个数据文件。

8.按照权利要求 6 的方法，其特征在于每个所述文件主体进而包括一个识别文件成分和文件主体的长度的标记，而且特征在于安全保护包括安全类型以及用于所述安全类型访问保密形式下的文件数据的安全算法。

9.按照权利要求 6 的方法，其特征在于文件尾部包含一个标识尾部长度的、安全说明及包装体的参数的标记。

10.按照权利要求 6 的方法，其特征在于文件成分是单独的文件。

11.按照权利要求 6 的方法，其特征在于文件成分是复合文件的节。

准备安全文件包装的方法

技术领域

本发明涉及电子数据传送领域并提供一种文件结构，这种文件结构允许安全地捆绑具有不同安全性要求的多个数据成分以用于存储和传送，对文件结构的任何篡改企图在打开组成的成分时将会变成非常明显。

背景技术

在商务交易中信息的电子存储及电子发送的使用日益增多。由于可能包括来自不同来源的数据商业信息是特别复杂的，为了具有一个有意义的文件或者一系列有意义的文件必须把这些数据保持在一起。而且这些数据中的一些数据可能是和其它不太敏感或不敏感信息结合的高敏感性信息，例如财务数据。

可以以不同的方式保持这种类型的电子信息，例如，采用带有多个节或者多个数据区的单个电子文件（复合文件）的形式以作为多个独立的电子文件或者电子资料，或者采用复合式电子文件结合的形式。可能要求把这些文件存储在计算机系统里，或者可能在两个用户间在同一个计算机系统上或在不同计算机系统构成的网络上交换这些文件。

取决于敏感性程度，电子信息的不同部分可能需要不同形式的安全保护，以防止或者观看信息或者更改信息的未经授权的访问。

长期以来已经认识到对于数据存储系统需要在保持整个文件的完整性的前提下实现安全的文件格式。在这些系统里，如在授予 Fischer 题目为“利用单个散列防止勿失文件的方法”的美国专利 5,475,826 号中所讨论的那样，通常在单个文件散列值下保持和封装所有记录的相互关系。

授予 Taligent 公司题目为“可扩充的面向对象的文件系统”的美国专利 5,504,892 号公开一种系统的一个例子，在其中利用面向对象编程的分层性质提供一个用于带有一个文件系统项目分类的可扩充面向对象的文件系统的框架，该文件系统项目分类再细分类成卷、目录和文件子分类。利用用户鉴别和保护范围防止对文件系统实体的未经批准的访

问。通过提供本地鉴别服务达到用户鉴别，并经过文件系统实体之一的方法实现保护范围。为了提供与外部文件系统的相互可操作性，该专利公开一种机制，这种机制在把外部文件传送到该专利公开的系统之前把外部文件包装成兼容格式。当向回传送外部文件时，这些文件解包装成外部文件系统的格式。

授于 Honeywell 公司题目为“带有格式控制的安全数据处理系统体系结构”的美国专利 4,713,753 号说明另一种数据处理系统的体系结构，以采用文件格式控制和受保护的文件系统来进行安全存储和数据处理。在这种方法里，在所有的时空中把受保护的系统文件保持在一个安全的处理机里，而用户对文件的访问是作为一种比较函数提供的，这种比较是在与各文件相关的各种格式与各个文件属性的函数之间或者与执行所需操作的子系统之间进行的。

欧洲专利申请 EP661651 - A1 号公开带有文件系统服务的目录服务的统一化，并且在公用逻辑格式下存储目录项目和其它文件。这种系统允许在这些项目以及所使用的公用名空间上运行公用的工具集。其采用安全措施以防止未经批准的对目录服务项目的访问。

两份 IBM 公司的技术公开通报，“数据库安全性/权限机制”(Vol.28, No. 3, 1985 年 8 月)以及“共享文件的更改通知服务”(Vol.36, No. 8, 1993 年 8 月)，说明包括着带有文件格式的文件维护实用程序的数据库安全和权限的机制。

在电子商务应用中，交易中的一些财务数据可能要求加密，其它信息可能要求数据完整性（只读访问），并且整个交易或者它的一些部分可能要求数字签字。该交易还可能包含明码形式下的寻址信息以便允许由通信软件解释。不能为了保护最敏感的信息简单地加密整个交易文件，因为这会把通信寻址信息转换成通信软件不能读出的形式。

