(19)国家知识产权局

(12)发明专利申请

(10)申请公布号 CN 117980902 A
(43)申请公布日 2024.05.03

(21)申请号 202280062404.6
(22)申请日 2022.03.02
(30)优先权数据
21197573.5 2021.09.17 EP
(85)PCT国际申请进入国家阶段日
2024.03.14
(86)PCT国际申请的申请数据
PCT/IB2022/051844 2022.03.02
(87)PCT国际申请的公布数据
WO2023/041989 EN 2023.03.23
(71)申请人 弗瑞普股份有限公司
地址 瑞士勒南
(72)发明人 D·乌鲁切克 G·盖琳
(74)专利代理机构 北京安信方达知识产权代理有限公司 11262
专利代理师 齐加文 杨明钊
(51)Int.Cl.
G06F 21/32(2006.01)
G06F 21/64(2006.01)
H04L 9/40(2006.01)
H04L 9/32(2006.01)
G09C 5/00(2006.01)

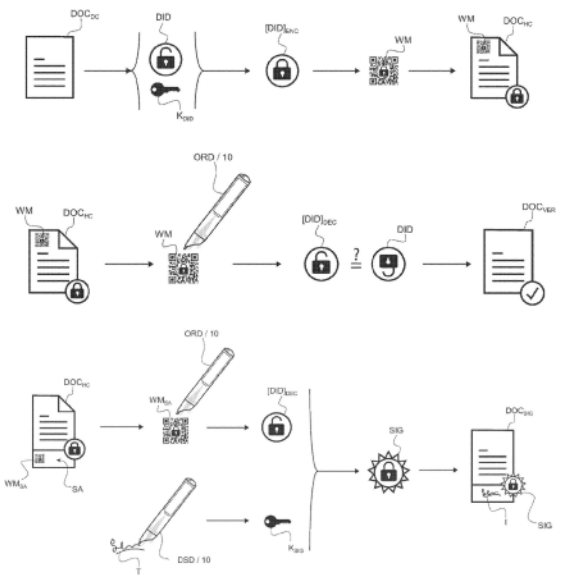
权利要求书2页 说明书9页 附图6页

(54)发明名称

签署文件的方法

(57)摘要

描述了一种签署文件的方法,其包括根据由至少一个签署者待签署的文件的数字拷贝(DOC_{DC})生成文件标识(DID),以及将该文件标识(DID)编码成一个或更多个水印(WM;WM_{SA};……)。产生结合了一个或更多个水印(WM;WM_{SA};……)的待签署的文件的硬拷贝(DOC_{HC})。使用光学读取器设备(ORD;10)读取在文件的硬拷贝(DOC_{HC})上设置的一个或更多个水印(WM;WM_{SA};……),并且对被编码成由光学读取器设备(ORD;10)读取的一个或更多个水印(WM;WM_{SA})的文件标识($[DID]_{ENC}$)进行解码。基于所解码的文件标识($[DID]_{DEC}$),将待签署的文件的硬拷贝(DOC_{HC})与待签署的文件的数字拷贝(DOC_{DC})相关联。使用数字签署设备(DSD;10)执行由至少一个签署者对文件的签署,以及使用数字签署设备(DSD;10)获得对于该至少一个签署者唯一的签署者信息(K_{SIG})。最后,基于解码的文件标识($[DID]_{DEC}$)和签署者信息(K_{SIG})生成文件的数字拷贝(DOC_{DC})的数字签名(SIG),之后将数字签名(SIG)应用于文件的数字拷贝(DOC_{DC})以产生文件的数字签署的拷贝(DOC_{SIG})。



CN 117980902 A

1.一种签署文件的方法,包括以下步骤:

(a)根据由至少一个签署者待签署的文件的数字拷贝(DOC_{DC})生成文件标识(DID);

(b)将所述文件标识(DID)编码成一个或更多个水印(WM;WM_{SA};WM_A);

(c)产生结合了所述一个或更多个水印(WM;WM_{SA};WM_A)的所述待签署的文件的硬拷贝(DOC_{HC});

(d)使用光学读取器设备(ORD;10)读取在所述文件的所述硬拷贝(DOC_{HC})上提供的所述一个或更多个水印(WM;WM_{SA};WM_A);

(e)对被编码成由所述光学读取器设备(ORD;10)读取的所述一个或更多个水印(WM;WM_{SA};WM_A)的文件标识($[DID]_{ENC}$)进行解码;

(f)基于所解码的文件标识($[DID]_{DEC}$),将所述待签署的文件的所述硬拷贝(DOC_{HC})与所述待签署的文件的所述数字拷贝(DOC_{DC})相关联;

(g)由所述至少一个签署者使用数字签署设备(DSD;10)来签署所述文件;

(h)使用所述数字签署设备(DSD;10)获得对于所述至少一个签署者唯一的签署者信息(K_{SIG});以及

(i)基于所述解码的文件标识($[DID]_{DEC}$)和所述签署者信息(K_{SIG})生成所述文件的所述数字拷贝(DOC_{DC})的数字签名(SIG),并将所述数字签名(SIG)应用于所述文件的所述数字拷贝(DOC_{DC})以产生所述文件的数字签署的拷贝(DOC_{SIG})。

2.根据权利要求1所述的方法,包括由多个签署者对所述文件的签署,

其中,由先前签署者签署的所述文件的所述数字签署的拷贝(DOC_{SIG})的数字签名(SIG)或其任何衍生物被用作文件标识(DID),以用于由至少一个其他签署者对所述文件的随后签署,或

其中,相同的文件标识(DID)用于由所有签署者进行签署的目的,并且所述文件的所述数字签署的拷贝(DOC_{SIG})的数字签名(SIG)基于所有签署者的级联签署者信息而生成。

3.根据权利要求1或2所述的方法,其中,所述光学读取设备(ORD)和所述数字签署设备(DSD)是同一个光学笔或触笔设备(10),所述光学笔或触笔设备(10)能够在步骤(d)读取所述一个或更多个水印(WM;WM_{SA};WM_A),并且能够通过提取对于在步骤(g)执行的所述至少一个签署者的签名唯一的生物识别信息而在步骤(h)获得所述签署者信息(K_{SIG})。

4.根据权利要求3所述的方法,其中,在所述文件的所述硬拷贝(DOC_{HC})上执行在步骤(g)的对所述文件的签署,并且其中,所述光学笔或触笔设备(10)还能够在所述文件的所述硬拷贝(DOC_{HC})上留下在步骤(g)执行的所述签署者的签名的墨迹(T),和/或

其中,在步骤(g)执行的所述签署者的签名的数字图像(I)被应用到所述文件的所述数字签署的拷贝(DOC_{SIG})。

5.根据权利要求3或4所述的方法,其中,所述文件的所述硬拷贝(DOC_{HC})的表面进一步被设置有位置编码图案(PEP),所述位置编码图案(PEP)被设计成允许所述光学笔或触笔设备(10)相对于所述文件的所述硬拷贝(DOC_{HC})的表面的位置确定,

