(19)国家知识产权局

(12)发明专利

(10)授权公告号 CN 113191122 B
(45)授权公告日 2023.05.26

(21)申请号 202110453484.5

(22)申请日 2021.04.26

(65)同一申请的已公布的文献号
申请公布号 CN 113191122 A

(43)申请公布日 2021.07.30

(73)专利权人 长江勘测规划设计研究有限责任公司
地址 430010 湖北省武汉市解放大道1863号

(72)发明人 周剑 王立军 魏鹏帅 卞小草 张家成 魏小红 叶玲 黄康 刘盟盟

(74)专利代理机构 武汉开元知识产权代理有限公司 42104
专利代理师 陈家安

(51)Int.Cl.
G06F 40/143(2020.01)
G06F 16/11(2019.01)
G06F 21/64(2013.01)

(56)对比文件
CN 111143281 A,2020.05.12
CN 111159101 A,2020.05.15
CN 112184172 A,2021.01.05
US 2010241651 A1,2010.09.23
骆建珍;杨安荣;马来娣;.电子档案“四性”检测要求及其实现方法.浙江档案.2017,(第12期),全文.

审查员 周晓童

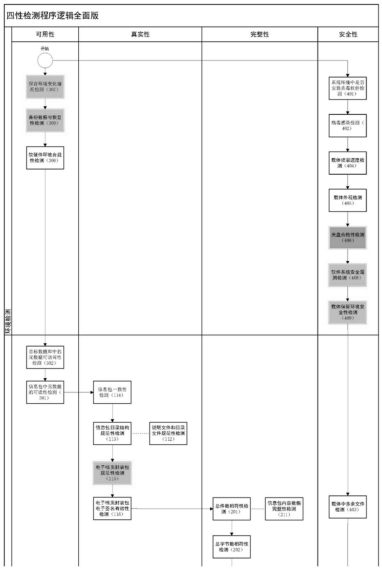
权利要求书2页 说明书7页 附图2页

(54)发明名称

面向服务的建设项目电子文件与电子档案四性检测方法

(57)摘要

本发明公开了一种面向服务的建设项目电子文件与电子档案四性检测方法。它包括如下步骤,步骤一:定义信息包结构;步骤二:调用接口,实现电子文件立档单位的内部业务部门、档案部门及档案馆相关业务系统远程调用四性检测接口进行电子文件或电子档案验证;步骤三:接收检测;后台通过接口收到相关数据后,对数据进行检测;步骤四:进行电子文件及电子档案四性检测,检测项目后的编号为调用的接口编号。本发明克服了现有技术纸质文件流转不便、查询繁琐等弊端;具有作为第三方服务供电子文件立档单位的内部业务部门、档案部门及档案馆用户进行调用,在线完成电子档案真实性、完整性、可用性、安全性验证,并实时返回相关检测结果及报告的优点。



CN 113191122 B

1.一种面向服务的建设项目电子文件与电子档案四性检测方法,其特征在于:包括如下步骤,

步骤一:定义信息包结构;

步骤二:调用接口,实现电子文件立档单位的内部业务部门、档案部门及档案馆相关业务系统远程调用四性检测接口进行电子文件或电子档案验证,具体如下:

1)检测前将被测电子文件及其元数据按指定的格式封装成信息包;

2)将信息包描述文件、封装好的信息包、备份文件传输至指定FTP;

3)调用接口服务传入检测接口编号、信息包路径、信息包封装拓扑结构描述文件路径、EEP元数据封装结构描述文件路径、数据库信息、归档范围及排序配置、用户元数据配置、备份文件路径及人工检测结果参数;

4)接收检测反馈消息,包括检测成功、失败消息及XML格式的成果报告;

5)对检测完成的电子文件进行标记,并关联检测报告;

步骤三:接收检测;

后台通过接口接收到相关数据后,对数据进行检测,检测方法如下:

1)对信息包路径解析得到信息包封装拓扑结构文件;

2)对信息包封装拓扑结构描述文件路径解析得到信息包封装拓扑结构描述文件;

3)利用信息包封装拓扑结构描述文件对信息包封装拓扑结构文件进行解析可得到所有实体文件及其元数据文件;

4)对EEP元数据封装结构描述文件路径解析得到信息包封装拓扑结构描述文件、EEP元数据封装结构描述文件;

5)利用EEP元数据封装结构描述文件对第3步得到的元数据文件进行解析得到电子文件的全部元数据值;

6)对数据库信息database、table、field解析可获取数据库中所记录的实体文件及其全部元数据值;

7)对用户元数据配置解析得到外部元数据策略;

8)在上述解析结果基础上,结合归档范围及排序配置、备份文件路径及人工检测数据共同作为输入值,完成各四性检测项目的计算比较分析;

步骤四:进行电子文件及电子档案四性检测,检测项目后的编号为调用的接口编号;

电子文件及电子档案四性检测方法,具体包括如下内容:

第一步,进行环境检测;

第二步,环境检测完成后,进入信息包及数据库元数据检测,同时开展可用性、真实性、完整性、安全性的检测工作,具体检测方法如下:

