(12) 按照专利合作条约所公布的国际申请

(19) 世界知识产权组织
国 际 局

(43) 国际公布日
2018 年 6 月 7 日 (07.06.2018)

WIPO | PCT

(10) 国际公布号
WO 2018/098879 A1

(51) 国际专利分类号:
G06T 1/00 (2006.01)

(21) 国际申请号: PCT/CN2016/112858

(22) 国际申请日: 2016 年 12 月 29 日 (29.12.2016)

(25) 申请语言: 中文

(26) 公布语言: 中文

(30) 优先权:
201611095829.X 2016年11月30日 (30.11.2016) CN

(71) 申请人: 深圳TCL数字技术有限公司(SHENZHEN TCL DIGITAL TECHNOLOGY LTD.) [CN/CN]; 中国广东省深圳市前海深港合作区前湾一路鲤鱼门街一号前海深港合作区管理局综合办公楼A栋201室(入驻深圳市前海商务秘书有限公司), Guangdong 518054 (CN)。

(72) 发明人: 江亭(JIANG, Ting); 中国广东省深圳市前海深港合作区前湾一路鲤鱼门街一号前海深港合作区管理局综合办公楼A栋201室(入驻深圳市前海商务秘书有限公司), Guangdong 518054 (CN)。

(74) 代理人: 深圳市世纪恒程知识产权代理事务所(CENFO INTELLECTUAL PROPERTY AGENCY); 中国广东省深圳市南山区南山大道3838号设计产业园金栋二层210-212（原南头城工业村11栋）, Guangdong 518052 (CN)。

(81) 指定国(除另有指明，要求每一种可提供的国家保护): AE, AG, AL, AM, AO, AT, AU, AZ, BA, BB, BG, BH, BN, BR, BW, BY, BZ, CA, CH, CL, CN, CO, CR, CU, CZ, DE, DJ, DK, DM, DO, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, GT, HN, HR, HU, ID, IL, IN, IR, IS, JP, KE, KG, KH, KN, KP, KR, KW, KZ, LA, LC, LK, LR, LS, LU, LY, MA, MD, ME, MG, MK, MN, MW, MX, MY, MZ, NA, NG, NI, NO, NZ, OM, PA, PE, PG, PH, PL, PT, QA, RO, RS, RU, RW, SA, SC, SD, SE, SG, SK, SL, SM, ST, SV, SY, TH, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, ZA, ZM, ZW。

WO 2018/098879 A1

(54) **Title:** METHOD AND DEVICE FOR ENCRYPTING DIGITAL WATERMARK

(54) **发明名称:** 数字水印加密方法及装置

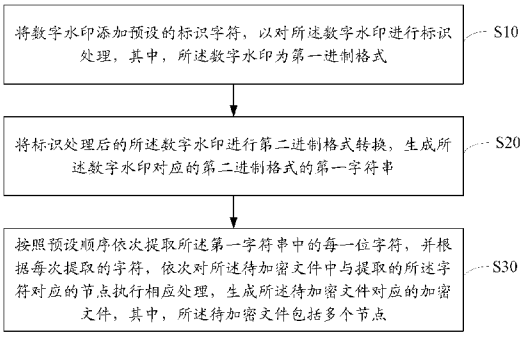

图 1

S10 ADD A PRESET IDENTIFICATION CHARACTER TO A DIGITAL WATERMARK, SO AS TO PERFORM IDENTIFICATION PROCESSING ON THE DIGITAL WATERMARK, THE DIGITAL WATERMARK BEING IN A FIRST NUMBERING SYSTEM FORMAT

S20 PERFORM A SECOND NUMBERING SYSTEM FORMAT TRANSFORMATION ON THE IDENTIFICATION-PROCESSED DIGITAL WATERMARK, TO GENERATE A FIRST CHARACTER STRING IN A SECOND NUMBERING SYSTEM FORMAT CORRESPONDING TO THE DIGITAL WATERMARK

S30 EXTRACT, IN SEQUENCE, EACH CHARACTER IN THE FIRST CHARACTER STRING ACCORDING TO A PRESET ORDER, AND ACCORDING TO THE EXTRACTED CHARACTER EACH TIME, PROCESS CORRESPONDINGLY, IN SEQUENCE, A NODE IN A TO-BE-ENCRYPTED FILE CORRESPONDING TO THE EXTRACTED CHARACTER TO GENERATE AN ENCRYPTED FILE CORRESPONDING TO THE TO-BE-ENCRYPTED FILE, THE TO-BE-ENCRYPTED FILE COMPRISING A PLURALITY OF NODES

(57) Abstract: A method for encrypting digital watermark, the method comprising the following steps: adding a preset identification character to a digital watermark, so as to perform identification processing on the digital watermark, the digital watermark being in a first numbering system format (S10); performing a second numbering system format transformation on the identification-processed digital watermark, to generate a first character string in a second numbering system format corresponding to the digital watermark (S20); and extracting, in sequence, each character in the first character string according to a preset order, and according to the extracted character each time, processing correspondingly, in sequence, a node in a to-be-encrypted file corresponding to the extracted character to generate an encrypted file corresponding to the to-be-encrypted file, the to-be-encrypted file comprising a plurality of nodes (S30). Further disclosed is a device for encrypting digital watermark, which improves the reliability of digital watermark encryption.

[见续页]

(84) 指定国(除另有指明，要求每一种可提供的地区保护)：ARIPO (BW, GH, GM, KE, LR, LS, MW, MZ, NA, RW, SD, SL, ST, SZ, TZ, UG, ZM, ZW), 欧亚 (AM, AZ, BY, KG, KZ, RU, TJ, TM), 欧洲 (AL, AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HR, HU, IE, IS, IT, LT, LU, LV, MC, MK, MT, NL, NO, PL, PT, RO, RS, SE, SI, SK, SM, TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, KM, ML, MR, NE, SN, TD, TG)。

本国际公布:

— 包括国际检索报告(条约第21条(3))。

(57) 摘要：一种数字水印加密方法，所述数字水印加密方法包括以下步骤：将数字水印添加预设的标识字符，以对所述数字水印进行标识处理，其中，所述数字水印为第一进制格式(S10)；将标识处理后的所述数字水印进行第二进制格式转换，生成所述数字水印对应的第二进制格式的第一字符串(S20)；按照预设顺序依次提取所述第一字符串中的每一位字符，并根据每次提取的字符，依次对待加密文件中与提取的所述字符对应的节点执行相应处理，生成所述待加密文件对应的加密文件，其中，所述待加密文件包括多个节点(S30)。还公开了一种数字水印加密装置，提高了数字水印加密的可靠性。

数字水印加密方法及装置

[1] 技术领域

[2] 本发明涉及数字水印技术领域，尤其涉及一种数字水印加密方法及装置。

[3] 背景技术

[4] 数字水印技术是将一些标识信息（即数字水印）嵌入数字载体（包括多媒体、文档、软件等）当中的技术，常用于保护信息安全或者信息隐藏，因此得到广泛应用。在对数字载体进行数字水印加密时，一般是将数字水印直接嵌入到数字载体当中，这会占用数字载体的一定存储空间，而当数字载体的可用存储空间不足时，嵌入数字水印会影响数字载体的正常使用，因此，数字水印加密的可靠性并非很高。

[5] 发明内容

[6] 本发明的主要目的在于提出一种数字水印加密方法及装置，旨在解决现有数字水印加密的可靠性不高的技术问题。

[7] 为实现上述目的，本发明提供的一种数字水印加密方法，所述数字水印加密方法包括以下步骤：

[8] 将数字水印添加预设的标识字符，以对所述数字水印进行标识处理，其中，所述数字水印为第一进制格式；

[9] 将标识处理后的所述数字水印进行第二进制格式转换，生成所述数字水印对应的第二进制格式的第一字符串；

[10] 按照预设顺序依次提取所述第一字符串中的每一位字符，并根据每次提取的字符，依次对待加密文件中与提取的所述字符对应的节点执行相应处理，生成所述待加密文件对应的加密文件，其中，所述待加密文件包括多个节点；

