[19] 中华人民共和国国家知识产权局

[51] Int. Cl.
*G06K 1/12 (2006.01)*
*G06K 15/02 (2006.01)*
*H04L 9/00 (2006.01)*
*G06F 21/00 (2006.01)*

[12] 发明专利说明书

专利号 ZL 200710152342.5

[45] 授权公告日 2009 年 12 月 2 日

[11] 授权公告号 CN 100565546C

[22] 申请日 2007.9.27

[21] 申请号 200710152342.5

[73] 专利权人 北京数字证书认证中心有限公司

地址 100029 北京市西城区裕民东路 3 号京版信息港二层

[72] 发明人 詹榜华 林雪焰 王新华 马臣云 冯承勇

[56] 参考文献

CN1350258A 2002.5.22

JP10 - 84341A 1998.3.31

CN1349179A 2002.5.15

CN1567340A 2005.1.19

审查员 刘莹莹

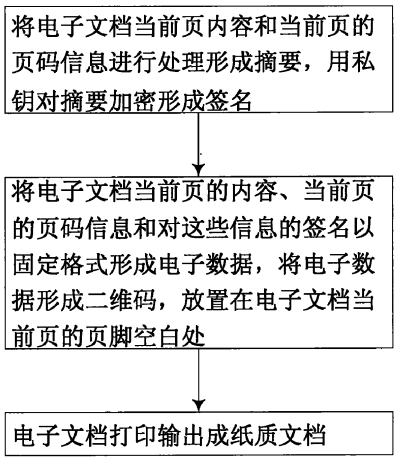
权利要求书 3 页 说明书 7 页 附图 4 页

[54] 发明名称

# 一种检验纸制文档内容是否被篡改的方法

[57] 摘要

本发明涉及数字签名和二维码技术，特别指使用数字签名和二维码技术实现一种检验纸制文档是否被篡改的方法。 本发明目的是将二维码与数字签名结合使用，提供一种检验纸制文档内容是否被篡改的方法，解决电子文档打印输出为纸制文档后文档内容真实性和有效性验证的问题。 本发明方法将电子文档当前页的内容、当前页的页码信息和页面内容签名以固定格式形成电子数据，将电子数据形成二维码，放置在电子文档当前页的页脚空白处，将电子文档打印输出为纸制文档。 采用本发明方法可以保证纸制文档内容的真实可靠，防止纸制文档内容被篡改后难以鉴别，并且通过这种机制能够确保文档拟定人对纸制文档内容的认可和不可否认。



1、一种检验纸制文档内容是否被篡改的方法，该方法包括：

（1）、电子文档的制作处理过程：I、将电子文档当前页内容和当前页的页码信息进行处理形成摘要，用私钥对摘要加密形成签名；II、将电子文档当前页的内容、当前页的页码信息和 I 中的签名以固定格式形成电子数据，将电子数据形成二维码，放置在电子文档当前页的页脚空白处；III、电子文档打印输出成纸制文档。

（2）、纸制文档内容是否被篡改进行验证过程：A、将纸制文档当前页扫描成图像格式，经过处理从图像二维码中保存的数据中获取当前页的内容、当前页页码信息和签名；B、将 A 中获取的当前页内容和当前页页码信息进行处理形成摘要 M；C、根据 A 中获取的签名中的私钥标识获取对应的公钥，使用公钥对 A 中获取的签名进行解密，得到摘要 M1；D、比较 M 和 M1；如果相同，则表示纸制文档当前页二维码中保存的数据没有被篡改过；E、将 A 中获取的当前页内容和当前页页码信息与纸制文档内容进行比对；如果相同，则表示纸制文档内容没有被篡改过，验证纸制文档通过。

2、根据权利要求 1 所述的检验纸制文档内容是否被篡改的方法，其特征在于，步骤（1）I中所述的将电子文档当前页内容和当前页的页码信息进行处理形成摘要，用私钥对摘要加密形成签名是指将电子文档当前页包含的文字内容和当前页的页码和该电子文档总页码信息作为输入，进行哈希运算，得到摘要信息，并使用数字证书中的签名私钥对摘要信息进行加密得到数字签名值。