1)首先进行目标数据库中的元数据可访问性检测、信息包中元数据的可读性检测,检测数据库及信息包是否连通,以进一步深入进行到后续的数据检测环节;

2)确定数据库连通及信息包为可读后,再进行信息包的一致性检测,确保信息包没有被篡改;

3)针对上述信息包,进行信息包目录结构规范性检测及说明文件和目录文件规范性检测,确保信息包的结构准确,便于进一步利用;

4)对信息包进行解析得到电子档案封装包,并对其进行电子档案封装包规范性检测,

确保信息包中的电子档案封装包结构合规,便于进一步利用;

5)针对上一步验证后的电子档案封装包,进行XML代码级的验证:电子档案封装包电子签名有效性检测,通过分析封装包中的电子签名有效性确保XML代码完整来源可行;

6)下一步进行信息包的深度解析检测,首先进行文件数量的比较,总件数相符性检测、信息包内容数据完整性检测、载体中多余文件检测,再进行文件存储大小的比较,总字节数相符性检测;

7)下一步进行元数据项目的比较,分析其准确性,先后进行元数据项完整性检、信息包元数据完整性检;

8)下一步进入元数据内容的分析,首先从档号的内容格式开始检测,进行档号规范性检测、元数据项与档案馆要求的一致性检测;

9)档号分析完成后,进一步扩展对电子文件自带的元数据属性进行检测,进行内容数据的电子属性一致性检测;

10)进一步进行元数据是否关联内容数据检测,分析各元数据指向的文件路径是否存在关联内容,并进行归档范围检测;

11)继续对其他元数据项目内容进行格式及内容方面的检测,包括元数据项数据长度检测、元数据项数据类型、格式检测、设定值域的元数据项值域符合度检测、元数据项数据值合理性检测、元数据项数据包含特殊字符检测、元数据项数据重复性检测、元数据必填著录项目检测、过程信息完整性检测、连续性元数据项检测;

第三步,进行电子文件的内容检测;

第四步,针对过程中的全部过程进行综合评判,完成操作过程安全性检测。

2.根据权利要求1所述的面向服务的建设项目电子文件与电子档案四性检测方法,其特征在于:在步骤四中,电子文件及电子档案四性检测方法中,当检测项目未通过时,将各项检测成果记录在案一起展示给用户。

3.根据权利要求2所述的面向服务的建设项目电子文件与电子档案四性检测方法,其特征在于:在步骤四中,进行环境检测的具体方法如下:

1)采用多线程的运算方式同时启动可用性检测与安全性检测;

2)可用性检测中先后进行保存环境变化情况检测、备份数据可恢复性检测、软硬件环境合规性检测;

3)在上一步检测的同时,系统同时在安全性检测单元中先后进行系统环境中是否安装杀毒软件检测、病毒感染检测、载体读取速度检测、载体外观检测、光盘合格性检测、软件系统安全漏洞检测、载体保管环境安全性检测。

4.根据权利要求3所述的面向服务的建设项目电子文件与电子档案四性检测方法,其特征在于:在步骤四中,进行电子文件的内容检测的具体方法如下:

1)在上一步完成全部元数据项目及其内容格式的检测后,深入对与元数据关联的电子文件逐一进行检测,首先完成固化信息有效性检测,确保每份电子文件均未被篡改;

2)接下来进行内容数据格式检测、内容数据的可读性检测、内容数据完整性检测、内容数据格式长期可用性检测、附件数据完整性检测、信息包中包含的内容数据格式合规性检测。

面向服务的建设项目电子文件与电子档案四性检测方法

技术领域

[0001] 本发明涉及工程领域和信息技术领域，更具体地说它是一种面向服务的建设项目电子文件与电子档案四性检测方法。

背景技术

[0002] 电子档案的四性是指真实性、完整性、可用性和安全性，根据《电子文件归档与电子档案管理规范》《文书类电子档案检测一般要求》中的定义，真实性指电子档案的内容、逻辑结构和背景与形成时的原始状况相一致的性质；完整性指电子档案的内容、结构和背景信息齐全且没有破坏、变异或丢失的性质；可用性指电子档案可以被检索、呈现和理解的性质；安全性指电子档案的管理过程可控、数据存储可靠，未被破坏、未被非法访问的性质。

[0003] 真实性不仅能反映社会各项活动的历史原貌，而且是构成电子档案价值属性的前提，是确保电子档案具有行政有效性和法律凭证性的重要基础；完整性是确保电子档案凭证价值的重要保障；可用性是电子档案存在和具有保存价值的基础，如果电子档案不能便捷使用，再有价值的档案资料也会失去存在的实际意义；安全性是真实性、完整性和可用性的基础，是维护电子档案凭证价值、法律效力的保障。