[11] 依次提取所述加密文件的每一个节点，并确定与提取的每一个节点对应的第二进制格式的字符，将确定的字符组成第二进制格式的第二字符串；

[12] 对所述第二字符串进行第一进制格式转换，生成第一进制格式的第三字符串，所述第三字符串中包含携带有所述标识字符的数字水印；

[13] 查找所述第三字符串中包含的所述标识字符，并根据所述标识字符获取所述数字水印。

[14] 优选地，所述查找所述第三字符串中包含的所述标识字符，并根据所述标识字符获取所述数字水印的步骤包括：

[15] 查找所述第三字符串中包含的两个所述标识字符；

[16] 提取两个所述标识字符之间的字符信息，所述字符信息为所述数字水印。

[17] 此外，为实现上述目的，本发明还提出一种数字水印加密方法，所述数字水印加密方法包括以下步骤：

[18] 将数字水印添加预设的标识字符，以对所述数字水印进行标识处理，其中，所述数字水印为第一进制格式；

[19] 将标识处理后的所述数字水印进行第二进制格式转换，生成所述数字水印对应的第二进制格式的第一字符串；

[20] 按照预设顺序依次提取所述第一字符串中的每一位字符，并根据每次提取的字符，依次对待加密文件中与提取的所述字符对应的节点执行相应处理，生成所述待加密文件对应的加密文件，其中，所述待加密文件包括多个节点。

[21] 优选地，所述将数字水印添加预设的标识字符的步骤包括：

[22] 在所述数字水印的头部位置和尾部位置添加所述标识字符。

[23] 优选地，当所述第二进制格式为二进制格式时，所述按照预设顺序依次提取所述第一字符串中的每一位字符，并根据每次提取的字符，依次对待加密文件中与提取的所述字符对应的节点执行相应处理的步骤包括：

[24] 按照预设顺序依次提取二进制格式的所述第一字符串中的每一位字符；

[25] 若当前提取的所述字符为二进制字符0，则维持所述待加密文件中与当前提取的所述字符对应的节点不变；

[26] 若当前提取的所述字符为二进制字符1，则在所述待加密文件中与当前提取的所述字符对应的节点的尾部位置添加一位空格字符。

[27] 优选地，所述依次对待加密文件中与提取的所述字符对应的节点执行相应处理，生成所述待加密文件对应的加密文件的步骤之后，还包括：

[28] 依次提取所述加密文件的每一个节点，并确定与提取的每一个节点对应的第二

进制格式的字符，将确定的字符组成第二进制格式的第二字符串；

[29] 对所述第二字符串进行第一进制格式转换，生成第一进制格式的第三字符串，所述第三字符串中包含携带有所述标识字符的数字水印；

[30] 查找所述第三字符串中包含的所述标识字符，并根据所述标识字符获取所述数字水印。

[31] 优选地，所述查找所述第三字符串中包含的所述标识字符，并根据所述标识字符获取所述数字水印的步骤包括：

[32] 查找所述第三字符串中包含的两个所述标识字符；

[33] 提取两个所述标识字符之间的字符信息，所述字符信息为所述数字水印。

[34] 此外，为实现上述目的，本发明还提出一种数字水印加密装置，所述数字水印加密装置包括：

[35] 标识模块，用于将数字水印添加预设的标识字符，以对所述数字水印进行标识处理，其中，所述数字水印为第一进制格式；

[36] 转换模块，用于将标识处理后的所述数字水印进行第二进制格式转换，生成所述数字水印对应的第二进制格式的第一字符串；

[37] 处理模块，用于按照预设顺序依次提取所述第一字符串中的每一位字符，并根据每次提取的字符，依次对待加密文件中与提取的所述字符对应的节点执行相应处理，生成所述待加密文件对应的加密文件，其中，所述待加密文件包括多个节点。

[38] 优选地，所述标识模块用于：

[39] 在所述数字水印的头部位置和尾部位置添加所述标识字符。

[40] 优选地，当所述第二进制格式为二进制格式时，所述处理模块包括：

[41] 提取单元，用于按照预设顺序依次提取二进制格式的所述第一字符串中的每一位字符；

[42] 处理单元，用于若当前提取的所述字符为二进制字符0，则维持所述待加密文件中与当前提取的所述字符对应的节点不变；若当前提取的所述字符为二进制字符1，则在所述待加密文件中与当前提取的所述字符对应的节点的尾部位置添加一位空格字符。

[43] 优选地，所述处理模块，还用于依次提取所述加密文件的每一个节点，并确定与提取的每一个节点对应的第二进制格式的字符，将确定的字符组成第二进制格式的第二字符串；

[44] 所述转换模块，还用于对所述第二字符串进行第一进制格式转换，生成第一进制格式的第三字符串，所述第三字符串中包含携带有所述标识字符的数字水印；

[45] 所述数字水印加密装置还包括：

[46] 获取模块，用于查找所述第三字符串中包含的所述标识字符，并根据所述标识字符获取所述数字水印。

[47] 优选地，所述获取模块包括：

[48] 查找单元，用于查找所述第三字符串中包含的两个所述标识字符；

[49] 获取单元，用于提取两个所述标识字符之间的字符信息，所述字符信息为所述数字水印。

[50] 本发明提出的数字水印加密方法和装置，当要对待加密文件进行数字水印加密时，首先将第一进制格式的数字水印添加预设的标识字符，然后对数字水印进行第二进制格式转换，生成数字水印对应的第二进制格式的第一字符串，之后按照预设顺序依次提取第一字符串中的每一位字符，并根据每次提取的字符，依次对待加密文件中与提取的字符所对应的节点执行相应处理，处理完成后生成该待加密文件对应的加密文件，因此，加密过程只是对待加密文件的节点进行处理，而并没有将数字水印直接嵌入到待加密文件中，避免了由于嵌入数字水印占用存储空间而影响待加密文件使用的问题，从而提高了数字水印加密的可靠性。

[51] 附图说明

[52] 图1为本发明数字水印加密方法第一实施例的流程示意图；

[53] 图2为本发明数字水印加密方法第二实施例的流程示意图；

[54] 图3为本发明数字水印加密装置第一实施例的功能模块示意图；

[55] 图4为本发明数字水印加密装置第一实施例中处理模块的细化功能模块示意图

[56] 图5为本发明数字水印加密装置第二实施例的功能模块示意图；

[57] 图6为本发明数字水印加密装置第二实施例中获取模块的细化功能模块示意图。

[58] 本发明目的实现、功能特点及优点将结合实施例，参照附图做进一步说明。

[59] 具体实施方式

[60] 应当理解，此处所描述的具体实施例仅仅用以解释本发明，并不用于限定本发明。

[61] 本发明提供一种数字水印加密方法，参照图1，图1为本发明数字水印加密方法第一实施例的流程示意图。

[62] 在该实施例中，所述数字水印加密方法包括以下步骤：

[63] 步骤S10，将数字水印添加预设的标识字符，以对所述数字水印进行标识处理，其中，所述数字水印为第一进制格式；

[64] 数字水印技术是将一些标识信息（即数字水印）嵌入数字载体当中（包括多媒体、文档、软件等）或是间接表示（修改特定区域的结构），且不影响原载体的使用价值，也不容易被探知和再次修改，但可以被生产方识别和辨认的技术，常用于保护信息安全或者信息隐藏。本实施例中，采用数字水印对待加密文件进行加密处理，其中，该待加密文件包括多媒体、文档、软件等等。

[65] 首先，对数字水印进行标识处理，将数字水印添加预设的标识字符，比如，预先设置数字水印对应的标识字符为“#”，本领域技术人员可以理解的是，也可以设置标识字符为其他字符，在此不作限制。其中，数字水印为第一进制格式，比如，数字水印为十进制格式。