3、根据权利要求 2 所述的检验纸制文档内容是否被篡改的方法，其特征在于，所述的数字证书是指存储在智能密码钥匙中用于加密和数字签名运算的数字证书，具有签名私钥不出密码钥匙的特点，可有效保护签名私钥的安全。

4、根据权利要求 1 所述的检验纸制文档内容是否被篡改的方法，其特征在

于，步骤（1）II中所述的将电子文档当前页的内容、当前页的页码信息和（1）I中的签名以固定格式形成电子数据是指，利用自定义的特有固定格式存储电子文档当前页的内容、当前页页码信息和文档总页码信息和（1）I中的签名。

5、根据权利要求 1 所述的检验纸制文档内容是否被篡改的方法，其特征在于，步骤（1）II中所述的将电子数据形成二维码，放置在电子文档当前页的页脚空白处是指利用二维码具有数据存储功能的特点，将电子数据转为二维码形式存储。

6、根据权利要求 5 所述的检验纸制文档内容是否被篡改的方法，其特征在于，所述的二维码是指 PDF417 码。

7、根据权利要求 1 所述的检验纸制文档内容是否被篡改的方法，其特征在于，步骤（2）A 中将纸制文档当前页扫描成图像格式，经过处理从图像二维码中保存的数据中获取当前页的内容、当前页页码信息和签名是指利用图像识别技术和二维码识别技术，将存储于二维码中的内容进行还原，从而分离出存储的当前页的内容，当前页的页码信息、文档总页码的信息和签名。

8、根据权利要求 1 所述的检验纸制文档内容是否被篡改的方法，其特征在于，步骤（2）B 中所述的将（2）A 中获取的当前页内容和当前页页码信息进行处理形成摘要 M 是指将还原的当前页文字内容、当前页页码信息和总页码信息作为输入，进行哈希运算，得到摘要信息。

9、根据权利要求 1 所述的检验纸制文档内容是否被篡改的方法，其特征在于，步骤（2）C 中所述根据（2）A 中获取的签名中的私钥标识获取对应的公钥是指从签名信息的数字证书中提取公钥信息。

10、根据权利要求 1 所述的检验纸制文档内容是否被篡改的方法，其特征在于，步骤（2）C 中所述使用公钥对（2）A 中获取的签名进行解密，得到摘要

M1 是指根据非对称密钥算法，使用私钥进行加密，使用该私钥对应的公钥也能够进行解密。

# 一种检验纸制文档内容是否被篡改的方法

## 技术领域

本发明涉及数字签名和二维码技术，特别指使用数字签名和二维码技术实现一种检验纸制文档是否被篡改的方法。

## 背景技术

对电子数据进行数字签名的技术已经很成熟，2005 年 4 月 1 日《中华人民共和国电子签名法》正式实施，对于经过签名的电子数据予以法律上的认可，并可作为法律证据使用。

现有方法中，尚没有一种可靠的方法对于电子文档打印输出纸制文档后的内容是否被篡改进行检验，从而对确认纸制文档内容的有效性带来了难度。二维码技术的发展，为电子数据向纸制文档的存储提供了一种途径，并可以实现电子数据基于纸制文档的大容量存储。

二维码是用某种特定的几何图形按一定规律在二维方向上分布的黑白相间的图形记录数据符号信息的；在代码编制上巧妙地利用构成计算机内部逻辑基础的“0”、“1”比特流的概念，使用若干个与二进制相对应的几何形体来表示文字数值信息，通过图像输入设备或光电扫描设备自动识读以实现信息自动处理。