[0004] 保证电子文件、电子档案的四性是电子文件能够成为电子档案的前提，也是电子档案能够长期保存的关键要素。2009年发布的《电子文件管理暂行办法》(两办厅字〔2009〕39号)首次提出了四性的概念，并且明确指出“电子文件归档时，应当进行真实、完整、可用和安全方面的鉴定、检测”；2012年国家档案局发布的《电子档案移交与接收办法》(档发〔2012〕7号)指出在电子档案移交和接收过程中要对电子档案的四性进行检测。为了规范电子档案的四性检测工作，国家档案局正着手制定电子档案四性检测方面的标准规范，目前已发布了《文书类电子档案检测一般要求》。

[0005] 由此可见，电子档案四性检测在电子档案生命周期管理过程中具有举足轻重的作用，是保证电子档案真实性、完整性、可用性、安全性的重要手段，也是确保电子档案凭证价值、查考价值和保存价值的重要措施。

[0006] 因此，开发一种电子档案四性检测方法很有必要。

发明内容

[0007] 本发明的目的是为了提供一种面向服务的建设项目电子文件与电子档案四性检测方法，作为第三方服务供电子文件立档单位的内部业务部门、档案部门及档案馆用户进行调用，在线完成电子档案真实性、完整性、可用性、安全性验证，并实时返回相关检测结果及报告。

[0008] 为了实现上述目的，本发明的技术方案为：一种面向服务的建设项目电子文件与电子档案四性检测方法，其特征在于：包括如下步骤，

[0009] 步骤一：定义信息包结构；

[0010] 步骤二：调用接口，实现电子文件立档单位的内部业务部门、档案部门及档案馆相

关业务系统远程调用四性检测接口进行电子文件或电子档案验证；

[0011] 步骤三：接收检测；

[0012] 后台通过接口收到相关数据后，对数据进行检测；

[0013] 步骤四：进行电子文件及电子档案四性检测，检测项目后的编号为调用的接口编号；

[0014] 电子文件及电子档案四性检测方法，具体包括如下内容：

[0015] 第一步，进行环境检测；

[0016] 第二步，环境检测完成后，进入信息包及数据库元数据检测，同时开展可用性、真实性、完整性、安全性的检测工作：

[0017] 第三步，进行电子文件的内容检测；

[0018] 第四步，针对过程中的全部过程进行综合评判，完成操作过程安全性检测。

[0019] 在上述技术方案中，在步骤二中，实现电子文件立档单位的内部业务部门、档案部门及档案馆相关业务系统远程调用四性检测接口进行电子文件或电子档案验证的方法，具体如下：

[0020] 1)检测前将被测电子文件及其元数据按指定的格式封装成信息包；

[0021] 2)将信息包描述文件、封装好的信息包、备份文件传输至指定FTP；

[0022] 3)调用接口服务传入检测接口编号、信息包路径、信息包封装拓扑结构描述文件路径、EEP元数据封装结构描述文件路径、数据库信息、归档范围及排序配置、用户元数据配置、备份文件路径及人工检测结果等参数；

[0023] 4)接收检测反馈消息，包括检测成功、失败消息及XML格式的成果报告；

[0024] 5)对检测完成的电子文件进行标记，并关联检测报告。

[0025] 在上述技术方案中，在步骤三中，后台通过接口收到相关数据后，检测方法如下：

[0026] 1)对信息包路径解析得到信息包封装拓扑结构文件；

[0027] 2)对信息包封装拓扑结构描述文件路径解析得到信息包封装拓扑结构描述文件；

[0028] 3)利用信息包封装拓扑结构描述文件对信息包封装拓扑结构文件进行解析可得到所有实体文件及其元数据文件；

[0029] 4)对EEP元数据封装结构描述文件路径解析得到信息包封装拓扑结构描述文件、EEP元数据封装结构描述文件；

[0030] 5)利用EEP元数据封装结构描述文件对第3步得到的元数据文件进行解析得到电子文件的全部元数据值；

[0031] 6)对数据库信息database、table、field解析可获取数据库中所记录的实体文件及其全部元数据值；

[0032] 7)对用户元数据配置解析得到外部元数据策略；

[0033] 8)在上述解析结果基础上，结合归档范围及排序配置、备份文件路径及人工检测数据共同作为输入值，完成各四性检测项目的计算比较分析。

[0034] 在上述技术方案中，在步骤四中，电子文件及电子档案四性检测方法中，当检测项目未通过时，将各项检测成果记录在案一起展示给用户。

[0035] 在上述技术方案中，在步骤四中，进行环境检测的具体方法如下：

[0036] 1)采用多线程的运算方式同时启动可用性检测与安全性检测；

[0037] 2)可用性检测中先后进行保存环境变化情况检测、备份数据可恢复性检测、软硬件环境合规性检测；

[0038] 3)在上一步检测的同时，系统同时在安全性检测单元中先后进行系统环境中是否安装杀毒软件检测、病毒感染检测、载体读取速度检测、载体外观检测、光盘合格性检测、软件系统安全漏洞检测、载体保管环境安全性检测。