[66] 可选地，所述步骤S10包括：

[67] 在所述数字水印的头部位置和尾部位置添加所述标识字符。

[68] 当对数字水印进行标识处理时，在数字水印的头部位置和尾部位置添加预设的标识字符，比如，在数字水印的头部位置和尾部位置分别添加字符“#”，以对数字水印进行标识处理。

[69] 步骤S20，将标识处理后的所述数字水印进行第二进制格式转换，生成所述数字水印对应的第二进制格式的第一字符串；

[70] 当对数字水印进行标识处理之后，将标识处理后的数字水印进行第二进制格式

转换，生成该数字水印对应的第二进制格式的第一字符串。比如，若第二进制格式为二进制格式，则将标识处理后的数字水印进行二进制格式转换，生成该数字水印对应的二进制格式的第一字符串，也即生成二进制01字符串。

[71] 步骤S30，按照预设顺序依次提取所述第一字符串中的每一位字符，并根据每次提取的字符，依次对所述待加密文件中与提取的所述字符对应的节点执行相应处理，生成所述待加密文件对应的加密文件，其中，所述待加密文件包括多个节点。

[72] 本实施例中，当生成第二进制格式的第一字符串之后，按照预设顺序依次提取该第一字符串中的每一位字符，比如按照从高位到低位的顺序依次提取该第一字符串的每一位字符，可以理解的是，也可以按照从低位到高位的顺序依次提取该第一字符串的每一位字符。由于待加密文件包含多个节点，根据每次提取的字符，依次对待加密文件中与提取的字符对应的节点执行相应处理。比如，根据提取的第一位字符，对待加密文件中的第一个节点进行相应处理，根据提取的第二位字符，对待加密文件中的第二个节点进行相应处理，按照此方式依次根据提取的每一位字符，对待加密文件中与该字符对应的节点进行相应处理。当根据第一字符串中的每位字符对待加密文件中与每位字符对应的节点进行相应处理完成之后，也即完成对待加密文件的加密处理，生成该待加密文件对应的加密文件。

[73] 可选地，在第二进制格式为二进制格式时，所述步骤S30包括：

[74] 步骤a，按照预设顺序依次提取二进制格式的所述第一字符串中的每一位字符；

[75] 步骤b，若当前提取的所述字符为二进制字符0，则维持所述待加密文件中与当前提取的所述字符对应的节点不变；

[76] 步骤c，若当前提取的所述字符为二进制字符1，则在所述待加密文件中与当前提取的所述字符对应的节点的尾部位置添加一位空格字符。

[77] 在第二进制格式为二进制格式时，对标识处理后的数字水印进行二进制格式转换，生成该数字水印对应的二进制格式的第一字符串，然后按照预设顺序依次提取二进制格式的第一字符串中的每一位字符，也即提取二进制字符0和二进制

字符1。若当前提取的字符为二进制字符0，则维持待加密文件中与当前提取的字符对应的节点不变；若当前提取的字符为二进制字符1，则在待加密文件中与当前提取的字符对应的节点的尾部位置添加一位空格字符。按照此方式依次根据提取的第一字符串中的每一位字符，对待加密文件中与该字符对应的节点进行相应处理。

[78] 下面以安卓应用的apk（AndroidPackage，安卓安装包）文件为例，对本发明数字水印加密方法进行详细说明。

[79] 当用户需要对某一款安卓应用的apk文件进行数字水印加密时，用户首先对数字水印进行标识处理，比如在数字水印的头部位置和尾部位置分别添加字符“#”。然后对添加了标识字符的数字水印进行进制格式转换，比如对添加了标识字符的数字水印进行二进制格式转换，生成二进制格式的第一字符串，也即二进制01字符串。

[80] 由于apk文件是一个zip压缩包，因此，要对该apk文件进行解压，解压后的apk文件包括AndroidManifest.xml文件、META-INF目录文件、res目录文件、lib目录文件、assets目录文件、classes.dex文件、resources.arsc文件。

[81] 其中，AndroidManifest.xml文件是每个安卓应用都必须定义和包含的，它描述了安卓应用的名字、版本、权限、引用的库文件等等信息；META-INF目录文件下存放的是签名信息，用来保证apk包的完整性和系统的安全；res目录文件存放资源文件、布局文件等，其中，drawable存放资源文件，layout、xml存放布局文件；lib目录文件下的子目录armeabi存放的是一些so文件；assets目录文件存放一些配置文件；classes.dex文件是Java源码编译后的代码文件；resources.arsc文件是编译后的资源文件，大多数情况下，需要汉化的单词、语句绝大多数都在这个文件里，汉化的时候首先就要看这个文件。

[82] 由于xml文件有巨大的冗余空间，便于嵌入数字水印等信息，因此，在对apk文件解压后，获取res目录文件下的xml文件。获取的该xml文件是经过编译生成的二进制文件，也即该xml文件为二进制格式，因此，在获取到该xml文件后，先对该xml文件进行十进制格式转换，获取到格式转换后的十进制格式xml文件。

[83] 之后，按照预设顺序依次提取第一字符串中的每一位字符，也即提取二进制字

符0和二进制字符1。若当前提取的字符为二进制字符0，则维持十进制格式xml文件中与当前提取的字符对应的item节点不变；若当前提取的字符为二进制字符1，则在十进制格式xml文件中与当前提取的字符对应的item节点的尾部位置添加一位空格字符。按照此方式依次根据提取第一字符串中的每一位字符，对十进制格式xml文件中与每一位字符对应的item节点进行相应处理，生成加密后的xml文件。

[84] 例如，若提取的第一位字符为二进制字符1，则在十进制格式xml文件的第一个item节点的尾部位置添加一位空格字符；若提取的第二位字符为二进制字符0，则维持十进制格式xml文件的第二个item节点不变。按照此方式依次根据提取的每一位字符，对十进制格式xml文件中与每一位字符对应的item节点进行相应处理。

[85] 加密完成之后，将加密后的xml文件进行二进制格式转换，然后将二进制格式转换后的xml文件与其他AndroidManifest.xml文件、META-INF目录文件、resources.arsc文件等各个文件一起压缩打包，生成加密后的apk文件。进一步地，由于有些apk文件需要通过签名进行校验，因此，在生成加密apk文件之后，对该加密apk文件进行签名处理。

[86] 本实施例提供的方案，当要对待加密文件进行数字水印加密时，首先将第一进制格式的数字水印添加预设的标识字符，然后对数字水印进行第二进制格式转换，生成数字水印对应的第二进制格式的第一字符串，之后按照预设顺序依次提取第一字符串中的每一位字符，并根据每次提取的字符，依次对待加密文件中与提取的字符所对应的节点执行相应处理，处理完成后生成该待加密文件对应的加密文件，因此，加密过程只是对待加密文件的节点进行处理，而并没有将数字水印直接嵌入到待加密文件中，避免了由于嵌入数字水印占用存储空间而影响待加密文件使用的问题，从而提高了数字水印加密的可靠性。

[87] 进一步地，如图2所示，基于第一实施例提出本发明数字水印加密方法第二实施例，在本实施例中，所述步骤S30之后，还包括：

[88] 步骤S40，依次提取所述加密文件的每一个节点，并确定与提取的每一个节点对应的第二进制格式的字符，将确定的字符组成第二进制格式的第二字符串；

[89] 步骤S50，对所述第二字符串进行第一进制格式转换，生成第一进制格式的第三字符串，所述第三字符串中包含携带有所述标识字符的数字水印；

[90] 步骤S60，查找所述第三字符串中包含的所述标识字符，并根据所述标识字符获取所述数字水印。

[91] 在本实施例中，要提取第一实施例中生成的加密文件所对应的数字水印时，首先依次提取该加密文件的每一个节点，由于加密文件中的节点是根据第二进制格式的第一字符串中的每一位字符进行相应处理过的，因此，根据提取的节点，可确定与提取的该节点对应的第二进制格式的字符。在依次确定出与提取的每一个节点对应的第二进制格式的字符之后，将确定的第二进制格式的字符组成第二进制格式的第二字符串，该第二字符串中包含了第二进制格式的第一字符串。