以前只能在一些类型的文件中实现对文件的仅仅一部分的加密。例如，可以得到可对电子表格里的某些单元加密的加密算法。但是，这种技术不适用于广泛类别的文件格式，也不适用于打算用于电子传送的文件。而且，对文件一些部分的加密不能和对文件的相同或不同部分的其它安全要求相结合。

简单的电子消费品购买是一种涉及要求多种安全保护的单个复合资料的交易例子。每个交易文件可能包括多个数据区，而且各个数据区可能具有不同于相同交易中的其它数据区的安全要求。例如，诸如信用卡号码及其终止时间可能需要加密，寻址信息可能需要数据完整性，而整个交易可能需要数字签字。

类似地，在实际交易中，通常买方和卖方按标准表格协商。打印在表格上的大多数信息不需要任何形式的安全保护。但是，价格将是保密的并且可能需要加密，尤其当用不安全的网络传送报价时。附属于报价的条件也可能需要加密，而且由于在买方还价中可能增减条件，某次发送中的加密信息的长度可能不同于下次发送中的长度。另外，协商中一方作出的修改将必须由作出修改的该方签字（草签）。

其它类型的商务应用例如可以包括由多于一个人准备或者多于一个来源发出的交易而形成的电子文档所产生的多个文件或资料。和政府部门的典型商务交易可能包括最终购货单以及背景资料。商务交易的其它例子是报价、征求报价、招标及征求招标、发货单以及确认。

由于几种资料和单个交易有关，为了传送或存储应该把所有的文件包装在一起。但是，包中的各个文件可能具有它自己的独立于交易中所使用的其它文件所要求的安全性类型的安全性要求，从而，存在一种能够把多个文件捆包成一个具有多种安全性要求的单个实体以供在这些应用中进行交换和存储的需求。

目前存在着几种可用于把几个文件包装成单个文件以供发送或存储的实用程序（例如，PC上的PKZIP和UNIX上的tar）。也存在着在多个文件记录之间提供数据交换的机制，例如可在Wang Laboratories公司的题目为“数据交换设备和方法”的美国5,021,995号专利中找到，该专利公开借助产生代表数据的用于标记源文件逻辑记录中的数据区的类格式实现文件记录之间的数据交换。还可以在Industrial Technology Research Institute的题目为“用于访问以不同文件系统各式存储的多个记录的接口”的美国5,522,066号专利中找到，该专利公开一种用于访问以不同的文件系统格式存储的多个记录的接口。但是，它们都没有提供一种一旦访问或捆包一些文件或一些记录之后保持和各个文件或记录相

关的不同安全特性的手段。

发明内容

本发明的一个目的是提供一种把几个文件成分捆包在一起的机制，这种机制和文件成分是否为文件的一部分、全文件、资料或者交易事务无关，并且同时保留这些成分的不同安全性要求。

本发明的再一个目的是提供一种和操作环境无关的并可用于所有文件类型的捆包机制。

因此，本发明提供一种准备安全文件包装的方法，该方法包括步骤：识别要包装在一起的文件成分，为每个文件成分规定安全参数以及规定安全文件包装的安全要求。接着，为每个文件成分获得用于安全要求的各种参数，调用和安全要求相关的安全函数并对该成分进行处理。还获得用于安全文件包装的安全要求参数并且调用和这些安全要求相关的安全函数以及创建一个安全包装文件，所述创建步骤进一步包括如下步骤：对用于所述安全包装文件的文件标题进行格式化，其中所述标题标识所述安全包装文件的起点和长度；重定所述文件成分的格式以提供(a)至少一个数据文件，其包含在所述安全包装文件中的所述处理的文件成分，其中所述数据文件的一部分采用保密形式，以及(b)在所述安全包装文件中用于每个所述处理的文件成分的文件主体，其中每个所述文件主体包含指向所述数据文件中的所述处理的文件成分的指针以及用于所述处理的文件成分的安全保护；以及对用于所述安全包装文件的文件尾部格式化，其中所述尾部对所述安全包装文件提供安全保护。