二维码能够在横向和纵向两个方位同时表达信息，因此能在很小的面积内表达大量的信息。

在目前几十种二维码中，常用的码制有：PDF417 二维码、 Datamatrix 二维码、 Maxicode 二维码、QR Code 等等，二维码具有以下特点：

1．高密度编码，信息容量大：可容纳多达 1850 个大写字母或 2710 个数字或 1108 个字节，或 500 多个汉字，比普通条码信息容量约高几十倍。

2．编码范围广：该条码可以把图片、声音、文字、签字、指纹等可以数字化的信息进行编码，用条码表示出来；可以表示多种语言文字；可表示图像数据。

3．容错能力强，具有纠错功能：这使得二维条码因穿孔、污损等引起局部损坏时，照样可以正确得到识读，损毁面积达50%仍可恢复信息。

4．译码可靠性高：它比普通条码译码错误率百万分之二要低得多，误码率不超过千万分之一。

5．可引入加密措施：保密性、防伪性好。

6．成本低，易制作，持久耐用。

7．条码符号形状、尺寸大小比例可变。

8．二维条码可以使用激光或CCD阅读器识读。

## 发明内容

（一）要解决的技术问题

本发明目的是将二维码与数字签名结合使用，提供一种检验纸制文档内容是否被篡改的方法，解决电子文档打印输出为纸制文档后文档内容真实性和有效性验证的问题。

（二）技术方案

根据本发明的一个实施例，本发明提供了一种检验纸制文档内容是否被篡改的方法，该方法包括：

（1）、电子文档的制作处理过程：I、将电子文档当前页内容和当前页的页码信息进行处理形成摘要，用私钥对摘要加密形成签名；II、将电子文档当前页的内容、当前页的页码信息和I中的签名以固定格式形成电子数据，将电子数据形成二维码，放置在电子文档当前页的页脚空白处；III、电子文档打印输出成纸

制文档。

（2）、纸制文档内容是否被篡改进行验证过程：A、将纸制文档当前页扫描成图像格式，经过处理从图像二维码中保存的数据中获取当前页的内容、当前页页码信息和签名；B、将 A 中获取的当前页内容和当前页页码信息进行处理形成摘要 M；C、根据 A 中获取的签名中的私钥标识获取对应的公钥，使用公钥对 A 中获取的签名进行解密，得到摘要 M1；D、比较 M 和 M1；如果相同，则表示纸制文档当前页二维码中保存的数据没有被篡改过；E、将 A 中获取的当前页内容和当前页页码信息与纸制文档内容进行比对；如果相同，则表示纸制文档内容没有被篡改过，验证纸制文档通过。

（三）有益效果

从上述技术方案可以看出，本发明具有以下有益效果：

1、本发明提供的检验纸制文档内容是否被篡改的方法，利用基于公钥基础设施（Pubic Key Infrastructure，PKI）技术及第三方数字证书认证中心颁发的电子签名制作数据对文档内容等相关信息进行可靠电子签名，符合《中华人民共和国电子签名法》的要求，具有法律效力，而且能方便地作为司法诉讼中的证据使用，为建立纠纷解决、责任认定机制提供可靠的技术基础，化解目前存在的业务风险。

2、本发明提供的检验纸制文档内容是否被篡改的方法，让文档拟定人利用信息产业部许可的第三方数字证书认证中心颁发的电子签名制作数据（数字证书及签名密钥）对文档内容等相关信息进行数字签名，确保对二维码内容所作的任何修改，均能被检验出来；同时利用二维码数据存储技术存储文档内容，从而确保对文档内容的任何修改，也能被检验出来。

**附图说明**

图 1 是本发明所述电子文档制作处理流程图；

图 2 是本发明所述验证纸制文档是否被篡改流程图；

图 3 是本发明所述纸制文档生成业务流程示意图；

图 4 是本发明所述验证纸制文档是否被篡改业务流程示意图。

## 具体实施方式

为使本发明的目的、技术方案和优点更加清楚明白，以下结合具体实施例，并参照附图，对本发明进一步详细说明。

本发明的核心内容是：利用数字签名和二维码数据存储技术，将文档内容、页码信息和对这些信息的数字签名值，以二维码形式打印在纸制文档的页脚空白处，从而保证纸制文档内容的真实可靠，防止纸制文档内容被篡改后难以鉴别，并且确保文档拟定人对纸制文档的认可和不可否认。