并且其中,所述光学笔或触笔设备(10)还被配置为基于对所述位置编码图案(PEP)的光学检测,执行所述光学笔或触笔设备(10)相对于所述文件的所述硬拷贝(DOC_{HC})的表面的位置确定。

6.根据权利要求5所述的方法,其中,所述位置编码图案(PEP)与步骤(c)的所述文件的

所述硬拷贝(DOC_{HC})一起打印,或者被提供在用于打印步骤(c)的所述文件的所述硬拷贝(DOC_{HC})的空白纸上。

7.根据权利要求1或2所述的方法,其中,所述数字签署设备(DSD)是用户认证设备,例如PIN保护设备、智能卡读卡器设备或生物识别设备,特别包括指纹识别设备、手写识别设备(10)、语音识别设备、视网膜识别设备或面部识别设备。

8.根据前述权利要求中任一项所述的方法,其中,所述一个或更多个水印是或包括在所述文件的所述硬拷贝(DOC_{HC})的签署区(SA)中提供的签署区水印(WM_{SA})。

9.根据权利要求3至6中任一项所述的方法,其中,所述一个或更多个水印是或包括在所述文件的所述硬拷贝(DOC_{HC})的签署区(SA)中提供的签署区水印(WM_{SA}),

并且其中,使用所述光学笔或触笔设备(10)同时执行在步骤(d)的读取所述签署区水印(WM_{SA})和在步骤(h)的获得所述签署者信息(K_{SIG})。

10.根据权利要求8或9所述的方法,其中,一个或更多个敏感区水印(WM_A)被进一步提供在所述文件的所述硬拷贝(DOC_{HC})的一个或更多个敏感区(A)中。

11.根据前述权利要求中任一项所述的方法,其中,每个水印(WM;WM_{SA};WM_A)是位置相关的,以防止所述水印(WM;WM_{SA};WM_A)在所述文件的所述硬拷贝(DOC_{HC})的其他区中的复制。

12.根据前述权利要求中任一项所述的方法,其中,所述一个或更多个水印(WM;WM_{SA};WM_A)中的任一个通过墨水被打印在所述文件的所述硬拷贝(DOC_{HC})上,所述墨水是肉眼不可见但借助于所述光学读取器设备(ORD;10)可检测的,诸如近红外(NIR)墨水。

13.根据前述权利要求中任一项所述的方法,其中,步骤(f)包括基于解码的文件标识($[DID]_{ENC}$)检查所述待签署的文件的真实性。

14.根据前述权利要求中任一项所述的方法,其中,所述文件标识(DID)基于密码散列函数或从密码散列函数导出。

15.根据前述权利要求中任一项所述的方法,其中,步骤(h)包括获得对于所述至少一个签署者唯一的私有加密密钥(K_{SIG})。

签署文件的方法

技术领域

[0001] 本发明总体上涉及签署文件的方法,且更具体地涉及这样一种方法,该方法允许纸质世界和数字世界的桥接(bridge)以确保文件的可靠且稳定的签署。

背景技术

[0002] 国际(PCT)公开第WO 2018/211475A1号公开了一种对文件进行签署和认证的方法,该方法将文件的数字签名(使用诸如SHA-256的典型散列函数)与签署者的生物识别签名(biometric signature)相结合。更具体地,所提出的方法包括:

[0003] a)创建要用签署设备控制器签署的数字文件(例如但不限于pdf文件)的第一散列;

[0004] b)将适用于视觉显示文件的数据集和第一散列转发到签署设备;

[0005] c)利用签署设备向签署者显示文件的图像;

[0006] d)利用签署设备记录签署者的生物识别签名;

[0007] e)利用签署设备提取签署者的生物识别标识符;

[0008] f)利用签署设备对生物识别标识符进行加密;

[0009] g)利用签署设备从加密的生物识别标识符创建第二散列;

[0010] h)使用签署设备级联第一散列和第二散列,并创建级联散列(concatenated hash);

[0011] i)使用签署设备,利用存储在该签署设备中的密码签署密钥来签署该级联散列,由此创建签署的级联散列;

[0012] j)将加密的生物识别标识符和签署的级联散列转发到签署设备控制器;以及

[0013] k)级联该文件、加密的生物识别标识符和签署的级联散列以创建签署的文件。

[0014] 根据WO 2018/211475A1,签署设备可以是任何合适的签署设备,包括例如由signotec公司销售的具有集成显示器的签名板(signature pad)。

[0015] 虽然WO 2018/211475A1的方法提供了增加的安全级别,因为文件的签署将文件本身的数字签名和关联于签署者的生物识别签名相结合,但是该方法具有某些实际限制,最显著的事实是,签署方法本质上发生在完全数字化、无纸化的世界中,并且因此没有提供允许纸质世界和数字世界的有效桥接的任何解决方案,请记住人们仍然十分专注于尽可能以纸质形式签署文件的愿望。

[0016] 美国专利第US 7,024,562B1号公开了一种用于执行安全数字签署的方法和系统,该方法和系统同样结合了生物识别标识符和从散列函数导出的文件的数字印章的使用。该解决方案实际上遭受与上文结合WO 2018/211475A1的方法所讨论的相同限制。

[0017] 美国专利第US 6,081,610A号公开了一种用于验证诸如支票和宣誓书的文件上的签名的系统和方法。最初,要获得经验证的签名的客户在某个时间点向签署者机构注册,并且为该客户唯一地建立具有公共部分和私有部分的秘密密钥。当文件需要经验证的签名时,客户向签名系统出示文件和他/她的身份证明,诸如预编程的计算机接口卡。该系统访

问客户密钥的私有部分的档案,并部分地基于文件的内容生成经编码的签名。因此,当文件的接收者稍后希望验证签名时,接收者使用客户的公钥来解码签名。然后可以针对文件的内容来验证签名。根据US 6,081,610A,优选地通过将签名直接打印到文件的硬拷贝上,将如此生成的签名与文件相关联。

[0018] 有些类似的解决方案在美国专利公开第US2006/0265590A1号和第US2006/0271787A1号中公开。在这种情况下,要进行数字签署的文件被输入到安全散列函数中,以产生压缩版本(或散列)。生成文件的数字签名,然后诸如通过打印将数字签名的物理表现(physical manifestation)(诸如2D条形码)附到文件的硬拷贝上。然后可以使用扫描仪或类似的光学读取器设备来读取数字签名的物理表现,以便被解密并允许验证文件的真实性。

[0019] 在国际(PCT)公开第WO 01/15382A1号中公开了又一种类似的解决方案。

[0020] 虽然在US 6,081,610A、US2006/0265590A1、US2006/0271787A1和WO 01/15382A1中公开的解决方案考虑了桥接纸质世界和数字世界,但是签署过程本身仍然仅发生在数字世界中,并且这些解决方案仅仅考虑为了验证和认证的目的将相关数字签名的物理表现附在文件的硬拷贝上。