[92] 之后，对第二进制格式的该第二字符串进行第一进制格式转换，生成第一进制格式的第三字符串。在对第二字符串进行第一进制格式转换时，也即对第二进制格式的第一字符串进行了第一进制格式转换，而第一字符串进行第一进制格式转换之后会生成携带有标识字符的数字水印，也即第三字符串中包含了携带有标识字符的数字水印。从该第三字符串中查找出该标识字符，当查找到该标识字符时，根据该标识字符，获取到数字水印。

[93] 可选地，若在对待加密文件进行数字水印加密的过程中，在数字水印的头部位置和尾部位置添加了标识字符，则生成的第三字符串中包含有两个标识字符。此时，所述步骤S60包括：

[94] 步骤d，查找所述第三字符串中包含的两个所述标识字符；

[95] 步骤e，提取两个所述标识字符之间的字符信息，所述字符信息为所述数字水印。

[96] 当生成第三字符串后，从第三字符串中查找出其包含的两个标识字符，然后提取出该两个标识字符之间的字符信息，该字符信息即为待加密文件在进行数字水印加密时所采用的数字水印，也即实现了从加密文件中提取出数字水印。

[97] 下面以加密apk文件为例，对本实施例中的数字水印加密方法进行详细说明。

[98] 当用户要从加密apk文件中提取出数字水印时，首先对该加密apk文件进行解压

，获取解压后的res目录文件下的xml文件。由于该xml文件是二进制格式的，因此，对该xml文件进行十进制格式转换，生成格式转换后的十进制格式xml文件。然后依次提取十进制格式xml文件中的item节点，并根据提取的item节点，确定与该item节点对应的二进制字符。例如，判断提取的每一个item节点的尾部位置是否有一位空格字符，当item节点的尾部位置有一位空格字符时，确定该item节点对应二进制字符1；当item节点的尾部位置没有空格字符时，确定该item节点对应二进制字符0。在确定每一个item节点对应的二进制字符之后，将确定的字符组成第二进制格式的第二字符串。

[99] 然后，将该第二字符串进行十进制格式转换，生成十进制的第三字符串，该第三字符中包含了携带标识字符的数字水印。从该第三字符串中查找出标识字符，并根据标识字符获取数字水印。比如，若在对apk文件进行数字水印加密的过程中，在数字水印的头部位置和尾部位置添加了标识字符，则在第三字符串中查找出两个标识字符，提取出该两个标识字符之间的字符信息，该字符信息就是在对apk文件进行数字水印加密时所采用的数字水印，也即完成了从加密apk文件中提取出数字水印。

[100] 本实施例提供的方案，要提取加密文件所对应的数字水印时，首先依次提取该加密文件的每一个节点，并确定与提取的每一个节点对应的第二进制格式的字符，将确定的字符组成第二进制格式的第二字符串，然后对该第二字符串进行第一进制格式转换，生成第一进制格式的第三字符串，该第三字符串中就包含携带有标识字符的数字水印，从第三字符串中查找出标识字符后，根据标识字符获取到数字水印，因此，本实施例的方案不仅实现了数字水印加密，而且还实现了加密文件的数字水印提取。

[101] 本发明提供一种数字水印加密装置。

[102] 参照图3，图3为本发明数字水印加密装置第一实施例的功能模块示意图。

[103] 需要强调的是，对本领域的技术人员来说，图4所示功能模块图仅仅是一个较佳实施例的示例图，本领域的技术人员围绕图4所示的数字水印加密装置的功能模块，可轻易进行新的功能模块的补充；各功能模块的名称是自定义名称，仅用于辅助理解该数字水印加密装置的各个程序功能块，不用于限定本发明的技

术方案，本发明技术方案的核心是，各自定义名称的功能模块所要达成的功能。

[104] 在本实施例中，所述数字水印加密装置包括：

[105] 标识模块10，用于将数字水印添加预设的标识字符，以对所述数字水印进行标识处理，其中，所述数字水印为第一进制格式；

[106] 数字水印技术是将一些标识信息（即数字水印）嵌入数字载体当中（包括多媒体、文档、软件等）或是间接表示（修改特定区域的结构），且不影响原载体的使用价值，也不容易被探知和再次修改，但可以被生产方识别和辨认的技术，常用于保护信息安全或者信息隐藏。本实施例中，采用数字水印对待加密文件进行加密处理，其中，该待加密文件包括多媒体、文档、软件等等。

[107] 首先，标识模块10对数字水印进行标识处理，将数字水印添加预设的标识字符，比如，预先设置数字水印对应的标识字符为“#”，本领域技术人员可以理解的是，也可以设置标识字符为其他字符，在此不作限制。其中，数字水印为第一进制格式，比如，数字水印为十进制格式。

[108] 可选地，所述标识模块10具体用于：

[109] 在所述数字水印的头部位置和尾部位置添加所述标识字符。

[110] 当对数字水印进行标识处理时，标识模块10在数字水印的头部位置和尾部位置添加预设的标识字符，比如，标识模块10在数字水印的头部位置和尾部位置分别添加字符“#”，以对数字水印进行标识处理。

[111] 转换模块20，用于将标识处理后的所述数字水印进行第二进制格式转换，生成所述数字水印对应的第二进制格式的第一字符串；

[112] 当标识模块10对数字水印进行标识处理之后，转换模块20将标识处理后的数字水印进行第二进制格式转换，生成该数字水印对应的第二进制格式的第一字符串。比如，若第二进制格式为二进制格式，则转换模块20将标识处理后的数字水印进行二进制格式转换，生成该数字水印对应的二进制格式的第一字符串，也即生成二进制01字符串。

[113] 处理模块30，用于按照预设顺序依次提取所述第一字符串中的每一位字符，并根据每次提取的字符，依次对待加密文件中与提取的所述字符对应的节点执行

相应处理，生成所述待加密文件对应的加密文件，其中，所述待加密文件包括多个节点。

[114] 本实施例中，当生成第二进制格式的第一字符串之后，处理模块30按照预设顺序依次提取该第一字符串中的每一位字符，比如按照从高位到低位的顺序依次提取该第一字符串的每一位字符，可以理解的是，也可以按照从低位到高位的顺序依次提取该第一字符串的每一位字符。由于待加密文件包含多个节点，根据每次提取的字符，处理模块30依次对待加密文件中与提取的字符对应的节点执行相应处理。比如，处理模块30根据提取的第一位字符，对待加密文件中的第一个节点进行相应处理，根据提取的第二位字符，对待加密文件中的第二个节点进行相应处理，处理模块30按照此方式依次根据提取的每一位字符，对待加密文件中与该字符对应的节点进行相应处理。当根据第一字符串中的每位字符对待加密文件中与每位字符对应的节点进行相应处理完成之后，也即完成对待加密文件的加密处理，生成该待加密文件对应的加密文件。

[115] 可选地，如图4所示，在第二进制格式为二进制格式时，所述处理模块30包括：

[116] 提取单元31，用于按照预设顺序依次提取二进制格式的所述第一字符串中的每一位字符；

[117] 处理单元32，用于若当前提取的所述字符为二进制字符0，则维持所述待加密文件中与当前提取的所述字符对应的节点不变；若当前提取的所述字符为二进制字符1，则在所述待加密文件中与当前提取的所述字符对应的节点的尾部位置添加一位空格字符。