如图 1、图 2 所示，图 1 为本发明提供的一种检验纸制文档内容是否被篡改的方法中的电子文档制作处理流程图，该方法包括以下步骤：

步骤 101：将电子文档当前页内容和当前页的页码信息进行处理形成摘要，用私钥对摘要加密形成签名；

步骤 102：将电子文档当前页的内容、当前页的页码信息和步骤 101 中的签名以固定格式形成电子数据，将电子数据形成二维码，放置在电子文档当前页的页脚空白处；

步骤 103：电子文档打印输出成纸制文档；

图 2 为本发明提供的一种检验纸制文档内容是否被篡改的方法中的纸制文档内容是否被篡改进行验证过程流程图，该方法包括以下步骤：

步骤 201：将纸制文档当前页扫描成图像格式，经过处理从图像二维码中保存的数据中获取当前页的内容、当前页页码信息和签名；

步骤 202：将步骤 201 中获取的当前页内容和当前页页码信息进行处理形成摘要 M；

步骤 203：根据步骤 201 中获取的签名中的私钥标识获取对应的公钥，使用公钥对步骤 201 中获取的签名进行解密，得到 M1；

步骤 204：比较 M 和 M1。如果相同，则表示纸制文档当前页二维码中保存的数据没有被篡改过；

步骤 205：将步骤 201 中获取的当前页内容和当前页页码信息与纸制文档对应页面内容进行比对。如果相同，则表示纸制文档内容没有被篡改过，验证纸制文档通过。

上述步骤 101 中所述将电子文档当前页内容和当前页的页码信息进行处理形成摘要，用私钥对摘要加密形成签名是指将电子文档当前页内容、当前页页码信息和文档总页码信息作为输入，进行哈希运算得到摘要信息；并利用智能 key 中存储的数字证书中的签名私钥对摘要信息进行数字签名；

上述步骤 102 中所述将电子文档当前页的内容、当前页的页码信息和步骤 101 中的签名以固定格式形成电子数据，将电子数据形成二维码，放置在电子文档当前页的页脚空白处是指将电子文档当前页的内容、当前页的页码信息、文档总页码的信息和签名值以自定义的固定数据存储格式并转换为 PDF417 码，输出在当页文档页脚空白处；

上述步骤 202 中所述将纸制文档当前页扫描成图像格式，经过处理从图像二维码中保存的数据中获取当前页的内容、当前页页码信息和签名是指使用二维码识读设备对二维码中存储的数据信息进行还原，从而可以分离出当前页的内容、页码信息和签名值；

上述步骤 202 中所述将步骤 201 中获取的当前页内容和当前页页码信息进行

处理形成摘要 M 是指将步骤 201 中还原的当前页内容、当前页页码信息和文档总页码信息作为输入进行哈希运算，从而得到摘要信息 M；

上述步骤 203 中所述根据步骤 201 中获取的签名中的私钥标识获取对应的公钥，使用公钥对步骤 201 中获取的签名进行解密，得到 M1 是指从签名信息中的数字证书中分离出签名私钥对应的公钥，并使用这个公钥对步骤 201 中获取的签名值进行解密，从而得到当前页文档内容、当前页页码信息和总页码信息的摘要信息 M1；

**实施例**

如图 3、图 4 所示为依照本发明实施例检验纸制文档内容是否被篡改的方法业务流程示意图，该方法包括以下步骤：

一、电子文档的制作处理过程

步骤 301：、将电子文档当前页内容和当前页的页码信息进行处理形成摘要；

步骤 302：用可靠第三方颁发的数字证书及私钥对步骤 301 中产生的摘要加密形成数字签名；

步骤 303：将电子文档当前页的内容、当前页的页码信息和步骤 301 中的签名以固定格式形成电子数据，将电子数据转换成 PDF417 二维码，放置在电子文档当前页的页脚空白处；

步骤 304：将电子文档打印输出为纸制文档。

二、纸制文档内容是否被篡改进行验证过程：

步骤 401：对纸制文档当前页中二维码进行识读，还原其中保存的当前页的内容、当前页页码信息和签名；

步骤 402：将步骤 401 中获取的当前页内容和当前页页码信息作为输入进行哈希运算，形成摘要信息 M；

步骤 403：根据步骤 401 中获取的签名信息中得到的公钥对步骤 401 中获取的签名进行解密，得到 M1；

步骤 404：比较 M 和 M1。如果相同，则表示纸制文档当前页二维码中保存的数据没有被篡改过；

步骤 405：将步骤 401 中获取的当前页内容和当前页页码信息与纸制文档内容进行比对。如果相同，则表示纸制文档内容没有被篡改过，验证纸制文档通过。

以上所述的具体实施例，对本发明的目的、技术方案和有益效果进行了进一步详细说明，所应理解的是，以上所述仅为本发明的具体实施例而已，并不用于限制本发明，凡在本发明的精神和原则之内，所做的任何修改、等同替换、改进等，均应包含在本发明的保护范围之内。