在另一个方面，本发明提供一种准备类安全文件包装体的方法，该方法包括选择在包装体中包装的文件成分，并且重定文件成分的格式以便为各个文件成分提供一个文件主体而且至少一个文件含有文件数据。该文件主体具有指向文件数据的指针及安全保护，并且最好还包括一个标识文件成分和文件长度的标记。安全保护最好还包括安全类型及这些类型相关的算法以便访问被保护的文件数据。

该方法还包括处理标识包装体的起点和长度的包装体的文件标题的步骤以及处理对包装体提供安全保护的文件尾部的步骤。

在再一个方面，本发明提供一种加密用于传送或存储的文件的包装体，其包括一个标题，用于标识包装体的起点和长度；至少一个文件主体，它包含着指向文件数据的指针、对文件数据的安全说明以及指向用于访问文件数据的输出文件说明参数；一个含有包装体的安全说明的尾部；以及一个含有文件数据的文件。

附图说明

现在结合附图详细说明本发明各种实施方式，附图中：

图 1 是根据现有技术的通信文件的示意表示;

图 2 是根据本发明实现的一种文件结构的示意表示;

图 3、4、5 分别示意表示根据本发明图 2 中所示文件结构的文件标题部分、文件主体部分和文件尾部部分;

图 6、8、9 是根据本发明的另一个方面对图 2 中所示的文件结构的替代方案。

图 7 表示用于通信目的约在 GSFF 文件之前抽出的地址; 以及

图 10 和图 11 是流程图, 分别说明根据本发明的再一个方面在类安全文件格式下为了传送或者存储对各种文件进行包装和解包装。

图 1 表示电子交易如提供商品的投标中的典型通信文件的结构。文件包括多个数据区, 每个数据区含有交易所需的重要信息。数据区 1 中包含传送的地址目的地。如上面所述, 地址一般是以明码为格式的, 从而地址可由在网络上传送时遇到的任何标准通信软件不费力地理解。但是, 在传送之前, 地址数据区 1 可能还要受到完整性检查, 以确保该数据描述有效地址。

数据区 2 包含来自贸易商的订购信息, 例如一宗数量的价格。因为该信息可能包括仅对某些客户有效的折扣, 有可能该数据区应加密从而只有收件人可以访问该信息。

数据区 3、4、5 可能包含不太机密的其它信息, 例如交货日期以及其它销售条件。尽管这些信息可以不会敏感到需要加密, 但仍可能需要采取其它的安全措施如文件散列法等等以限制到只由收件人访问。

最后, 数据区 6 包含投标方的数字签字, 当收件人接受投标时需要数字“回签”。

图 1 的投标资料可以是单份交易文件, 或者它可以只是构成更大交易的一些资料中的一份资料。如果图 1 的资料例如和提供在适当的制造过程中运行的系统软件有关, 则当和其它资料汇总形成交易以供传送时, 软件说明以及甚至软件的来源都是高度机密要求对整个文件进行安全包装的信息, 另外还要对价格条款进而加密。

从而, 为了解决这些不同的安全要求, 本发明提供一种类安全文件格式 (GSFF), 它的一种实施方式在图 2 中表示。这种文件格式允许

把多个文件包装到单个实体中以便存储或交换。每个文件可以具有不同于其它文件的安全要求。在这种安全文件格式下借助单个包装体可以交换不同的文件类型。这种文件格式还允许把一个文件划分成多个节并且把这些节包装到单个文件里。文件的每个节具有它自己的安全保护。这允许只保护敏感性的信息并让其它的节具有较少的安全保护或者不具有安全保护。这产生更高的性能，因为只有文件的一小部分需要与安全有关的操作。

本发明的类安全文件格式支持的安全性能包括通过加密的数据保密，通过散列法的数据完整性、报文摘要、报文鉴别代码（由 ANSI 标准定义的 MAC）以及数字签字。

如图 2 中所示，类安全文件格式包括一个文件标题 10，接着是多个概括性地用 12 标注的文件主体，一个文件尾部 14，其后是数据 16。如后面所说明的实施，每个文件主体 12 可以具有不同于其它主体的安全要求。例如，一个文件可能需要加密，而另一个文件可能只需要数据完整性保护。