[0039] 在上述技术方案中，在步骤四中，环境检测完成后，进入信息包及数据库元数据检测，同时开展可用性、真实性、完整性、安全性的检测工作，具体检测方法如下：

[0040] 1)首先进行目标数据库中的元数据可访问性检测、信息包中元数据的可读性检测，检测数据库及信息包是否连通，以进一步深入进行到后续的数据检测环节；

[0041] 2)确定数据库连通及信息包为可读后，再进行信息包的一致性检测，确保信息包没有被篡改；

[0042] 3)针对上述信息包，进行信息包目录结构规范性检测及说明文件和目录文件规范性检测，确保信息包的结构准确，便于进一步利用；

[0043] 4)对信息包进行解析得到电子档案封装包，并对其进行电子档案封装包规范性检测，确保信息包中的电子档案封装包结构合规，便于进一步利用；

[0044] 5)针对上一步验证后的电子档案封装包，进行XML代码级的验证：电子档案封装包电子签名有效性检测，通过分析封装包中的电子签名有效性确保XML代码完整来源可行；

[0045] 6)下一步进行信息包的深度解析检测，首先进行文件数量的比较，总件数相符性检测、信息包内容数据完整性检测、载体中多余文件检测，再进行文件存储大小的比较，总字节数相符性检测；

[0046] 7)下一步进行元数据项目的比较，分析其准确性，先后进行元数据项完整性检、信息包元数据完整性检；

[0047] 8)下一步进入元数据内容的分析，首先从档号的内容格式开始检测，进行档号规范性检测、元数据项与档案馆要求的一致性检测；

[0048] 9)档号分析完成后，进一步扩展对电子文件自带的元数据属性进行检测，进行内容数据的电子属性一致性检测；

[0049] 10)进一步进行元数据是否关联内容数据检测，分析各元数据指向的文件路径是否存在关联内容，并进行归档范围检测；

[0050] 11)继续对其他元数据项目内容进行格式及内容方面的检测，包括元数据项数据长度检测、元数据项数据类型、格式检测、设定值域的元数据项值域符合度检测、元数据项数据值合理性检测、元数据项数据包含特殊字符检测、元数据项数据重复性检测、元数据必填著录项目检测、过程信息完整性检测、连续性元数据项检测。

[0051] 在上述技术方案中，在步骤四中，进行电子文件的内容检测的具体方法如下：

[0052] 1)在上一步完成全部元数据项目及其内容格式的检测后，深入对与元数据关联的电子文件逐一进行检测，首先完成固化信息有效性检测，确保每份电子文件均未被篡改；

[0053] 2)接下来进行内容数据格式检测、内容数据的可读性检测、内容数据完整性检测、内容数据格式长期可用性检测、附件数据完整性检测、信息包中包含的内容数据格式合规性检测。

[0054] 本文所述的四性是指真实性、完整性、可用性和安全性。

[0055] 本发明具有如下优点：

[0056] (1)本发明中的水利水电工程质量验评电子文件形成、归档及电子档案移交管理系统采用信息化手段，形成的电子文件及电子档案可完全替代传统的纸质文件，从而消除了纸质文件流转不便、查询繁琐、保管麻烦等弊端；

[0057] (2)本发明采用四性检测等技术，确保电子文件及电子档案全生命周期内真实、完整、可靠、可用；

[0058] (3)本发明适用于水利水电工程质量验评电子文件形成、归档及电子档案移交管理工作，在实际应用中可有效减少人员、物资投入，可复制性高，适用于同类工程项目应用，具有可观的经济效益和社会效益。

附图说明

[0059] 图1为本发明面向服务的建设项目电子文件与电子档案四性检测的流程图的一部分。

[0060] 图2为本发明面向服务的建设项目电子文件与电子档案四性检测的流程图的另一部分。

[0061] 图1和图2组成本发明所述面向服务的建设项目电子文件与电子档案四性检测的完整流程图。

具体实施方式

[0062] 下面结合附图详细说明本发明的实施情况，但它们并不构成对本发明的限定，仅作举例而已。同时通过说明使本发明的优点更加清楚和容易理解。

[0063] 参阅附图可知：一种面向服务的建设项目电子文件与电子档案四性检测方法，具体包括：

[0064] 步骤一：信息包结构定义；

[0065] 预定义并共享信息包结构(information package structrue)，便于后台自动识别、提取包内数据进行分析，实现四性检测服务的自动化；

[0066] 预定义并共享信息包结构采用XMLSchema标准格式进行信息包结构描述，由用户根据不同建设项目电子文件归档及电子档案管理业务需求并参考相关规范要求制作信息包封装拓扑结构及电子文件EEP元数据封装结构描述文件(XSD格式)；

[0067] 步骤二：接口服务；

[0068] 提供一套供在线调用的接口服务，仅需业务系统将信息包描述文件、信息包路径、数据库等参数传入，由远端服务器配合用户进行检测并实时返回检测结果及报告，实现电子文件立档单位的内部业务部门、档案部门及档案馆相关业务系统远程调用四性检测接口进行电子文件或电子档案验证，实现方法如下：

[0069] 1)检测前将被测电子文件(档案)及其元数据按指定的格式封装成信息包；

[0070] 2)将信息包描述文件、封装好的信息包、备份文件传输至指定FTP；

[0071] 3)调用接口服务传入检测接口编号、信息包路径、信息包封装拓扑结构描述文件路径、EEP元数据封装结构描述文件路径、数据库信息、归档范围及排序配置、用户元数据配置、备份文件路径及人工检测结果等参数；