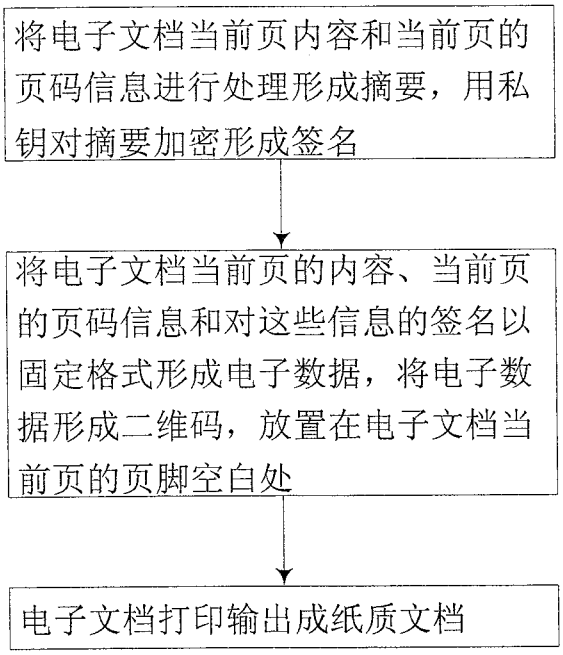

将电子文档当前页内容和当前页的页码信息进行处理形成摘要，用私钥对摘要加密形成签名
将电子文档当前页的内容、当前页的页码信息和对这些信息的签名以固定格式形成电子数据，将电子数据形成二维码，放置在电子文档当前页的页脚空白处
电子文档打印输出成纸质文档