根据其要求包装每个文件，并且在一个文件主体中对此作出说明。在文件主体节中包括一个指向数据的指针并把数据置放在文件尾部之后。

本发明的类安全文件格式是一种基于目录的文件格式。文件标题、文件主体和文件尾部被认为是包装体中的目录。文件标题含有文件标识符、类安全文件格式的版本号以及包装体的长度，每个文件主体含有和该文件主体相关的项目。文件尾部可以用于对整个包装体的安全保护。

图 3 中示意表示文件标题的结构。文件标题包括类安全文件格式标识符 20 即一个由一些字节组成的简单标识文件格式的标记（如区分 Intel 公司和 Motorola 公司的字节次序），类安全文件格式的版本号 22，文件指示符 24 以及类安全文件格式下的整个文件的长度 26。

每个文件主体说明包装体中的一个文件。如图 4 中示意表示的那样，文件主体包括文件主体标记 28 以及在此之后的安全说明 30，文件主体标记用于把文件类型标识成文件主体并且表述文件长度。安全说明包括安全类型、安全算法、安全算法参数、密码-密钥信息、操作方式、

滤波器、字符集、输出文件说明参数、数据长度以及一个用于文件尾部之后的安全保护文件数据的数据指针。

图 5 中示意性表示的文件尾部包括一个文件尾部标记 32, 用于把该文件标识成尾部并且规定尾部文件的长度。尾部文件还包括一个节 34, 以表述安全说明及参数。安全说明所包含的字节规定安全类型、安全算法、安全算法参数、密码-密钥信息、操作方式、滤波器、字符集以及其它安全参数。

图 6 示意性表示根据本发明的用于传送目的的类安全文件格式的一种变型的实施方式。在该实施方式中, 明码形式的地址 42 是第一数据段, 之后是用于附加数据的附加数据段 (44 和 48), 加密数据 46 和数字签字数据 50。因为已经知道 GSFF 文件的标题、各文件体以及文件尾部的长度, 可以立即定位地址数据并用于通信目的。

在图 7 中所示的格式下还可以从 GSFF 文件抽取出地址数据并用于通信, 在该图中地址 52 处于被包装文件或者文件集合之首。这两种例子对于向单一的地址发送具有安全要求的一些资料是有用的。

图 8 和图 9 表示向多个目的地发送数据的两种变型的实施方式。在图 8 中, GSFF 文件中含有作为前二个数据段的多个地址 58 和 60。保密数据段 62 发送到这二个地址。在图 9 中, GSFF 文件含有多个数据段和多个地址。对每个地址将发送不同的数据段 (组)。

对于图 6、7、8、9 中表示的所有情况, 在不破坏 GSFF 文件的数据完整性特性的前提下通信软件可以方便地定位、提取或使用地址信息以便发送保密信息。对于发送 GSFF 文件中所包含的保密数据既无须加密也不必数字签字核实。

本发明还提供向不同的文件施加安全措施的方法, 这些方法表示在图 10 和图 11 的流程图中。

图 10 表示所谓的在类安全文件格式 (GSFF) 下“包装”单个复合文件或者一些文件的各个步骤。

按照最佳实施方式, 第一步骤是识别要处理的各个文件 (在包装多个文件的情况下) 或者各个节 (在包装单个文件的情况下) (块 78)。需要规定每个文件 (或者一个文件的每个节) 的安全要求 (块 80)。这

个步骤确定每个文件（或者一个文件的每个节）需要什么样的安全保护、每种安全保护的安全算法、如果施加时选定算法的操作方式、滤波器要求、所使用的字符集、输出文件名以及其它信息。类似地，需要规定整个 GSFF 文件的安全要求（块 82）。在确定安全要求之后，得到每个安全算法使用的参数，并处理每个文件（或者一个文件的每个节）（块 84）。在得到整个 GSFF 文件所需的安全算法的参数之后，调用每个安全算法的相关安全函数，以建立 GSFF 文件（块 86）。