[0072] 其中,检测接口编号<nquery>为字符类型,档号查询接口编号,采用base64编码;信息包路径<ipurl>为字符类型,记录信息包的FTP路径信息,采用base64编码;信息包封装拓扑结构描述文件路径<ipschemaurl>为字符类型,记录信息包封装拓扑结构,采用base64编码;EEP元数据封装结构描述文件路径<eepschemaurl>为字符类型,记录电子文件EEP元数据封装结构,采用base64编码;数据库信息包含<database>、<table>、<field>信息,<database>为XML类型以记录数据库访问信息,采用base64编码,<table>为XML类型记录数据表的信息,采用base64编码,<field>为XML类型记录数据字段信息,包含字段类型、长度、值域、合理取值、重复性等参数,采用base64编码;归档范围及排序配置<gdscope>为XML类型,记录待检测归档范围及排序清单参数;用户元数据配置<config>为字符类型,记录元数据字段配置信息、重复性等配置参数,采用base64编码;备份文件路径<backupurl>为字符类型,记录备份文件的FTP路径,采用base64编码;人工检测结果<handinput>为XML类型,记录人工检测项目中输入的参数,采用base64编码;

[0073] 4)接收检测反馈消息,包括检测成功、失败消息及XML格式的成果报告;

[0074] 5)对检测完成的电子文件(档案)进行标记,并关联检测报告;

[0075] 步骤三:接收检测;

[0076] 后台通过接口收到相关数据后,检测方案如下:

[0077] 1)对信息包路径解析得到信息包封装拓扑结构文件(XML格式);

[0078] 2)对信息包封装拓扑结构描述文件路径解析得到信息包封装拓扑结构描述文件(XSD格式);

[0079] 3)利用信息包封装拓扑结构描述文件对信息包封装拓扑结构文件进行解析可得到所有实体文件及其元数据文件(XML格式);

[0080] 4)对EEP元数据封装结构描述文件路径解析得到信息包封装拓扑结构描述文件(XSD格式)、EEP元数据封装结构描述文件(XSD格式);

[0081] 5)利用EEP元数据封装结构描述文件对第3)步得到的元数据文件进行解析得到电子文件的全部元数据值;

[0082] 6)对数据库信息database、table、field解析可获取数据库中所记录的实体文件及其全部元数据值;

[0083] 7)对用户元数据配置解析得到外部元数据策略;

[0084] 8)在上述解析结果基础上,结合归档范围及排序配置、备份文件路径及人工检测数据共同作为输入值,完成各四性检测项目的计算比较分析;

[0085] 步骤四:四性检测;

[0086] 参考《文书类电子档案检测一般要求》(DA/T 70-2018)及程序开发逻辑,在企业业务部门向档案部门进行电子文件归档环节,企业档案部门向外部档案系统进行电子档案移交时以及在档案系统中进行长期保存时,按照以下程序进行电子文件及电子档案四性检测,检测项目后的编号为调用的接口编号;

[0087] 具体的四性检测方法,包括如下步骤:

[0088] 第一步,进行环境检测;

[0089] 1)采用多线程的运算方式同时启动可用性检测与安全性检测;其中,多线程的运算方式是系统运算常用的手段;

[0090] 2)可用性检测中先后进行保存环境变化情况检测(307)、备份数据可恢复性检测(309)、软硬件环境合规性检测(306);其中,保存环境变化情况检测、备份数据可恢复性检测、软硬件环境合规性检测均为现有技术;

[0091] 3)在上一步检测的同时,后台同时在安全性检测单元中先后进行系统环境中是否安装杀毒软件检测(401)、病毒感染检测(402)、载体读取速度检测(404)、载体外观检测(405)、光盘合格性检测(406)、软件系统安全漏洞检测(408)、载体保管环境安全性检测(409);无论检测是否合格均进行下一步检测,全部检测完成后,后台将检测记录展示给用户,即:将各项检测成果记录在案一起展示给用户;其中,环境中是否安装杀毒软件检测(401)、病毒感染检测(402)、载体读取速度检测(404)、载体外观检测(405)、光盘合格性检测(406)、软件系统安全漏洞检测(408)、载体保管环境安全性检测(409)均为现有技术;

[0092] 第二步,环境检测完成后,进入信息包及数据库元数据检测,同时开展可用性、真实性、完整性、安全性的检测工作;

[0093] 1)首先进行目标数据库中的元数据可访问性检测(302)、信息包中元数据的可读性检测(301),检测数据库及信息包是否连通,以进一步深入进行到后续的数据检测环节;检测合格进入下一步,检测不合格无法进入后续环节;其中,目标数据库中的元数据可访问性检测(302)、信息包中元数据的可读性检测(301)均为现有技术;

[0094] 2)确定数据库连通及信息包为可读后,再进行信息包的一致性检测(114),确保信息包没有被篡改;无论检测是否合格均进行下一步检测,全部检测完成后,后台将检测记录展示给用户,即:将各项检测成果记录在案一起展示给用户;其中,信息包的一致性检测(114)为现有技术;