[0021] 因此,仍然存在对改进的解决方案的需要。

[0022] 发明概述

[0023] 本发明的总体目的是提供一种签署文件的方法,该方法消除了已知解决方案的限制和约束。

[0024] 更具体地,本发明的目的是提供这样一种解决方案,其有效且可靠地桥接纸质世界和数字世界。

[0025] 本发明的又一个目的是提供这样一种解决方案,其实际上允许任意数量的签署者签署任何给定的文件,并且这绝对可以确定的是,以硬拷贝形式提交的用于签署的文件是正确的文件。

[0026] 本发明的另一个目的是提供这样一种解决方案,其有效地结合了文件本身的数字签署和对于签署该文件的每个签署者唯一的信息。

[0027] 本发明的再一个目的是提供这样一种解决方案,其优选地允许以尽可能自然且不会让人吃惊的方式将签署过程付诸实践。

[0028] 由于权利要求中限定的解决方案,这些目的以及其他目的得以实现。

[0029] 因此,提供了一种签署文件的方法,其特征在权利要求1中记载,即签署文件的方法包括以下步骤:

[0030] (a)根据由至少一个签署者待签署的文件的数字拷贝生成文件标识(document identification);

[0031] (b)将文件标识编码成一个或更多个水印;

[0032] (c)产生结合了一个或更多个水印的待签署文件的硬拷贝;

[0033] (d)使用光学读取器设备读取在文件的硬拷贝上提供的一个或更多个水印;

[0034] (e)对被编码成由光学读取器设备读取的一个或更多个水印的文件标识进行解码;

[0035] (f)基于所解码的文件标识,将待签署文件的硬拷贝与待签署文件的数字拷贝相

关联;

[0036] (g)由至少一个签署者使用数字签署设备来签署文件;

[0037] (h)使用数字签署设备获得对于至少一个签署者唯一的签署者信息;和

[0038] (i)基于所解码的文件标识和签署者信息生成文件的数字拷贝的数字签名,并将该数字签名应用于文件的数字拷贝以产生文件的数字签署的拷贝。

[0039] 根据实施例,该方法包括由多个签署者对文件进行签署,并且由先前签署者签署的文件的数字签署的拷贝的数字签名或其任何衍生物被用作文件标识,以用于由至少一个其他签署者对该文件的随后签署。替代地,相同的文件标识可以用于由所有签署者进行签署的目的,并且文件的数字签署的拷贝的数字签名可以基于所有签署者的级联签署者信息而生成。

[0040] 根据特别优选的实施例,光学读取器设备和数字签署设备是同一个光学笔或触笔设备,该光学笔或触笔设备能够在步骤(d)读取一个或更多个水印,并且通过提取对于在步骤(g)执行的至少一个签署者的签名唯一的生物识别信息而在步骤(h)获得签署者信息。

[0041] 在后一种优选的上下文中,在步骤(g)对文件的签署可以特别地在文件的硬拷贝上进行,并且光学笔或触笔设备可以进一步在文件的硬拷贝上留下在步骤(g)执行的签署者的签名的墨迹。附加地或替代地,在步骤(g)执行的签署者的签名的数字图像可以被应用到文件的数字签署的拷贝上。

[0042] 实际上,人们将认识到,在步骤(g)对文件的签署优选且有利地直接发生在文件的硬拷贝上,但是替代地其他实施例可以提供文件的数字拷贝的签名。

[0043] 优选地,文件的硬拷贝的表面可以进一步设置有位置编码图案,该位置编码图案被设计成允许光学笔或触笔设备相对于文件的硬拷贝的表面进行位置确定,在这种情况下,光学笔或触笔设备还被配置成基于对所述位置编码图案的光学检测来执行光学笔或触笔设备相对于文件的硬拷贝的表面的位置确定。这些位置编码图案可以在步骤(c)与文件的硬拷贝一起打印,或者在步骤(c)被提供在用于打印文件的硬拷贝的空白纸上。

[0044] 根据本发明的实施例,数字签署设备可以是用户认证设备,诸如PIN保护设备、智能卡读卡器设备或生物识别设备。生物识别设备特别可以是指纹识别设备、手写识别设备、语音识别设备、视网膜识别设备或面部识别设备,所有这些都适合于执行步骤(g)和(h)。然而,使用光学笔或触笔设备作为光学读取器设备和数字签署设备仍然是优选的和特别有利的实施例。

[0045] 一个或更多个水印优选地是或包括在文件的硬拷贝的签署区中提供的签署区水印。特别地,在这种情况下,在步骤(d)读取签署区水印和在步骤(h)获得签署者信息可以有利地使用前述光学笔或触笔设备来同时执行。

[0046] 此外,还可以在文件的硬拷贝的一个或更多个敏感区中提供一个或更多个敏感区水印。

[0047] 优选地,每个水印是位置相关的(即,对与文件上每个水印的实际位置相关的附加信息进行编码),以防止水印在文件的硬拷贝的其他区中的复制。

[0048] 一个或更多个水印中的任何一个可以有利地借助于诸如近红外(NIR)墨水的墨水打印在文件的硬拷贝上,该墨水是肉眼不可见的但是借助于光学读取器设备是可检测的。以此方式,水印不会以任何方式在视觉上干扰在待签署文件上提供的信息。

[0049] 上面提到的步骤(f)可以特别包括基于解码的文件标识来检查待签署文件的真实性,从而提供进一步的验证步骤,确保呈现给相关签署者进行签署的文件的硬拷贝确实对应于没有以任何方式被篡改的真实文件(authentic document)。

[0050] 文件标识尤其可以基于密码散列函数或从密码散列函数导出。

[0051] 此外,步骤(h)优选地包括获得对于至少一个签署者唯一的私有加密密钥,从而提供增强的安全性,因为相关加密密钥仅由签署文件的相关签署者可访问。

[0052] 下面讨论本发明的进一步的有利的实施例。

[0053] 附图简述

[0054] 通过阅读本发明实施例的以下详细描述,本发明的其他特征和优点将更清楚地显现,这些实施例仅通过非限制性示例呈现,并由附图示出,其中:

[0055] 图1是本发明旨在实现的基本原理的示意图,即桥接纸质世界和数字世界以确保文件的可靠且稳定的签署;

[0056] 图2是示出根据本发明实施例执行的步骤的示意图,目的是将文件标识编码成水印,该水印旨在应用到待签署文件的硬拷贝上;

[0057] 图3是示出根据本发明实施例执行的步骤的示意图,目的是读取并验证待签署文件的硬拷贝的真实性;

[0058] 图4是示出根据本发明实施例执行的步骤的示意图,目的是签署文件并生成对应的数字签名;

[0059] 图5是根据本发明特别优选的实施例的光学笔或触笔设备的示意图,该光学笔或触笔设备用作用于读取应用在待签署文件的硬拷贝上的水印的光学读取器设备,并且用作用于签署文件的数字签署设备;和