图 11 表示接收时涉及到的“解包装”类安全文件格式文件的各个步骤。“解包装”处理开始于打开文件（块 88）和检验 GSFF 文件标识符（块 89）。如果打开的文件是一个 GSFF 文件，则继续处理；不然的话，则停止。处理 GSFF 文件标题以确定 GSFF 版本、文件指示符及文件长度（块 90）。读入各个文件主体以及文件尾部信息，并且确定整个 GSFF 文件以及每个文件（或者一个文件的每个节）的安全保护类型（块 92）。为整个 GSFF 文件调用各个安全函数（块 94）。安全函数的一个例子是用于整个 GSFF 文件的数字验证函数。然后，对每个文件（或者对一个文件的每个节）调用各个安全函数（块 96）。在多个被包装文件的情况下把输出数据写入到多个文件里，或者在被包装的复合文件的情况下把输出数据写入到单个文件里（块 98）。关闭 GSFF 文件并结束“解包装”处理（块 100）。

上面提出的解决方法 and 操作环境无关并且适用于任何的文件类型，并允许用户对复合文件的一部分或者一个文件包中的单个文件进行加密和/或数字签字。每个资料/文件处理成一个具有多个安全要求的实体。可以自由地在不同的操作环境下交换按类安全文件格式（GSFF）包装的单个文件或者文件集合。