[118] 在第二进制格式为二进制格式时，转换模块20对标识处理后的数字水印进行二进制格式转换，生成该数字水印对应的二进制格式的第一字符串，然后提取单元31按照预设顺序依次提取二进制格式的第一字符串中的每一位字符，也即提取二进制字符0和二进制字符1。若当前提取的字符为二进制字符0，则处理单元32维持待加密文件中与当前提取的字符对应的节点不变；若当前提取的字符为二进制字符1，则处理单元32在待加密文件中与当前提取的字符对应的节点的尾部位置添加一位空格字符。处理单元32按照此方式依次根据提取的第一字符串

中的每一位字符，对待加密文件中与该字符对应的节点进行相应处理。

[119] 本实施例提供的方案，当要对待加密文件进行数字水印加密时，首先标识模块10将第一进制格式的数字水印添加预设的标识字符，然后转换模块20对数字水印进行第二进制格式转换，生成数字水印对应的第二进制格式的第一字符串，之后处理模块30按照预设顺序依次提取第一字符串中的每一位字符，并根据每次提取的字符，依次对待加密文件中与提取的字符所对应的节点执行相应处理，处理完成后生成该待加密文件对应的加密文件，因此，加密过程只是对待加密文件的节点进行处理，而并没有将数字水印直接嵌入到待加密文件中，避免了由于嵌入数字水印占用存储空间而影响待加密文件使用的问题，从而提高了数字水印加密的可靠性。

[120] 进一步地，如图5所示，基于第一实施例提出本发明数字水印加密装置第二实施例，在本实施例中，所述处理模块30还用于：

[121] 依次提取所述加密文件的每一个节点，并确定与提取的每一个节点对应的第二进制格式的字符，将确定的字符组成第二进制格式的第二字符串；

[122] 所述转换模块20还用于：

[123] 对所述第二字符串进行第一进制格式转换，生成第一进制格式的第三字符串，所述第三字符串中包含携带有所述标识字符的数字水印；

[124] 所述数字水印加密装置还包括：

[125] 获取模块40，用于查找所述第三字符串中包含的所述标识字符，并根据所述标识字符获取所述数字水印。

[126] 在本实施例中，要提取第一实施例中生成的加密文件所对应的数字水印时，首先处理模块30依次提取该加密文件的每一个节点，由于加密文件中的节点是根据第二进制格式的第一字符串中的每一位字符进行相应处理过的，因此，根据提取的节点，可确定与提取的该节点对应的第二进制格式的字符。在依次确定出与提取的每一个节点对应的第二进制格式的字符之后，将确定的第二进制格式的字符组成第二进制格式的第二字符串，该第二字符串中包含了第二进制格式的第一字符串。

[127] 之后，转换模块20对第二进制格式的该第二字符串进行第一进制格式转换，生

成第一进制格式的第三字符串。在对第二字符串进行第一进制格式转换时，也即对第二进制格式的第一字符串进行了第一进制格式转换，而第一字符串进行第一进制格式转换之后会生成携带有标识字符的数字水印，也即第三字符串中包含了携带有标识字符的数字水印。获取模块40从该第三字符串中查找出该标识字符，当查找到该标识字符时，根据该标识字符，获取到数字水印。

[128] 可选地，若在对待加密文件进行数字水印加密的过程中，标识模块10在数字水印的头部位置和尾部位置添加了标识字符，则生成的第三字符串中包含有两个标识字符。此时，如图6所示，所述获取模块40包括：

[129] 查找单元41，用于查找所述第三字符串中包含的两个所述标识字符；

[130] 获取单元42，用于提取两个所述标识字符之间的字符信息，所述字符信息为所述数字水印。

[131] 当生成第三字符串后，查找单元41从第三字符串中查找出其包含的两个标识字符，然后获取单元42提取出该两个标识字符之间的字符信息，该字符信息即为待加密文件在进行数字水印加密时所采用的数字水印，也即实现了从加密文件中提取出数字水印。

[132] 本实施例提供的方案，要提取加密文件所对应的数字水印时，首先处理模块30依次提取该加密文件的每一个节点，并确定与提取的每一个节点对应的第二进制格式的字符，将确定的字符组成第二进制格式的第二字符串，然后转换模块20对该第二字符串进行第一进制格式转换，生成第一进制格式的第三字符串，该第三字符串中就包含携带有标识字符的数字水印，获取模块40从第三字符串中查找出标识字符后，根据标识字符获取到数字水印，因此，本实施例的方案不仅实现了数字水印加密，而且还实现了加密文件的数字水印提取。

[133] 以上仅为本发明的优选实施例，并非因此限制本发明的专利范围，凡是利用本发明说明书及附图内容所作的等效结构或等效流程变换，或直接或间接运用在其它相关的技术领域，均同理包括在本发明的专利保护范围内。

权利要求书

[权利要求 1] 一种数字水印加密方法，其特征在于，所述数字水印加密方法包括步骤：

将数字水印添加预设的标识字符，以对所述数字水印进行标识处理，其中，所述数字水印为第一进制格式；

将标识处理后的所述数字水印进行第二进制格式转换，生成所述数字水印对应的第二进制格式的第一字符串；

按照预设顺序依次提取所述第一字符串中的每一位字符，并根据每次提取的字符，依次对待加密文件中与提取的所述字符对应的节点执行相应处理，生成所述待加密文件对应的加密文件，其中，所述待加密文件包括多个节点；

依次提取所述加密文件的每一个节点，并确定与提取的每一个节点对应的第二进制格式的字符，将确定的字符组成第二进制格式的第二字符串；

对所述第二字符串进行第一进制格式转换，生成第一进制格式的第三字符串，所述第三字符串中包含携带有所述标识字符的数字水印；

查找所述第三字符串中包含的所述标识字符，并根据所述标识字符获取所述数字水印。

[权利要求 2] 如权利要求1所述的数字水印加密方法，其特征在于，所述查找所述第三字符串中包含的所述标识字符，并根据所述标识字符获取所述数字水印的步骤包括：

查找所述第三字符串中包含的两个所述标识字符；

提取两个所述标识字符之间的字符信息，所述字符信息为所述数字水印。

[权利要求 3] 一种数字水印加密方法，其特征在于，所述数字水印加密方法包括步骤：

将数字水印添加预设的标识字符，以对所述数字水印进行标识处

理，其中，所述数字水印为第一进制格式；

将标识处理后的所述数字水印进行第二进制格式转换，生成所述数字水印对应的第二进制格式的第一字符串；

按照预设顺序依次提取所述第一字符串中的每一位字符，并根据每次提取的字符，依次对待加密文件中与提取的所述字符对应的节点执行相应处理，生成所述待加密文件对应的加密文件，其中，所述待加密文件包括多个节点。

[权利要求 4] 如权利要求3所述的数字水印加密方法，其特征在于，当所述第二进制格式为二进制格式时，所述按照预设顺序依次提取所述第一字符串中的每一位字符，并根据每次提取的字符，依次对待加密文件中与提取的所述字符对应的节点执行相应处理的步骤包括：

按照预设顺序依次提取二进制格式的所述第一字符串中的每一位字符；

若当前提取的所述字符为二进制字符0，则维持所述待加密文件中与当前提取的所述字符对应的节点不变；

若当前提取的所述字符为二进制字符1，则在所述待加密文件中与当前提取的所述字符对应的节点的尾部位置添加一位空格字符。

[权利要求 5] 如权利要求4所述的数字水印加密方法，其特征在于，所述依次对待加密文件中与提取的所述字符对应的节点执行相应处理，生成所述待加密文件对应的加密文件的步骤之后，还包括：

依次提取所述加密文件的每一个节点，并确定与提取的每一个节点对应的第二进制格式的字符，将确定的字符组成第二进制格式的第二字符串；

对所述第二字符串进行第一进制格式转换，生成第一进制格式的第三字符串，所述第三字符串中包含携带有所述标识字符的数字水印；

查找所述第三字符串中包含的所述标识字符，并根据所述标识字符获取所述数字水印。

[权利要求 6] 如权利要求3所述的数字水印加密方法，其特征在于，所述将数字水印添加预设的标识字符的步骤包括：

在所述数字水印的头部位置和尾部位置添加所述标识字符。

[权利要求 7] 如权利要求6所述的数字水印加密方法，其特征在于，所述依次对待加密文件中与提取的所述字符对应的节点执行相应处理，生成所述待加密文件对应的加密文件的步骤之后，还包括：