[0060] 图6是提供有多个水印的文件的硬拷贝的示意图,该多个水印包括在签署区中提供的水印和在文件的不同的敏感区中提供的水印。

[0061] 发明的具体实施方式

[0062] 将结合多种说明性实施例来描述本发明。应当理解,本发明的范围涵盖本文公开的实施例的特征的所有组合和子组合。

[0063] 下文将在使用光学笔或触笔设备作为光学读取器设备和数字签署设备两者的特定和优选上下文中特别描述本发明的方法的实施例,但是将认识到,本发明的方法不限于这种用途。实际上,如下文将描述的,本发明的方法可以使用例如不同且分离的光学读取器和数字签署设备来实现。

[0064] 在2020年9月28日以本申请人的名义发布的、标题为“Optical stylus for optical position determination device”的欧洲专利申请第20198791.4号中公开了一种光学笔或触笔设备,该光学笔或触笔设备在图3、图4和图5中示意性示出,在整体上用参考数字10表示,特别适用于本发明的上下文,该专利申请的内容通过引用以其整体并入本文。

[0065] 这里不会给出相关光学笔/触笔设备10的详细描述,因为这种详细描述已经在前述欧洲专利申请中提供。可以理解的是,光学笔/触笔设备10既能够读取在待签署文件的硬拷贝上提供的水印(如下所解释),又能够提取签署者的生物识别签名,即,在签署期间使用光学笔/触笔设备10检测和表征签署者进行的移动。更具体地,光学笔/触笔设备10包括能

够读取水印的光学传感器装置(和相关联的处理装置)。优选地,光学笔/触笔设备10还被配置成基于对在文件的硬拷贝的表面上提供的位置编码图案PEP的光学检测,执行光学笔/触笔设备10相对于待签署文件的硬拷贝的表面的位置确定(参见图5)。也就是说,可以提供其他替代或补充装置来允许笔/触笔设备10的位置确定,包括例如一个或更多个辅助传感器,诸如加速度计、陀螺仪、磁力计、飞行时间传感器、接近度传感器等。还可以考虑其他参数,诸如签署者在签署期间施加的可变压力、笔/触笔的倾斜度和其他定向特征、签署期间速度和加速度的变化等。实际上,这些辅助传感器不仅可以用于光学笔/触笔设备10的位置确定,还可以用于在签署过程中提取签署者特定特征,这些独特的特征最终有助于认证签署者。

[0066] 图1是本发明旨在实现的基本原理的示意图,即桥接纸质世界和数字世界以确保文件的可靠且稳定的签署。更具体地,本发明的方法依赖于使用待签署文件的硬拷贝(标示为DOC_{HC})和待签署文件的数字拷贝(标示为DOC_{DC}),以在签署过程完成之后产生文件的数字签署的拷贝(标示为DOC_{SIG})。应用于文件的数字签署的拷贝DOC_{SIG}的数字签名SIG在本文中也将被称为“生物识别-数字签名(biometric-digital signature)”,因为它优选地基于文件的数字签名和对于签署文件的签署者唯一的生物识别签名。

[0067] 从一般的角度来看,本发明的方法包括执行以下基本步骤,即:

[0068] (a)根据由至少一个签署者待签署的文件的数字拷贝DOC_{DC}生成文件标识(下文标示为DID);

[0069] (b)将文件标识编码为一个或更多个水印(下文标示为WM、WM_{SA}和/或WM_{A});

[0070] (c)产生结合了一个或更多个水印的待签署文件的硬拷贝DOC_{HC};

[0071] (d)使用光学读取器设备(标示为ORD)读取在文件的硬拷贝DOC_{HC}上提供的一个或更多个水印;

[0072] (e)对被编码成由光学读取器设备ORD读取的一个或更多个水印的文件标识进行解码;

[0073] (f)基于所解码的文件标识,将待签署文件的硬拷贝DOC_{HC}与待签署文件的数字拷贝DOC_{DC}相关联;

[0074] (g)由至少一个签署者使用数字签署设备(标示为DSD)来签署文件;

[0075] (h)使用数字签署设备DSD获得对于至少一个签署者唯一的签署者信息;和

[0076] (i)基于所解码的文件标识和签署者信息生成文件的数字拷贝DOC_{DC}的数字签名(标示为SIG),并将该数字签名SIG应用于文件的数字拷贝DOC_{DC}以产生文件的数字签署的拷贝DOC_{SIG}。

[0077] 该方法可以由一个或更多个签署者执行。如果该方法涉及由多个签署者对文件进行签署,则特别有利的是使用由先前签署者签署的文件的数字签署的拷贝DOC_{SIG}的数字签名SIG(或其任何衍生物)作为文件标识DID,以用于由至少一个其他签署者对文件进行后续签署。替代地,相同的文件标识DID可以用于由所有签署者进行签署的目的,并且文件的数字签署的拷贝DOC_{SIG}的数字签名SIG可以基于所有签署者的级联签署者信息而生成。

[0078] 换句话说,在涉及一个或多个签署者的最简单情况下,文件标识可以例如是通过将典型散列函数应用于待签署文件而获得的文件散列(该散列可以使用如本领域已知的任何合适的加密密钥对的公共部分和私有部分来被加密和解密)。在涉及多个签署者的另一

种情况下,文件标识可以基于待签署文件的先前签署版本的数字签名SIG,应当理解,数字签名SIG本身适当且可靠地标识由其他签署者待签署的文件。

[0079] 图2是示出根据本发明实施例执行的步骤的示意图,目的是将文件标识(标示为DID)编码成水印(标示为WM),该水印旨在应用到待签署文件的硬拷贝DOC_{HC}上。换句话说,图2示出了上面讨论的步骤(a)至(c)的实施例。

[0080] 正如已经提到的,适合的文件标识DID可以是通过将散列函数应用于待签署文件的数字拷贝DOC_{DC}而产生的散列。该散列可以使用适合的加密密钥K_{DID}进行加密,如本领域已知的那样。加密的文件标识(标示为$[DID]_{ENC}$)然后可以被编码成对应的水印WM,例如采用合适的2D条形码的形式,该2D条形码然后可以被应用到待签署文件的硬拷贝DOC_{HC}的任何期望部分上。实际上,多于一个水印可以被生成并被应用到待签署文件的硬拷贝DOC_{HC}上。

[0081] 在待签署文件的硬拷贝DOC_{HC}上应用相关水印后,这种水印可以被利用以确保将文件的硬拷贝DOC_{HC}移交给其以用于签署的任何签署者可以在对文件的签署之前适当地检查该文件。如稍后将解释的,在文件的硬拷贝DOC_{HC}的一个或更多个敏感区中可以进一步提供一个或更多个水印。这些水印可以特别是位置相关的,即对与文件上每个水印的相关位置相关的进一步信息进行编码。

[0082] 图3是示出根据本发明实施例执行的步骤的示意图,目的是读取并验证待签署文件的硬拷贝DOC_{HC}的真实性。换句话说,图3示出了上面讨论的步骤(d)至(f)的实施例。