尽管已对最佳实施方式作出说明，熟练的技术人员显而易见的修改应复盖在附属权利要求书的范围之内。

图 1

现有技术

1 地址
2 价格/数量
3 发货日期
4 条件
5 条件
6 数字签字

图 2

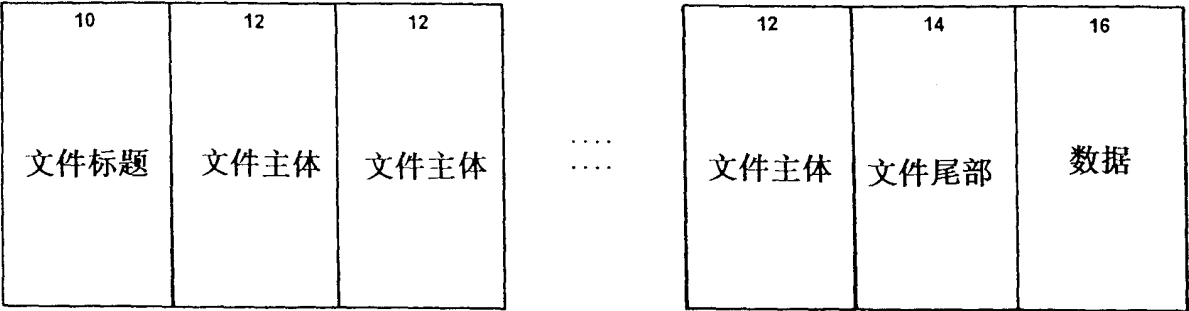


图 3

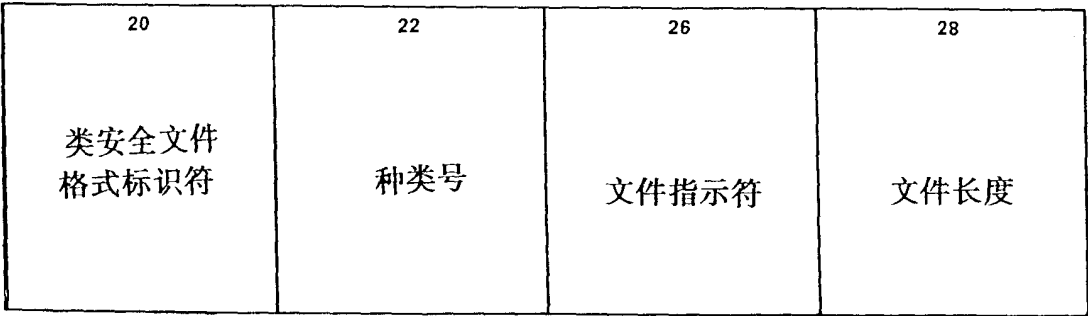


图 4

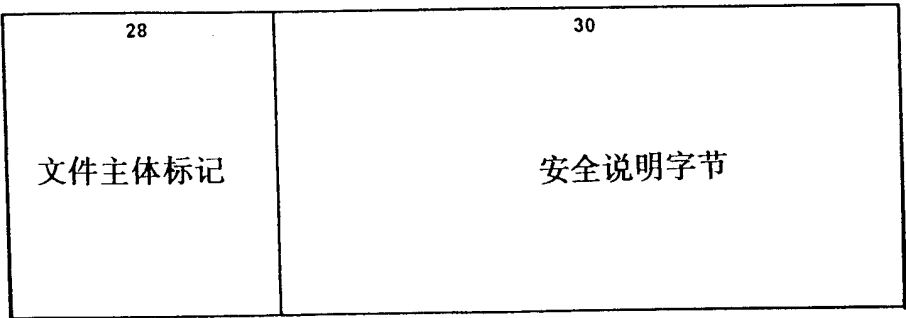


图 5