依次提取所述加密文件的每一个节点，并确定与提取的每一个节点对应的第二进制格式的字符，将确定的字符组成第二进制格式的第二字符串；

对所述第二字符串进行第一进制格式转换，生成第一进制格式的第三字符串，所述第三字符串中包含携带有所述标识字符的数字水印；

查找所述第三字符串中包含的所述标识字符，并根据所述标识字符获取所述数字水印。

[权利要求 8] 如权利要求6所述的数字水印加密方法，其特征在于，当所述第二进制格式为二进制格式时，所述按照预设顺序依次提取所述第一字符串中的每一位字符，并根据每次提取的字符，依次对待加密文件中与提取的所述字符对应的节点执行相应处理的步骤包括：

按照预设顺序依次提取二进制格式的所述第一字符串中的每一位字符；

若当前提取的所述字符为二进制字符0，则维持所述待加密文件中与当前提取的所述字符对应的节点不变；

若当前提取的所述字符为二进制字符1，则在所述待加密文件中与当前提取的所述字符对应的节点的尾部位置添加一位空格字符。

[权利要求 9] 如权利要求8所述的数字水印加密方法，其特征在于，所述依次对待加密文件中与提取的所述字符对应的节点执行相应处理，生成所述待加密文件对应的加密文件的步骤之后，还包括：

依次提取所述加密文件的每一个节点，并确定与提取的每一个节

点对应的第二进制格式的字符，将确定的字符组成第二进制格式的第二字符串；

对所述第二字符串进行第一进制格式转换，生成第一进制格式的第三字符串，所述第三字符串中包含携带有所述标识字符的数字水印；

查找所述第三字符串中包含的所述标识字符，并根据所述标识字符获取所述数字水印。

[权利要求 10] 如权利要求9所述的数字水印加密方法，其特征在于，所述查找所述第三字符串中包含的所述标识字符，并根据所述标识字符获取所述数字水印的步骤包括：

查找所述第三字符串中包含的两个所述标识字符；

提取两个所述标识字符之间的字符信息，所述字符信息为所述数字水印。

[权利要求 11] 一种数字水印加密装置，其特征在于，所述数字水印加密装置包括：

标识模块，用于将数字水印添加预设的标识字符，以对所述数字水印进行标识处理，其中，所述数字水印为第一进制格式；

转换模块，用于将标识处理后的所述数字水印进行第二进制格式转换，生成所述数字水印对应的第二进制格式的第一字符串；

处理模块，用于按照预设顺序依次提取所述第一字符串中的每一位字符，并根据每次提取的字符，依次对待加密文件中与提取的所述字符对应的节点执行相应处理，生成所述待加密文件对应的加密文件，其中，所述待加密文件包括多个节点。

[权利要求 12] 如权利要求11所述的数字水印加密装置，其特征在于，当所述第二进制格式为二进制格式时，所述处理模块包括：

提取单元，用于按照预设顺序依次提取二进制格式的所述第一字符串中的每一位字符；

处理单元，用于若当前提取的所述字符为二进制字符0，则维持所

述待加密文件中与当前提取的所述字符对应的节点不变；若当前提取的所述字符为二进制字符1，则在所述待加密文件中与当前提取的所述字符对应的节点的尾部位置添加一位空格字符。

[权利要求 13] 如权利要求12所述的数字水印加密装置，其特征在于，所述处理模块，还用于依次提取所述加密文件的每一个节点，并确定与提取的每一个节点对应的第二进制格式的字符，将确定的字符组成第二进制格式的第二字符串；

所述转换模块，还用于对所述第二字符串进行第一进制格式转换，生成第一进制格式的第三字符串，所述第三字符串中包含携带有所述标识字符的数字水印；

所述数字水印加密装置还包括：

获取模块，用于查找所述第三字符串中包含的所述标识字符，并根据所述标识字符获取所述数字水印。

[权利要求 14] 如权利要求11所述的数字水印加密装置，其特征在于，所述标识模块用于：

在所述数字水印的头部位置和尾部位置添加所述标识字符。

[权利要求 15] 如权利要求14所述的数字水印加密装置，其特征在于，所述处理模块，还用于依次提取所述加密文件的每一个节点，并确定与提取的每一个节点对应的第二进制格式的字符，将确定的字符组成第二进制格式的第二字符串；

所述转换模块，还用于对所述第二字符串进行第一进制格式转换，生成第一进制格式的第三字符串，所述第三字符串中包含携带有所述标识字符的数字水印；

所述数字水印加密装置还包括：

获取模块，用于查找所述第三字符串中包含的所述标识字符，并根据所述标识字符获取所述数字水印。

[权利要求 16] 如权利要求14所述的数字水印加密装置，其特征在于，当所述第二进制格式为二进制格式时，所述处理模块包括：

提取单元，用于按照预设顺序依次提取二进制格式的所述第一字符串中的每一位字符；

处理单元，用于若当前提取的所述字符为二进制字符0，则维持所述待加密文件中与当前提取的所述字符对应的节点不变；若当前提取的所述字符为二进制字符1，则在所述待加密文件中与当前提取的所述字符对应的节点的尾部位置添加一位空格字符。

[权利要求 17] 如权利要求16所述的数字水印加密装置，其特征在于，所述处理模块，还用于依次提取所述加密文件的每一个节点，并确定与提取的每一个节点对应的第二进制格式的字符，将确定的字符组成第二进制格式的第二字符串；