[0083] 读取应用到文件的硬拷贝DOC_{HC}上的、包括例如图3所示的水印WM的一个或更多个水印可以借助于任何合适的光学读取器设备ORD(包括例如扫描仪)来执行。优选地,水印的读取借助于前述光学笔/触笔设备10来执行。被编码成水印WM的相关文件标识然后可以被解码,产生解密的文件标识$[DID]_{DEC}$,并与文件的对应数字拷贝DOC_{DC}的文件标识DID进行比较以确保文件的硬拷贝被正确地识别和验证(如图3中由文件的经验证的拷贝(标示为DOC_{VER})所描绘的)。待签署文件的对应数字拷贝DOC_{DC}可以存储在任何合适的文件库中。实际上,执行对文件真实性的验证可以迟于(beyond)对文件的硬拷贝DOC_{HC}的识别和将该硬拷贝DOC_{HC}与其数字对应物相关联。

[0084] 一旦待签署文件被成功验证并视情况可以被认证,则该方法可以进一步进行对文件的实际签署。还可以通过在文件的敏感区中提供专用水印来考虑对待签署文件的特别敏感部分的验证。

[0085] 签署者对文件的签署是借助于合适的数字签署设备DSD来执行的,该设备允许获得对于相关签署者唯一的签署者信息。在一个实施例中,数字签署设备DSD可以是用户认证设备,诸如PIN保护设备或智能卡读卡器设备,在这种情况下,签署者需要拥有合适的智能卡,该智能卡持有例如对于签署者唯一的加密证书。在其他实施例中,数字签署设备DSD可以是生物识别设备,诸如指纹识别设备、手写识别设备、语音识别设备、视网膜识别设备或面部识别设备。人们将认识到,数字签署设备DSD的基本目的是借助于任何合适的认证方法(包括生物统计学)来验证签署者的身份。上述光学笔/触笔设备10实际上构成可用作数字签署设备DSD的合适的手写识别设备的一个可能示例。

[0086] 图4是示出根据本发明实施例执行的步骤的示意图,目的是签署文件并生成其对应的数字签名。换句话说,图4示出了上面讨论的步骤(g)至(i)的实施例。

[0087] 在该说明性示例中,待签署文件的硬拷贝DOC_{HC}优选地提供有至少一个水印(标示

为WM_{SA}),在文件的签署区SA中提供该水印,水印WM_{SA}同样是基于待签署文件的合适文件标识而生成的。如果需要,可以提供进一步的水印,特别是为了检查待签署文件的敏感区。

[0088] 优选地,前述光学笔/触笔设备10不仅用于签署文件和获得相关的签署者信息(即,用作数字签署设备DSD),而且还用作用于读取水印WM_{SA}的光学读取器设备ORD。换句话说,读取水印WM_{SA}(例如为了验证文件的真实性)和获得签署者信息在这里有利地使用同一个光学笔/触笔设备10来同时执行。在其他实施例中,光学笔/触笔设备10可以专门用作数字签署设备DSD,并且可以借助于能够读取应用在待签署文件的硬拷贝DOC_{HC}上的相关水印的单独的光学读取器设备ORD来进行文件验证。

[0089] 在说明性示例中,对被编码成水印WM_{SA}的文件标识进行解码,并且提取对于签署者的签名唯一的生物标识信息以获得相关的签署者信息。更具体地,在说明性示例中,获得对于至少一个签署者唯一的私有加密密钥K_{SIG}。该私有加密密钥K_{SIG}仅由相关签署者基于签署者的签名的相关生物识别特征可访问。换句话说,所需的加密密钥K_{SIG}只有在签署者的签名的生物识别特征与签署者的预先存在的生物识别签名一致的情况下,才能被访问。在其他实施例中,私有加密密钥K_{SIG}可以由其他用户认证装置访问,这取决于所采用的数字签署设备DSD的特定性质。

[0090] 所解码的文件标识$[DID]_{DEC}$以及对于签署者唯一的相关加密密钥K_{SIG}用于生成文件的数字拷贝DOC_{DC}的数字签名(或“生物识别-数字签名”)SIG,该数字签名SIG可以应用于文件的数字拷贝DOC_{DC}以产生文件的数字签署的拷贝DOC_{SIG},从而完成数字签署过程。在所示的实施例中,通过使用私有加密密钥K_{SIG}以及应用如本领域已知的任何适合的加密技术对文件标识DID进行加密来产生相关的生物识别-数字签名SIG。

[0091] 因此,人们将认识到,相关的数字签名SIG不仅适当地标识正在签署的文件,而且还标识签署该文件的签署者(或多个签署者)的身份。

[0092] 实际上,本发明的方法的步骤(g)至(i)共同构成了与例如在前文中讨论的US 6,081,610A、US2006/0265590A1、US2006/0271787A1和WO 01/15382A1中公开的已知解决方案的关键区别,因为最终应用于文件的数字拷贝DOC_{DC}以产生数字签署的拷贝DOC_{SIG}的数字签名SIG不是完全基于文件本身生成的,而是基于如借助于数字签署设备DSD获得的、对于签署者唯一的签署者信息K_{SIG}生成的。这导致了纸质世界和数字世界之间特别稳定且有效的桥接。

[0093] 优选地,直接在文件的硬拷贝DOC_{HC}上执行文件的签署,并且光学笔/触笔设备10还被配置为能够在文件的硬拷贝DOC_{HC}上留下签署者的签名的墨迹(标示为T),就像一支普通的笔。

[0094] 附加地或替代地,可以将签署者的签名的数字图像(标示为I)应用到文件的数字签署的拷贝DOC_{SIG}上。在该上下文中,前述光学笔/触笔10可以充当能够将手写内容转换成期望的数字图像I的手写数字化器(handwriting digitizer)。

[0095] 如上所述且如图5示意性示出的,文件的硬拷贝DOC_{HC}的表面可以设置有位置编码图案PEP,该位置编码图案PEP被设计成允许光学笔/触笔设备10相对于文件的硬拷贝DOC_{HC}的表面的位置确定(如例如在以本申请人的名义在2020年9月28日发布的欧洲专利申请第20198791.4号中公开的)。在这种情况下,光学笔/触笔设备10还被配置为基于对所述位置编码图案PEP的光学检测,执行光学笔/触笔设备10相对于文件的硬拷贝DOC_{HC}的表面的位置

确定。位置编码图案PEP可以与待签署文件的硬拷贝DOC_{HC}一起打印或提供在用于打印待签署文件的硬拷贝DOC_{HC}的空白纸上。

[0096] 如前所述,可以在待签署文件的硬拷贝上提供多于一个水印,以不仅检查文件的身份和真实性,而且如果需要,还可以确保待签署文件的其他特定区(例如,包括日期、财务要素等)作为签署过程的一部分被适当地检查或审查,诸如文件的特别敏感区。图6示意性地示出了文件的硬拷贝DOC_{HC},其设置有在抬头部分中的第一水印WM,在签署区SA中的签署区水印WM_{SA}以及在文件的敏感区A中的另一水印WM_{A}。