[0095] 3)针对上述信息包,进行信息包目录结构规范性检测(113)及说明文件和目录文件规范性检测(112),确保信息包的结构准确,便于进一步利用;其中,信息包目录结构规范性检测(113)及说明文件和目录文件规范性检测(112)均为现有技术;

[0096] 4)对信息包进行解析得到电子档案封装包,并对其进行电子档案封装包规范性检测(115),确保信息包中的电子档案封装包(EEP包)结构合规,便于进一步利用;其中,电子档案封装包规范性检测(115)为现有技术;

[0097] 5)针对上一步验证后的电子档案封装包,进行XML代码级的验证:电子档案封装包电子签名有效性检测(116),通过分析封装包中的电子签名有效性确保XML代码完整来源可行;其中,XML代码级的验证方法为现有技术;

[0098] 6)下一步进行信息包的深度解析检测,首先进行文件数量的比较,总件数相符性检测(201)、信息包内容数据完整性检测(211)、载体中多余文件检测(403),再进行文件存储大小的比较,总字节数相符性检测(202);无论检测是否合格均进行下一步检测,全部检测完成后,后台将检测记录展示给用户,即:将各项检测成果记录在案一起展示给用户;其中,信息包的深度解析检测方法为现有技术;

[0099] 7)下一步进行元数据项目的比较,分析其准确性,先后进行元数据项完整性检测(203)、信息包元数据完整性检测(210);无论检测是否合格均进行下一步检测,全部检测完成后,后台将检测记录展示给用户,即:将各项检测成果记录在案一起展示给用户;其中,元数据项完整性检测(203)、信息包元数据完整性检测(210)均为现有技术。

[0100] 8)下一步进入元数据内容的分析,首先从档号的内容格式开始检测,进行档号规

范性检测(107)、元数据项(全宗号、目录号、分类号)与档案馆要求的一致性检测(109);无论检测是否合格均进行下一步检测,全部检测完成后,后台将检测记录展示给用户,即:将各项检测成果记录在案一起展示给用户;其中,档号规范性检测(107)、元数据项(全宗号、目录号、分类号)与档案馆要求的一致性检测(109)均为现有技术;

[0101] 9)档号分析完成后,进一步扩展对电子文件自带的元数据属性进行检测,进行内容数据的电子属性一致性检测(110);无论检测是否合格均进行下一步检测,全部检测完成后,后台将检测记录展示给用户,即:将各项检测成果记录在案一起展示给用户;其中,内容数据的电子属性一致性检测(110)为现有技术;

[0102] 10)进一步进行元数据是否关联内容数据检测(111),分析各元数据指向的文件路径是否存在关联内容,并进行归档范围检测(209);无论检测是否合格均进行下一步检测,全部检测完成后,后台将检测记录展示给用户,即:将各项检测成果记录在案一起展示给用户;其中,元数据是否关联内容数据检测(111)、归档范围检测(209)均为现有技术;

[0103] 11)继续对其他元数据项目内容进行格式及内容方面的检测,包括元数据项数据长度检测(102)、元数据项数据类型、格式检测(103)、设定值域的元数据项值域符合度检测(104)、元数据项数据值合理性检测(105)、元数据项数据包含特殊字符检测(106)、元数据项数据重复性检测(108)、元数据必填著录项目检测(204)、过程信息完整性检测(205)、连续性元数据项检测(206);无论检测是否合格均进行下一步检测,全部检测完成后,后台将检测记录展示给用户,即:将各项检测成果记录在案一起展示给用户;其中,元数据项数据长度检测(102)、元数据项数据类型、格式检测(103)、设定值域的元数据项值域符合度检测(104)、元数据项数据值合理性检测(105)、元数据项数据包含特殊字符检测(106)、元数据项数据重复性检测(108)、元数据必填著录项目检测(204)、过程信息完整性检测(205)、连续性元数据项检测(206)均为现有技术;

[0104] 第三步,进行电子文件(档案)的内容检测;

[0105] 1)在上一步完成全部元数据项目及其内容格式的检测后,深入对与元数据关联的电子文件(档案)逐一进行检测,首先完成固化信息有效性检测(101),确保每份电子文件(档案)均未被篡改;其中,固化信息有效性检测(101)为现有技术;

[0106] 2)接下来进行内容数据格式检测(303)、内容数据的可读性检测(304)、内容数据完整性检测(207)、内容数据格式长期可用性检测(305)、附件数据完整性检测(208)、信息包中包含的内容数据格式合规性检测(308);无论检测是否合格均进行下一步检测,全部检测完成后,后台将检测记录展示给用户,即:将各项检测成果记录在案一起展示给用户;其中,内容数据格式检测(303)、内容数据的可读性检测(304)、内容数据完整性检测(207)、内容数据格式长期可用性检测(305)、附件数据完整性检测(208)、信息包中包含的内容数据格式合规性检测(308)均为现有技术;