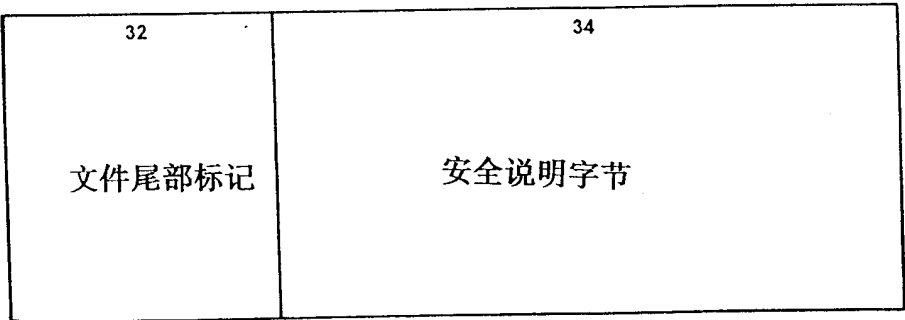


图 6

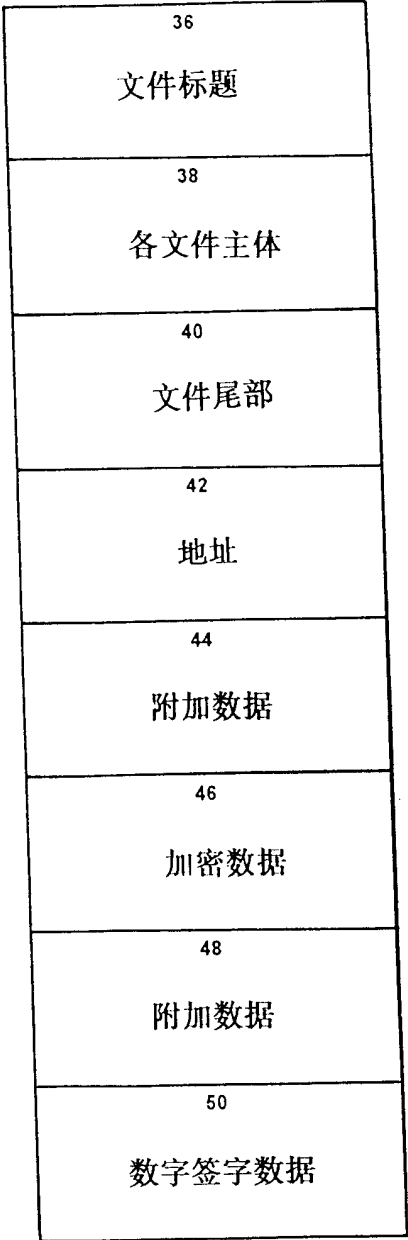


图7

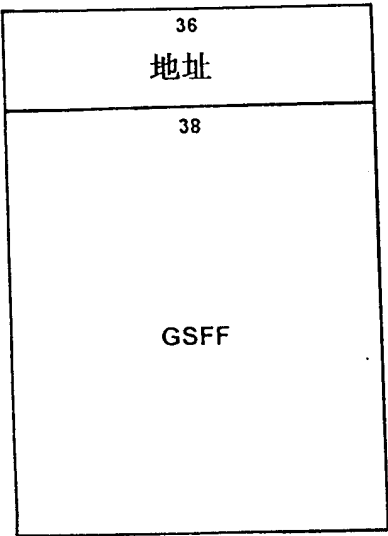


图 8

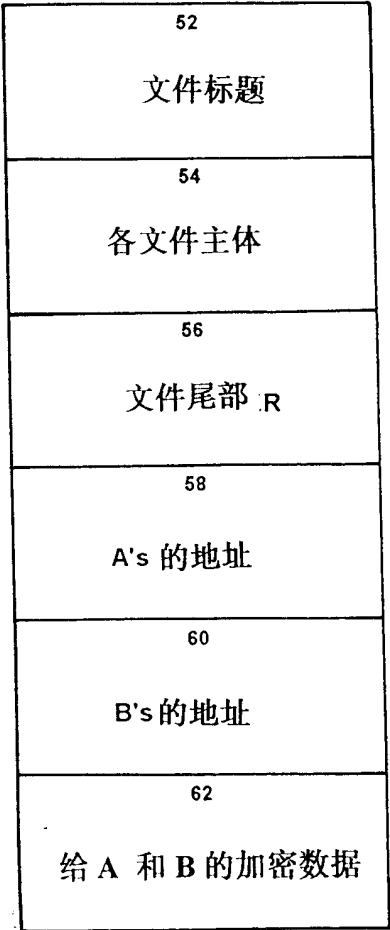


图 9

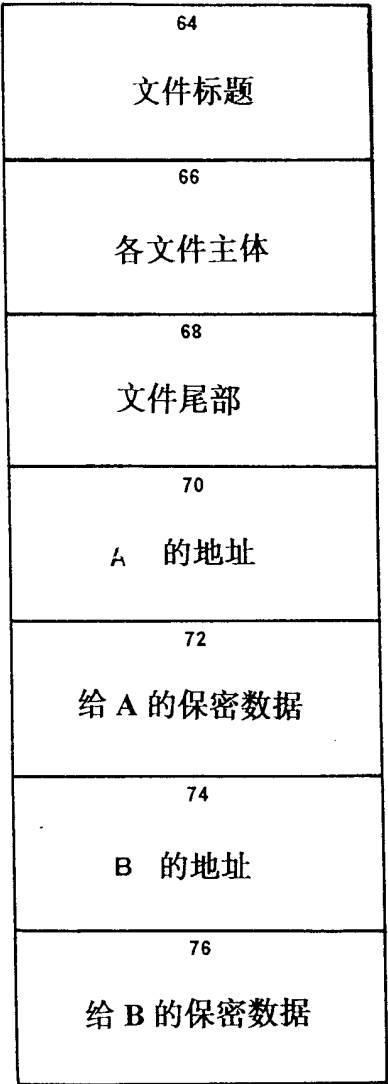


图10

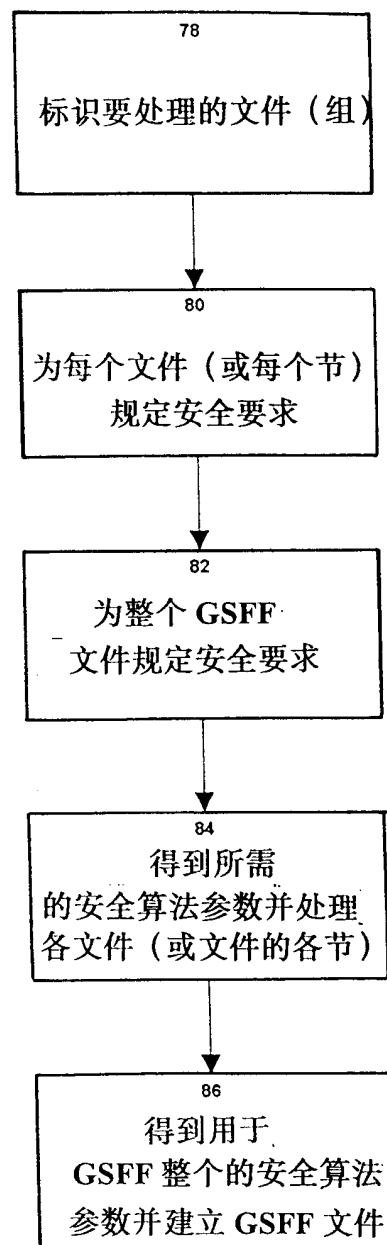


图11