[0097] 作为进一步的改进,在待签署文件的硬拷贝DOC_{HC}上应用的每个水印可以是位置相关的,即可以对与文件上的每个水印的实际位置相关的附加信息进行编码,以防止水印在文件的硬拷贝DOC_{HC}的其他区中的复制。在这种情况下,如果发现相关水印定位在与编码在水印中的位置不同的位置处,这将指示文件篡改,即使发现正确的文件标识DID被编码在相关水印中,该签署过程也可以中断。

[0098] 此外,相关水印中的任一个都可以借助于墨水打印在文件的硬拷贝DOC_{HC}上,该墨水肉眼不可见但借助于光学读取器设备ORD可检测。特别地,每个水印可以用借助于光学笔/触笔设备10可检测的近红外(NIR)墨水打印。对于前述位置编码图案PEP的提供也可以考虑同样的情况,然而优选的是在这种情况下避免相关水印和位置编码图案PEP之间的任何可能的光学干扰,例如通过使用不同的墨水。

[0099] 在不脱离由所附权利要求限定的本发明范围的情况下,可以对上述实施例进行各种修改和/或改进。

[0100] 例如,如前所述,不同的设备可以用作光学读取器设备ORD和用作数字签署设备DSD。然而,使用光学笔/触笔设备作为光学读取器设备ORD和数字签署设备DSD仍然是特别优选和有利的解决方案。

[0101] 此外,虽然图4示出了文件的签署是直接在待签署文件的硬拷贝DOC_{HC}上执行的,但是替代地其他实施例可以考虑例如通过在可能提供签署区的可视描述的数字平板设备上签署文件来对数字拷贝DOC_{DC}进行签署。在其他实施例中,由数字签署设备DSD进行的成功用户认证可以被认为指示由相关签署者签署相关文件的适当意图,而不需要文件的实际手写签署。例如,如果通过例如指纹或面部识别来认证签署者的身份,则可能是这种情况。但是,签署文件的硬拷贝DOC_{HC}仍然是优选的解决方案,因为它更普遍地被公众接受,并且在这方面更自然。

[0102] 本文使用的参考数字和符号的列表

[0103] DOC_{HC}待签署文件的硬拷贝(打印拷贝)

[0104] DOC_{DC}待签署文件的数字拷贝(电子拷贝)

[0105] DOC_{VER}文件的经验证拷贝

[0106] DOC_{SIG}文件的数字签署的拷贝

[0107] DID文件标识(例如,散列值)

[0108] $[DID]_{ENC}$编码的/加密的文件标识DID

[0109] $[DID]_{DEC}$解码的/解密的文件标识DID

[0110] K_{DID} 文件标识DID的加密密钥

[0111] K_{SIG} 与签署者相关联的私有加密密钥(例如,生物识别加密密钥)

[0112] SIG 文件的数字签署的拷贝DOC_{SIG}的数字签名(例如,生物识别-数字签名)

[0113] SA 待签署文件上的签署区

[0114] A 待签署文件上的敏感区

[0115] I 签署者的签名的墨迹

[0116] I 签署者的签名的数字图像

[0117] WM 编码文件标识DID的水印

[0118] WM_{SA}如在签署区SA中应用的编码文件标识DID的签署区水印

[0119] WM_{A} 如在敏感区A中应用的编码文件表示DID的敏感区水印

[0120] PEP 位置编码图案

[0121] ORD 用于读取水印WM、WM_{SA}、WM_{A}的光学读取器设备(例如,光学笔或触笔设备10)

[0122] DSD 用于签署文件的数字签署设备(例如,光学笔或触笔设备10)