图 1

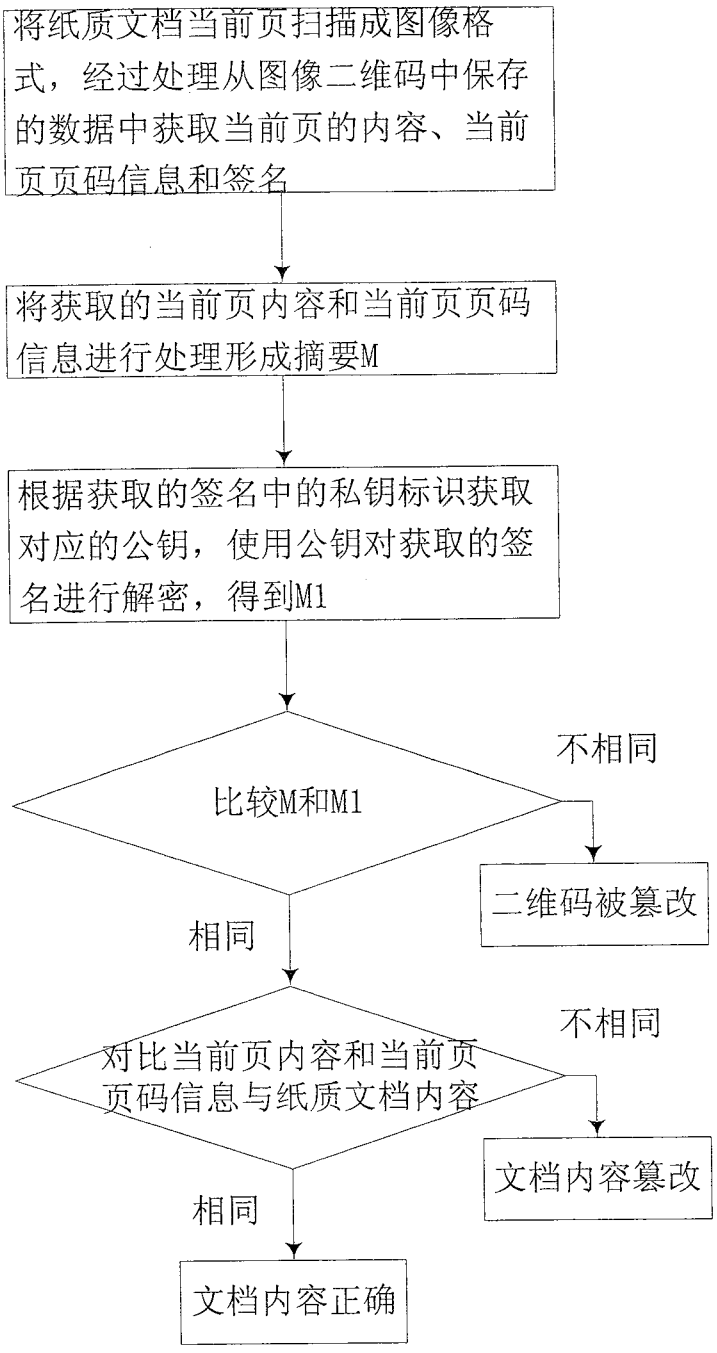

将纸质文档当前页扫描成图像格式，经过处理从图像二维码中保存的数据中获取当前页的内容、当前页页码信息和签名
将获取的当前页内容和当前页页码信息进行处理形成摘要M
根据获取的签名中的私钥标识获取对应的公钥，使用公钥对获取的签名进行解密，得到M1
比较M和M1
不相同
二维码被篡改
相同
对比当前页内容和当前页页码信息与纸质文档内容
不相同
文档内容篡改
相同
文档内容正确