所述转换模块，还用于对所述第二字符串进行第一进制格式转换，生成第一进制格式的第三字符串，所述第三字符串中包含携带有所述标识字符的数字水印；

所述数字水印加密装置还包括：

获取模块，用于查找所述第三字符串中包含的所述标识字符，并根据所述标识字符获取所述数字水印。

[权利要求 18] 如权利要求17所述的数字水印加密装置，其特征在于，所述获取模块包括：

查找单元，用于查找所述第三字符串中包含的两个所述标识字符；

获取单元，用于提取两个所述标识字符之间的字符信息，所述字符信息为所述数字水印。

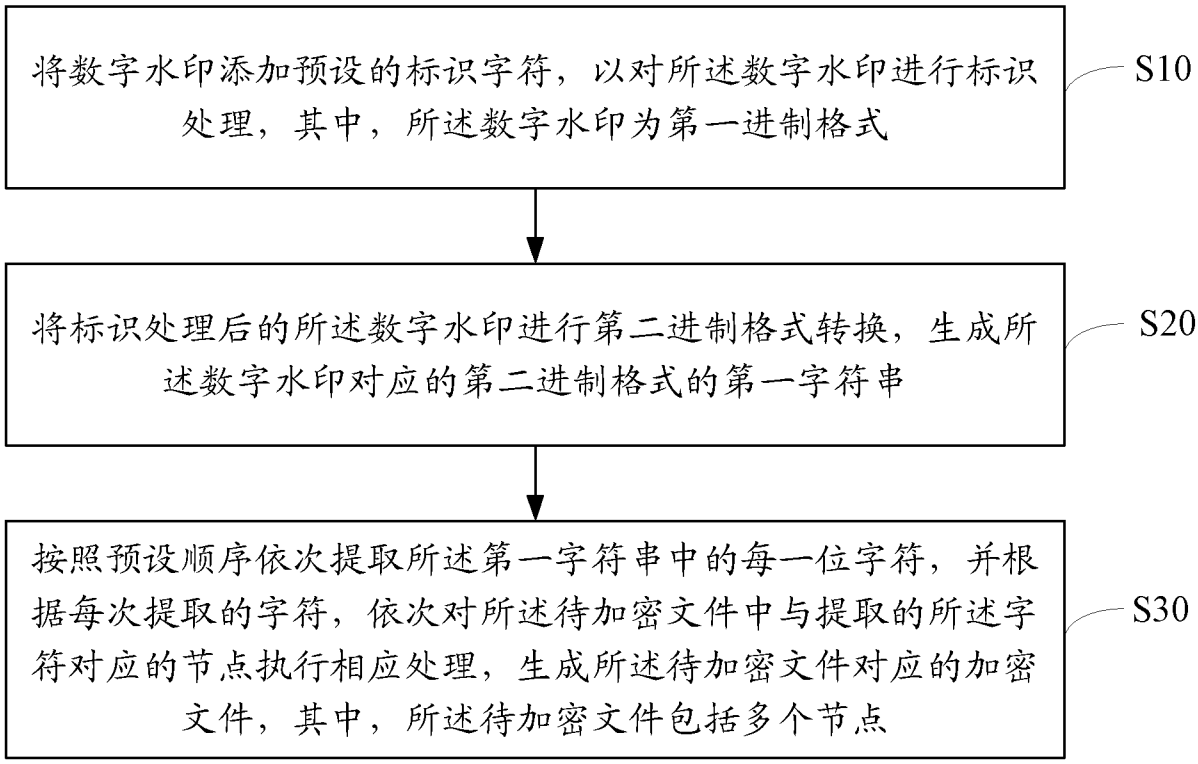
将数字水印添加预设的标识字符，以对所述数字水印进行标识处理，其中，所述数字水印为第一进制格式
S10
将标识处理后的所述数字水印进行第二进制格式转换，生成所述数字水印对应的第二进制格式的第一字符串
S20
按照预设顺序依次提取所述第一字符串中的每一位字符，并根据每次提取的字符，依次对所述待加密文件中与提取的所述字符对应的节点执行相应处理，生成所述待加密文件对应的加密文件，其中，所述待加密文件包括多个节点
S30

图 1

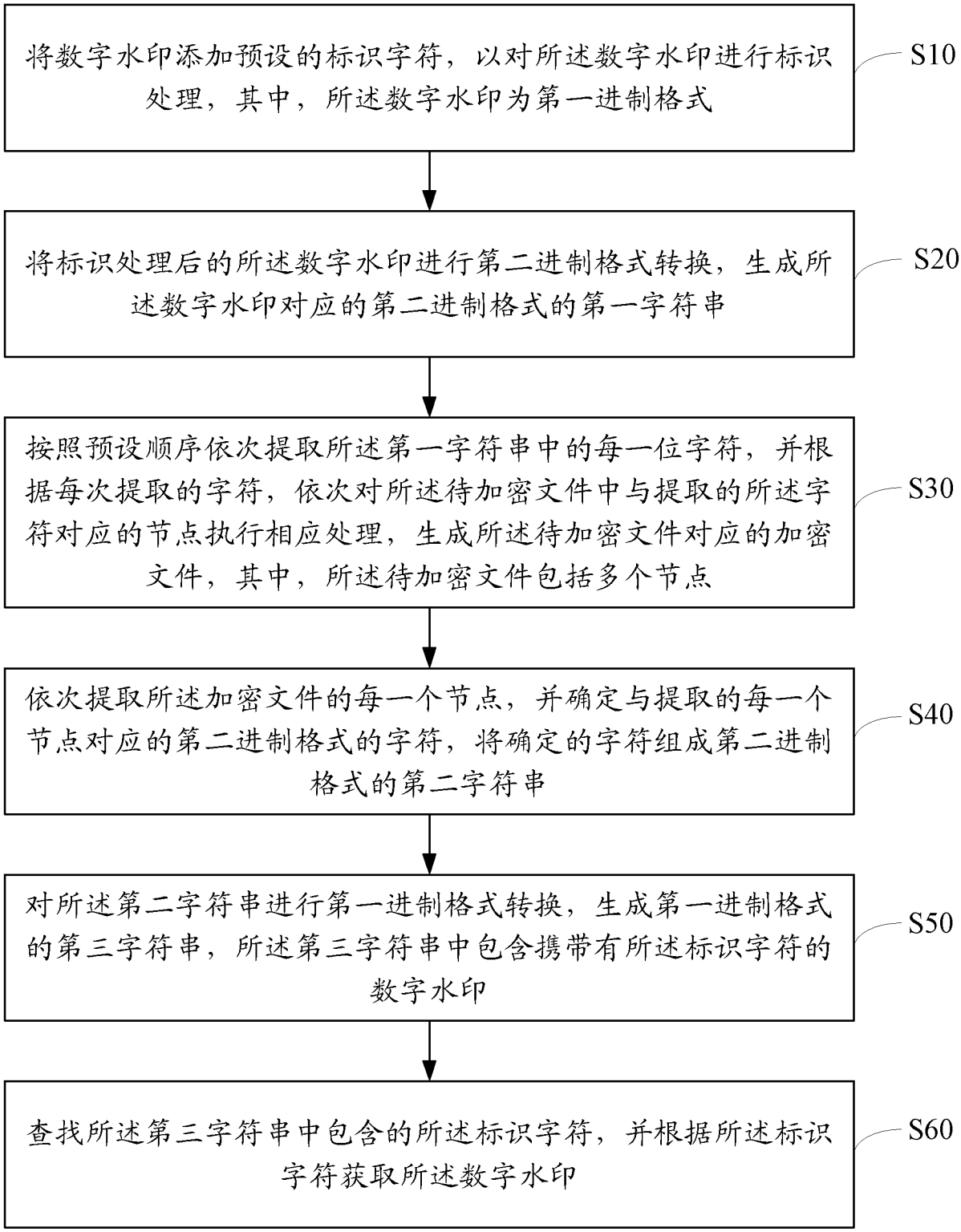
将数字水印添加预设的标识字符，以对所述数字水印进行标识处理，其中，所述数字水印为第一进制格式
S10
将标识处理后的所述数字水印进行第二进制格式转换，生成所述数字水印对应的第二进制格式的第一字符串
S20
按照预设顺序依次提取所述第一字符串中的每一位字符，并根据每次提取的字符，依次对所述待加密文件中与提取的所述字符对应的节点执行相应处理，生成所述待加密文件对应的加密文件，其中，所述待加密文件包括多个节点
S30
依次提取所述加密文件的每一个节点，并确定与提取的每一个节点对应的第二进制格式的字符，将确定的字符组成第二进制格式的第二字符串
S40
对所述第二字符串进行第一进制格式转换，生成第一进制格式的第三字符串，所述第三字符串中包含携带有所述标识字符的数字水印
S50
查找所述第三字符串中包含的所述标识字符，并根据所述标识字符获取所述数字水印
S60