[0123] 10 用作光学读取器设备ORD和数字签署设备DSD两者的光学笔或触笔设备。

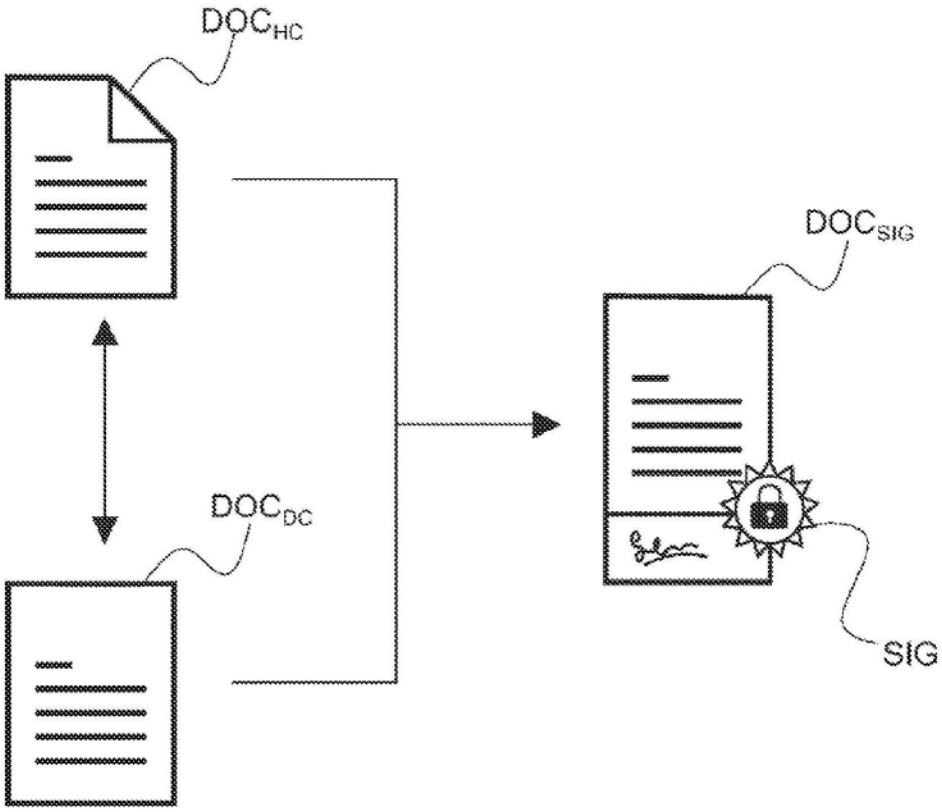


图1

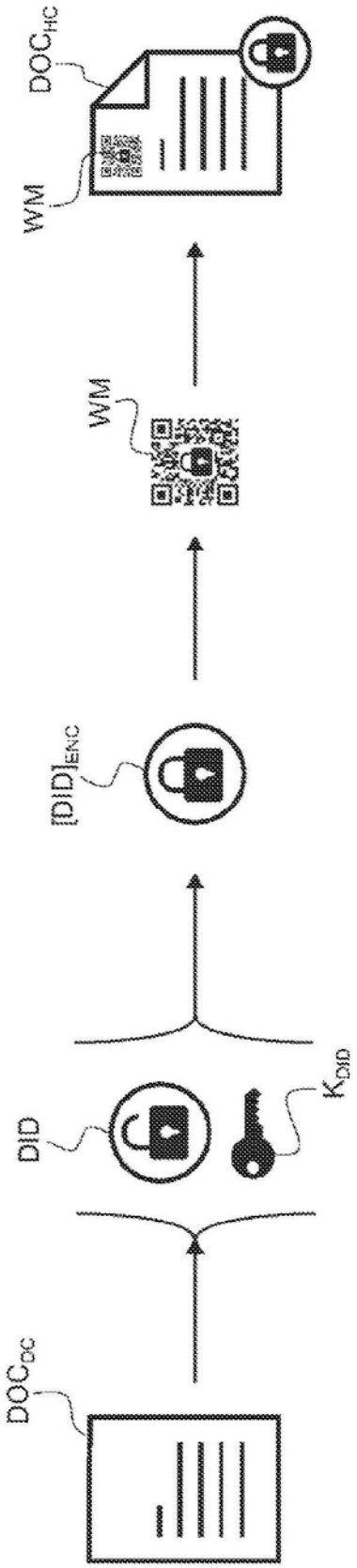


图2

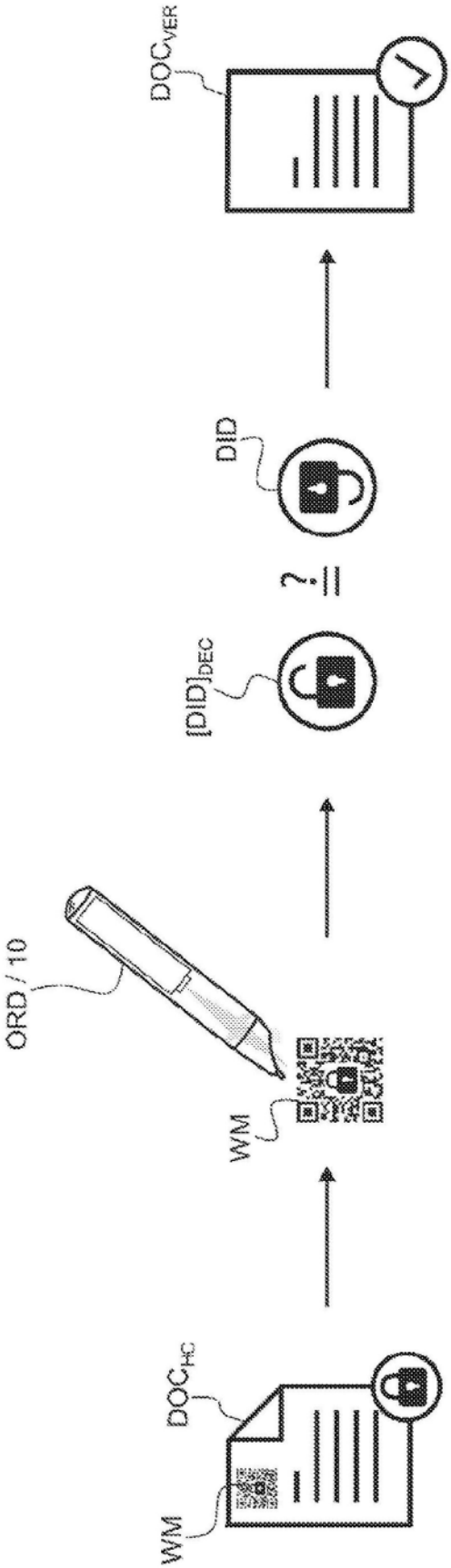