图 2

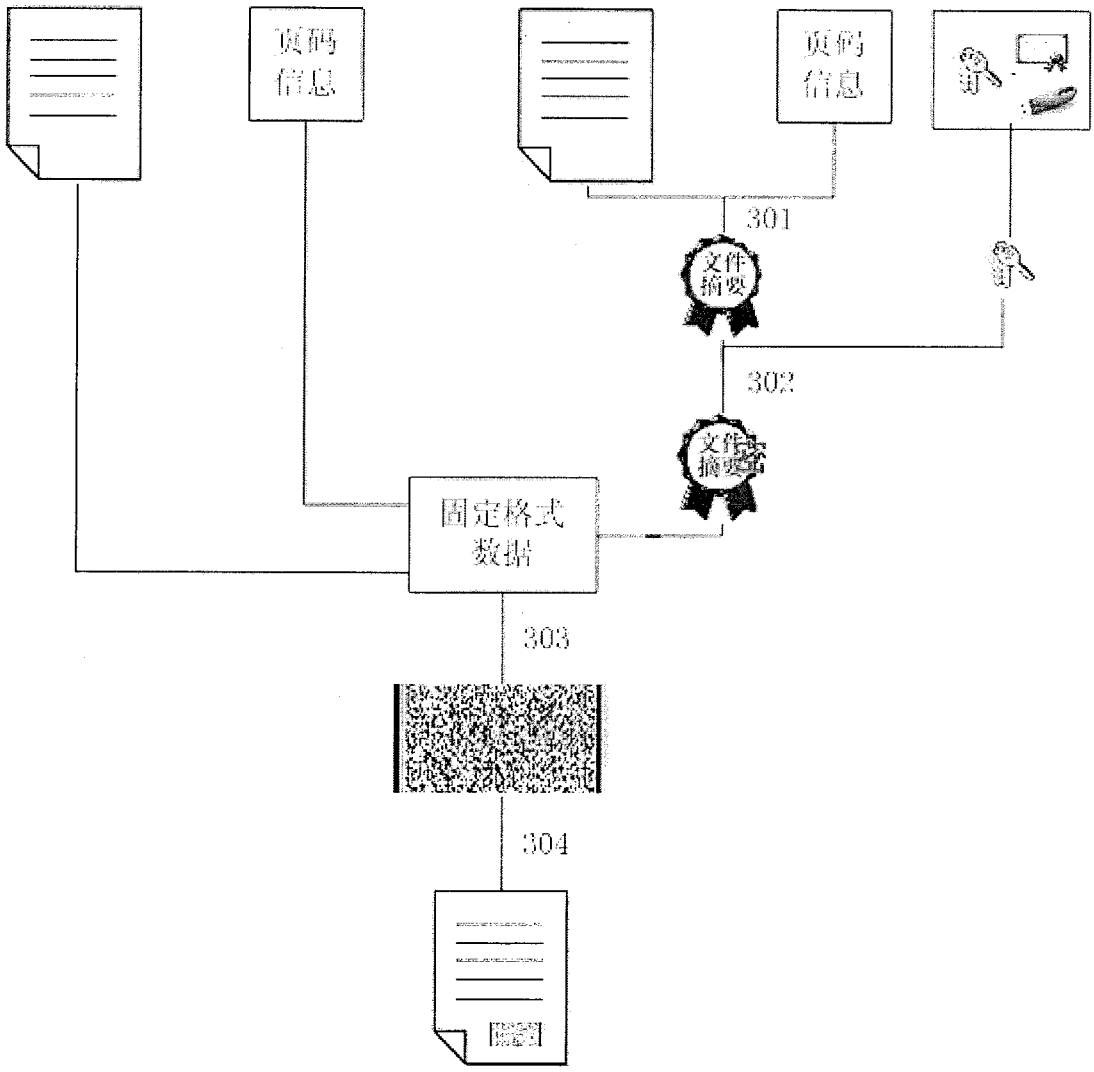



图 3

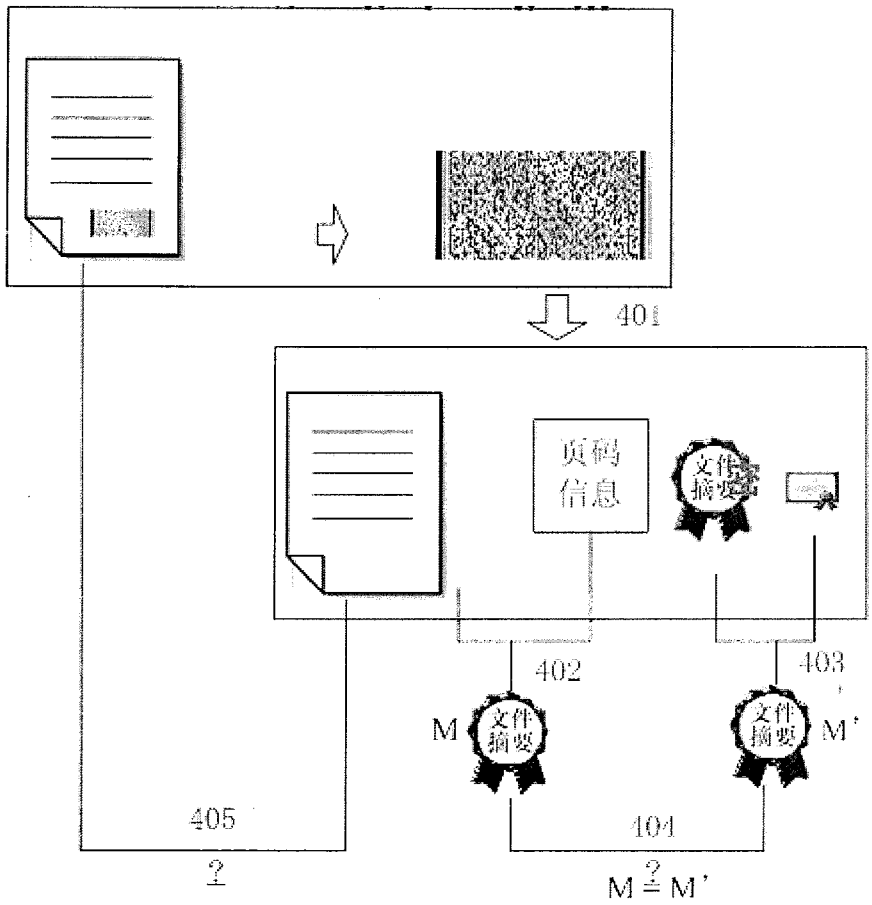



图 4