图 2

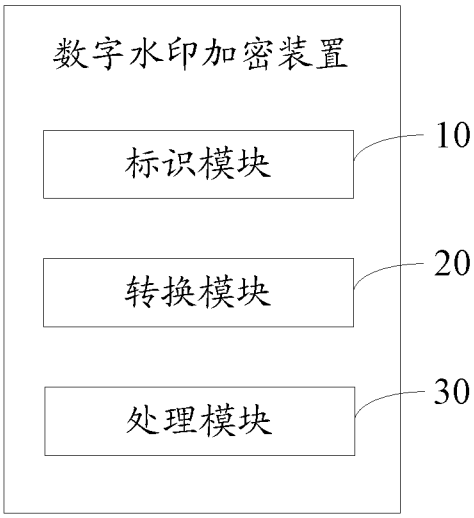

图 3

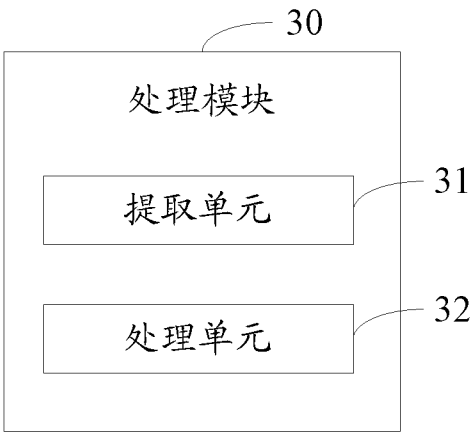

图 4

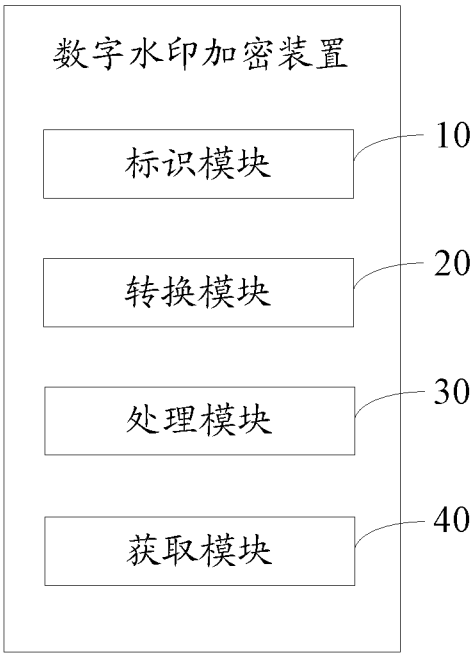
数字水印加密装置
标识模块
10
转换模块
20
处理模块
30
获取模块
40

图 5

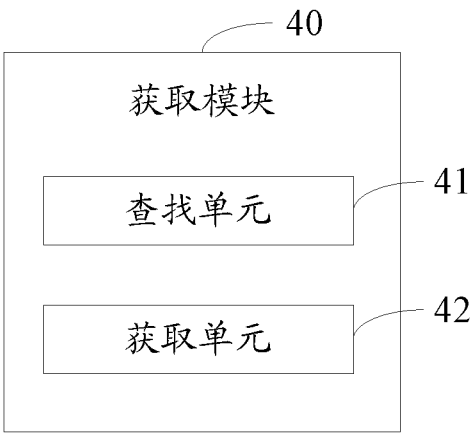
40
获取模块
查找单元
41
获取单元
42

图 6

INTERNATIONAL SEARCH REPORT

International application No.
PCT/CN2016/112858

A. CLASSIFICATION OF SUBJECT MATTER

G06T 1/00 (2006.01) i

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)

G06T, G06F, G06K

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)

CNPAT, CNKI, WPI, EPODOC, IEEE: 水印, 数字, 加密, 标识, 格式, 转换, 字符, 插入, 嵌入, 节点, watermark, digital, encrypt, identif+, format, conver+, character, embed+, insert, node

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	CN 104134023 A (BEIJING UNIVERSITY OF POSTS AND TELECOMMUNICATIONS), 05 November 2014 (05.11.2014), description, paragraphs 0060-0075, 0115-0125 and 0137	1-3, 6-7, 11, 14-15
X	CN 101751656 A (PEKING UNIVERSIT et al.), 23 June 2010 (23.06.2010), description, paragraphs 0060-0100	1-3, 6-7, 11, 14-15
X	CN 103873954 A (AISINO CORPORATION INC.), 18 June 2014 (18.06.2014), description, paragraphs 0043-0066	1-3, 6-7, 11, 14-15
A	US 20110243374 A1 (HUANG, H.J. et al.), 06 October 2011 (06.10.2011), entire document	1-18

☐ Further documents are listed in the continuation of Box C. ☒ See patent family annex.

* Special categories of cited documents:

"A" document defining the general state of the art which is not considered to be of particular relevance

"E" earlier application or patent but published on or after the international filing date

"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)

"O" document referring to an oral disclosure, use, exhibition or other means

"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art

"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
19 July 2017	02 August 2017
Name and mailing address of the ISA State Intellectual Property Office of the P. R. China No. 6, Xitucheng Road, Jimenqiao Haidian District, Beijing 100088, China Facsimile No. (86-10) 62019451	Authorized officer LI, Nan Telephone No. (86-10) 62413690

INTERNATIONAL SEARCH REPORT
Information on patent family members

International application No.
PCT/CN2016/112858

Patent Documents referred in the Report	Publication Date	Patent Family	Publication Date
CN 104134023 A	05 November 2014	None	
CN 101751656 A	23 June 2010	None	
CN 103873954 A	18 June 2014	None	
US 20110243374 A1	06 October 2011	TW 201135480 A	16 October 2011

国际检索报告

国际申请号
PCT/CN2016/112858

A. 主题的分类

G06T 1/00(2006.01)i

按照国际专利分类(IPC)或者同时按照国家分类和IPC两种分类

B. 检索领域

检索的最低限度文献(标明分类系统和分类号)

G06T, G06F, G06K

包含在检索领域中的除最低限度文献以外的检索文献

在国际检索时查阅的电子数据库(数据库的名称，和使用的检索词（如使用）)

CNPAT, CNKI, WPI, EPODOC, IEEE: 水印, 数字, 加密, 标识, 格式, 转换, 字符, 插入, 嵌入, 节点, watermark, digital, encrypt, identif+, format, conver+, character, embed+, insert, node

C. 相关文件

类 型*	引用文件，必要时，指明相关段落	相关的权利要求
X	CN 104134023 A (北京邮电大学) 2014年 11月 5日 (2014-11-05) 说明书第0060-0075，0115-0125，0137段	1-3，6-7，11，14-15
X	CN 101751656 A (北京大学 等) 2010年 6月 23日 (2010-06-23) 说明书第0060-0100段	1-3，6-7，11，14-15
X	CN 103873954 A (航天信息股份有限公司) 2014年 6月 18日 (2014-06-18) 说明书第0043-0066段	1-3，6-7，11，14-15
A	US 20110243374 A1 (HUANG, YING-JIEH 等) 2011年 10月 6日 (2011-10-06) 全文	1-18

☐ 其余文件在C栏的续页中列出。

☑ 见同族专利附件。

* 引用文件的具体类型：

"A" 认为不特别相关的表示了现有技术一般状态的文件

"E" 在国际申请日的当天或之后公布的在先申请或专利

"L" 可能对优先权要求构成怀疑的文件，或为确定另一篇引用文件的公布日而引用的或者因其他特殊理由而引用的文件（如具体说明的）

"O" 涉及口头公开、使用、展览或其他方式公开的文件

"P" 公布日先于国际申请日但迟于所要求的优先权日的文件

"T" 在申请日或优先权日之后公布，与申请不相抵触，但为了理解发明之理论或原理的在后文件

"X" 特别相关的文件，单独考虑该文件，认定要求保护的发明不是新颖的或不具有创造性

"Y" 特别相关的文件，当该文件与另一篇或者多篇该类文件结合并且这种结合对于本领域技术人员为显而易见时，要求保护的发明不具有创造性

"&" 同族专利的文件

国际检索实际完成的日期	国际检索报告邮寄日期
2017年 7月 19日	2017年 8月 2日

ISA/CN的名称和邮寄地址

中华人民共和国国家知识产权局(ISA/CN)
中国北京市海淀区蓟门桥西土城路6号 100088

传真号 (86-10)62019451

受权官员

李楠

电话号码 (86-10)62413690

国际检索报告
关于同族专利的信息

国际申请号
PCT/CN2016/112858

检索报告引用的专利文件			公布日（年/月/日）	同族专利			公布日（年/月/日）
CN	104134023	A	2014年 11月 5日	无			
CN	101751656	A	2010年 6月 23日	无			
CN	103873954	A	2014年 6月 18日	无			
US	20110243374	A1	2011年 10月 6日	TW	201135480	A	2011年 10月 16日