图3

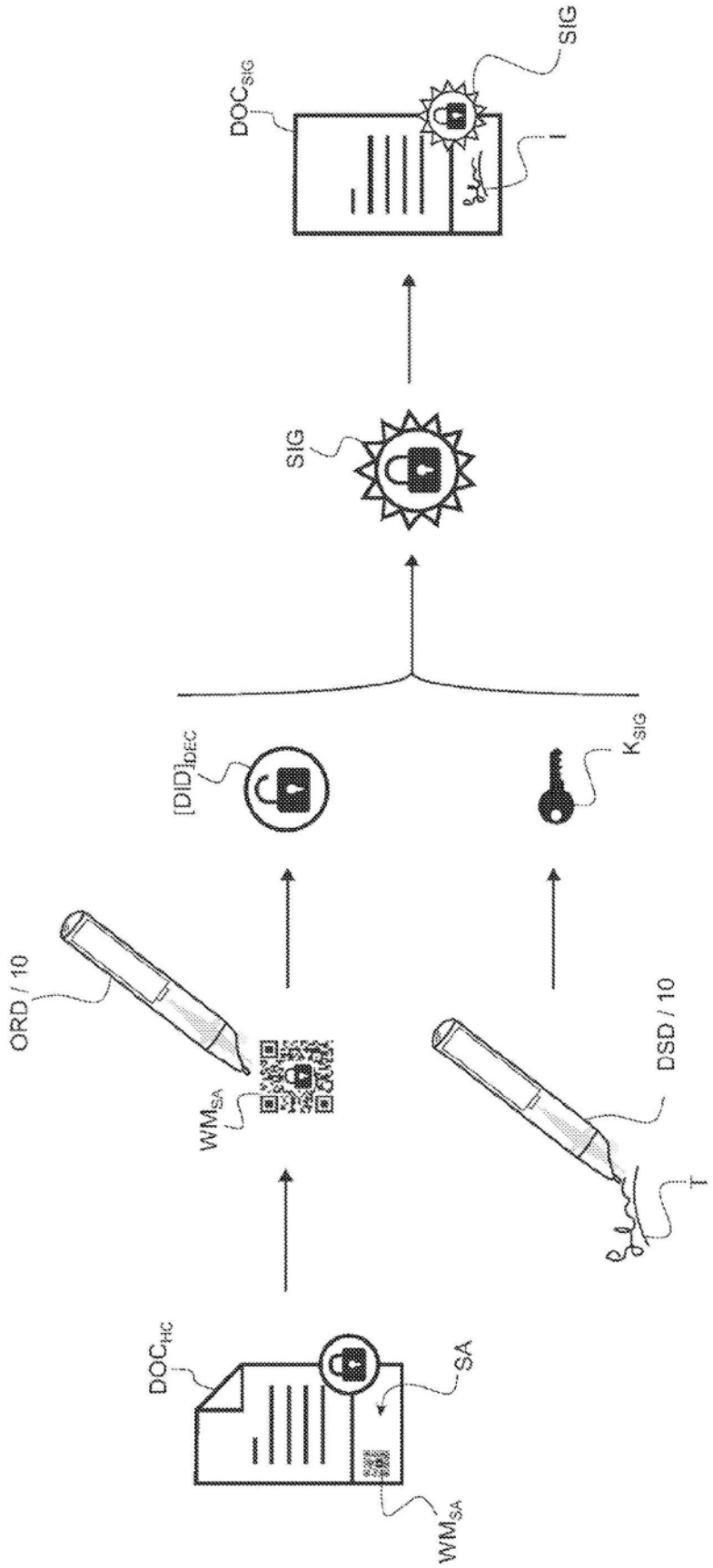


图4

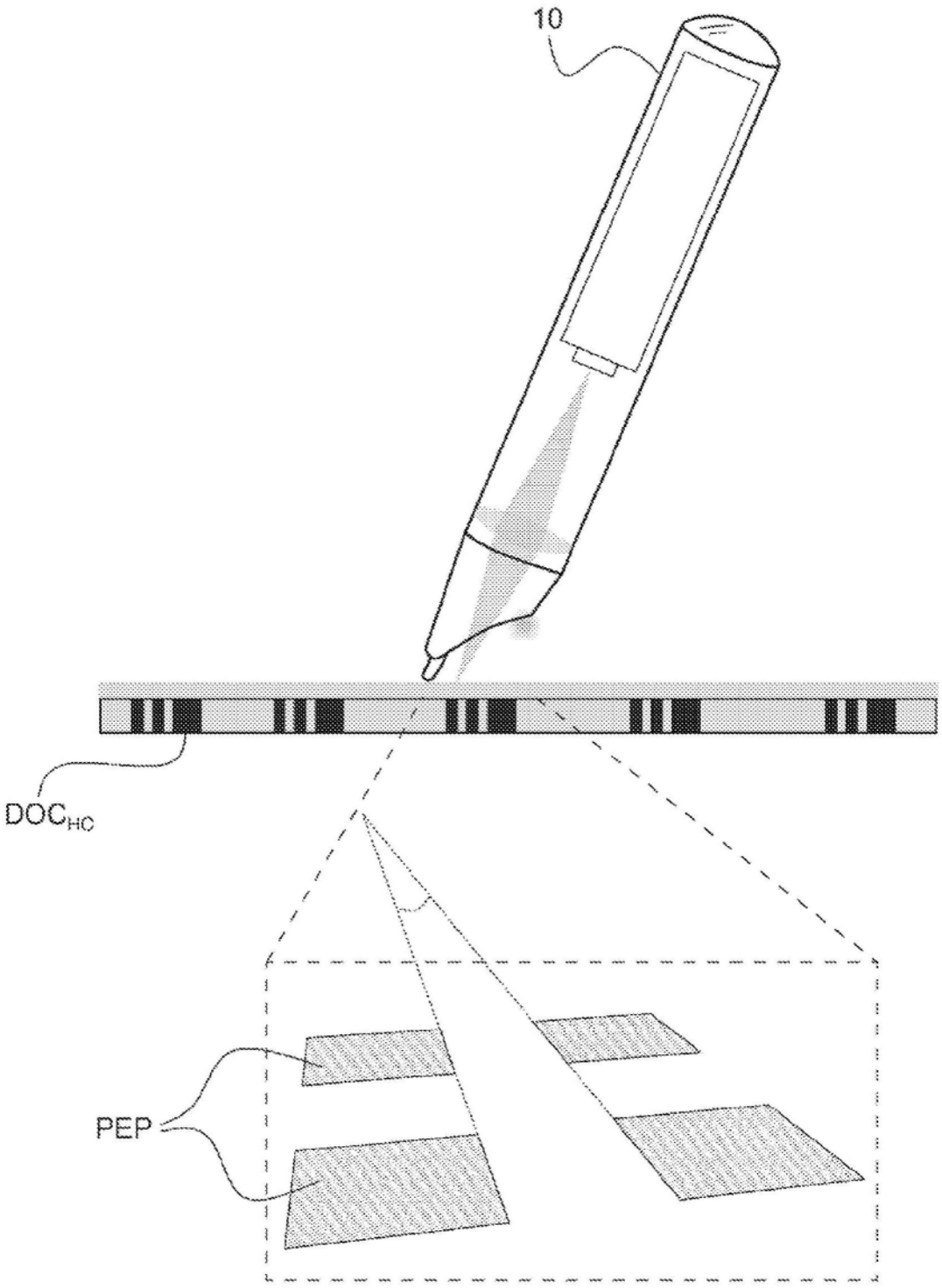


图5

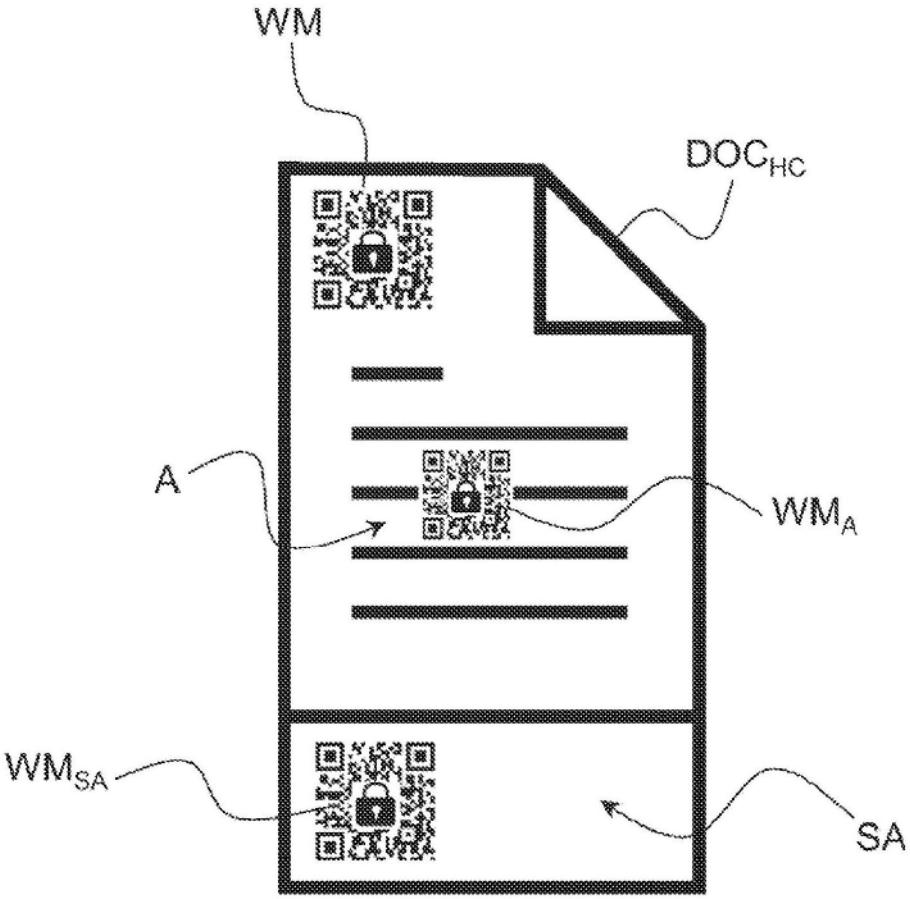


图6