[0107] 第四步,针对过程中的全部过程进行综合评判,完成操作过程安全性检测(407);利用系统交互选择安全性评价意见;其中,操作过程安全性检测(407)为现有技术。

[0108] 上述四性检测实施过程中:实施步骤中若某项检测未通过、后台不会终止整个实施程序,而是将各项检测成果记录在案一起展示给用户;若某环节的检测中无需某项检测时,实施时可按顺序跳到下一步检测程序。

[0109] 其它未说明的部分均属于现有技术。

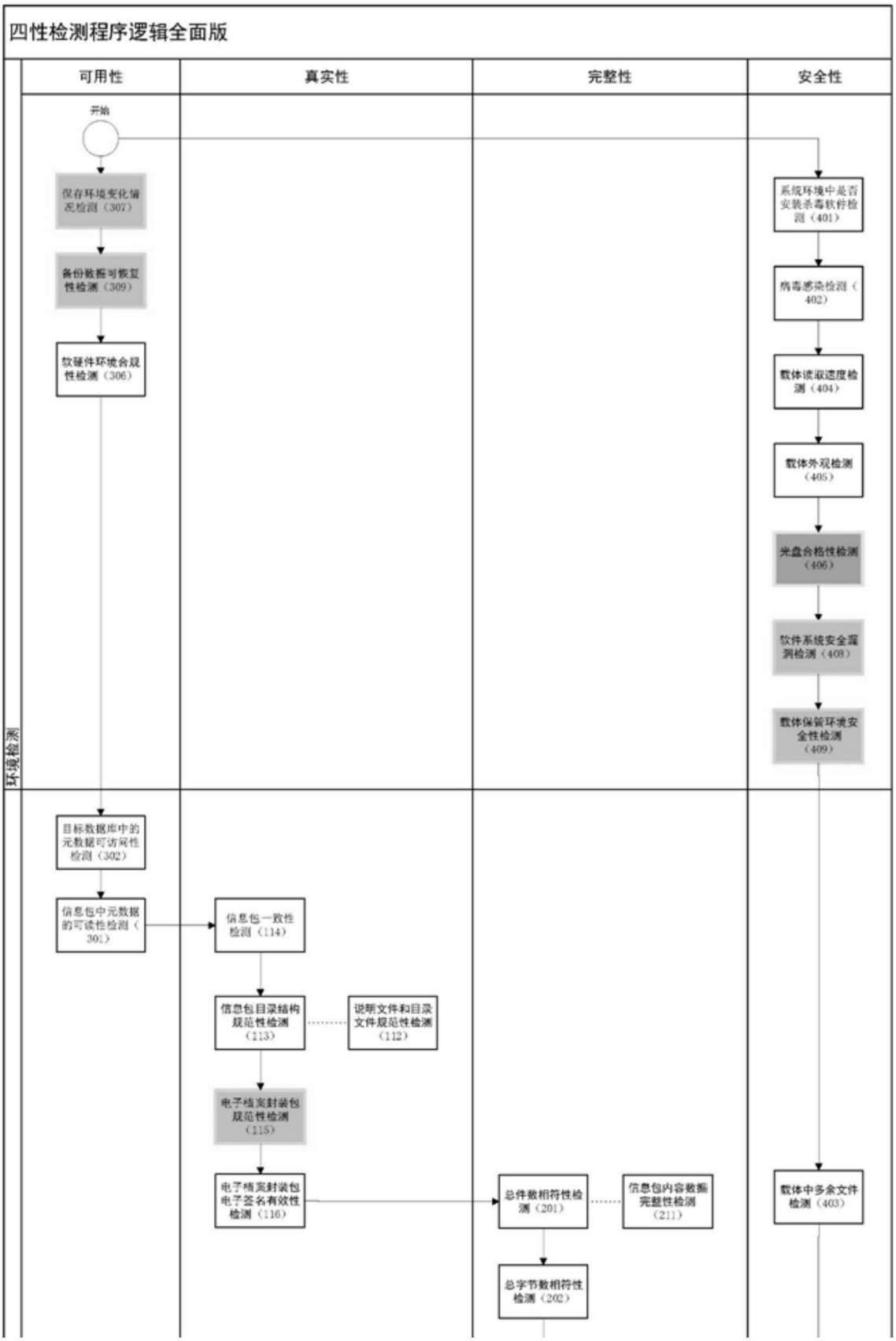

四性检测程序逻辑全面版
可用性
真实性
完整性
安全性
环境检测
开始
保存环境变化情况检测（307）
备份数据可恢复性检测（309）
软硬件环境合规性检测（306）
系统环境中是否安装杀毒软件检测（401）
病毒感染检测（402）
载体读取速度检测（404）
载体外观检测（405）
光盘合格性检测（406）
软件系统安全漏洞检测（408）
载体保管环境安全性检测（409）
目标数据库中的元数据可访问性检测（302）
信息包中元数据的可读性检测（301）
信息包一致性检测（114）
信息包目录结构规范性检测（113）
说明文件和目录文件规范性检测（112）
电子档案封装包规范性检测（115）
电子档案封装包电子签名有效性检测（116）
总件数相符性检测（201）
信息包内容数据完整性检测（211）
总字节数相符性检测（202）
载体中多余文件检测（403）

图1

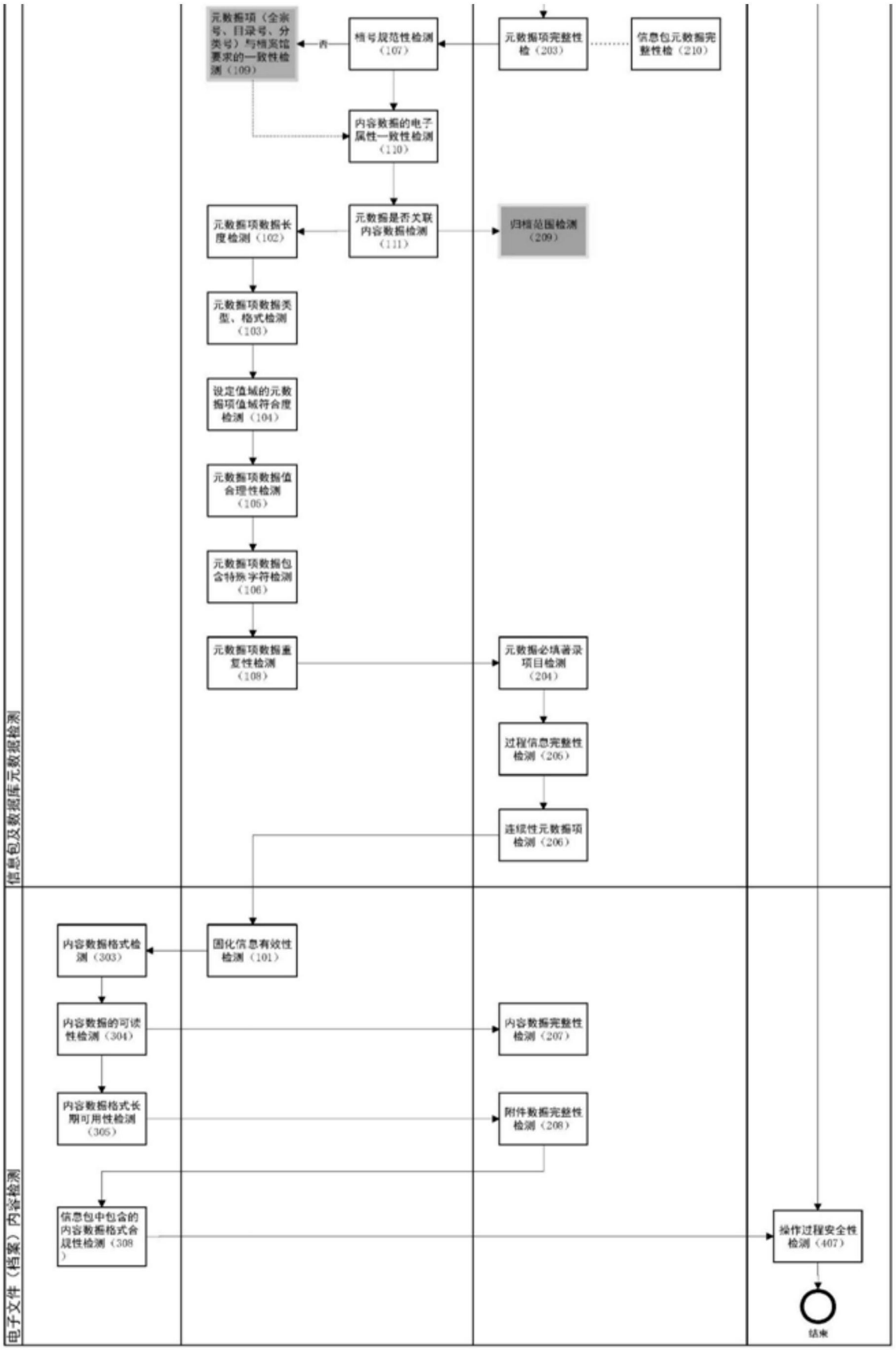

信息包及数据库元数据检测
电子文件（档案）内容检测
元数据项（全宗号、目录号、分类号）与档案馆要求的一致性检测（109）
否
档号规范性检测（107）
元数据项完整性检（203）
信息包元数据完整性检（210）
内容数据的电子属性一致性检测（110）
元数据项数据长度检测（102）
元数据是否关联内容数据检测（111）
归档范围检测（209）
元数据项数据类型、格式检测（103）
设定值域的元数据项值域符合度检测（104）
元数据项数据值合理性检测（105）
元数据项数据包含特殊字符检测（106）
元数据项数据重复性检测（108）
元数据必填著录项目检测（204）
过程信息完整性检测（205）
连续性元数据项检测（206）
固化信息有效性检测（101）
内容数据格式检测（303）
内容数据的可读性检测（304）
内容数据格式长期可用性检测（305）
信息包中包含的内容数据格式合规性检测（308）
内容数据完整性检测（207）
附件数据完整性检测（208）
操作过程安全性检测（407）
结束

图2