ICS 35.030
CCS L 80

中华人民共和国国家标准

GB/T 45909—2025

网络安全技术　数字水印技术实现指南

Cybersecurity technology—Implementation guideline of digital watermarking technology

2025-06-30 发布　　2026-01-01 实施

国家市场监督管理总局
国家标准化管理委员会　发布

目　　次

前　言

本文件按照GB/T 1.1—2020《标准化工作导则　第1部分：标准化文件的结构和起草规则》的规定起草。

请注意本文件的某些内容可能涉及专利。本文件的发布机构不承担识别专利的责任。

本文件由全国网络安全标准化技术委员会(SAC/TC 260)提出并归口。

本文件起草单位：阿里巴巴(北京)软件服务有限公司、阿里云计算有限公司、中国电子技术标准化研究院、北京快手科技有限公司、中国信息通信研究院、清华大学、亚信科技(成都)有限公司、蚂蚁科技集团股份有限公司、深信服科技股份有限公司、北京天融信网络安全技术有限公司、慧盾信息安全科技(苏州)股份有限公司、北京火山引擎科技有限公司、中国信息安全测评中心、国家信息技术安全研究中心、国家计算机网络应急技术处理协调中心、北京数安行科技有限公司、中国移动通信集团有限公司、合肥高维数据技术有限公司、公安部第三研究所、启明星辰信息技术集团股份有限公司、北京远鉴信息技术有限公司、杭州安恒信息技术股份有限公司、奇安信科技集团股份有限公司、杭州美创科技股份有限公司、杭州海康威视数字技术股份有限公司、深圳市联软科技股份有限公司。

本文件主要起草人：朱红儒、孙勇、孙巍巍、杨锐、周晨炜、徐羽佳、朱雪峰、落红卫、陈湉、曹京、景慧昀、金涛、徐恪、廖双晓、林冠辰、宋博韬、包英明、孟斌、连一汉、范航宇、孙明亮、杨韬、张晓娜、刘玉红、江为强、静静、郭玉刚、丁治国、周瑞群、郑榕、田丽丹、马勇、周杰、李超豪、宫小茜、王龑。

网络安全技术　数字水印技术实现指南

1　范围

本文件提供了数字水印技术的实现框架、功能、流程、水印算法选择、水印服务封装形式选择等方面的建议。

本文件适用于数字水印技术的设计、开发、应用和测试。

2　规范性引用文件

下列文件中的内容通过文中的规范性引用而构成本文件必不可少的条款。其中，注日期的引用文件，仅该日期对应的版本适用于本文件；不注日期的引用文件，其最新版本（包括所有的修改单）适用于本文件。

GB/T 25069　信息安全技术　术语

3　术语和定义

GB/T 25069 界定的以及下列术语和定义适用于本文件。

3.1

数字水印技术　digital watermarking technology

通过在数字内容中嵌入不易察觉的特定信息，标识或保护数字媒体的版权、来源或内容的信息安全技术。

注：简称数字水印，本文件所称“数字水印”是指隐式水印（也称“暗水印”“隐形水印”“隐性水印”“不可见水印”），其所嵌入的信息对数据使用者是隐蔽且不可辨识的。

3.2

水印信息　watermark information

通过数字水印技术（3.1）在数字媒体中嵌入的特定信息。

注：常见水印信息包括但不限于版权信息、溯源信息、链路信息、机构/员工标识符（ID）、时间信息等。

3.3

水印载体　watermark carrier

用于嵌入或携带水印信息（3.2）的文档、图像、音频、视频、网页、数据库等数字内容。

注：本文件中简称载体。

3.4

水印编码　watermark encoding

将水印信息（3.2）转换为适合嵌入到水印载体（3.3）的形式或格式。

3.5

水印解码　watermark decoding

将从水印载体（3.3）中提取出的水印信息（3.2）复原为其原始形式或格式。

3.6

水印嵌入　watermark embedding

将水印信息（3.2）嵌入到水印载体（3.3）中的过程。

3.7

水印提取　watermark extraction

从水印载体(3.3)中检测和识别水印信息(3.2)的过程。

3.8

失真干扰　distortion interference

水印载体(3.3)在传输、使用等过程中,因有意或无意的修改或处理,导致其携带的水印信息(3.2)质量下降、损坏或无法正常提取的现象。

3.9

水印攻击　watermark attack

有意试图破译、破坏、移除、修改、伪造水印载体(3.3)中水印信息(3.2)的行为。

注:包括但不限于对水印载体进行裁剪、形变、压缩、滤波、去噪、涂抹、拼接、提取破译等。

3.10

数字水印算法　digital watermarking algorithms

支撑数字水印技术(3.1)实现的方法,包括数字水印嵌入/提取算法和数字水印编码/解码算法。

3.11

增强型数字水印算法　enhanced digital watermarking algorithms

能够抵抗失真干扰(3.8)、防御水印攻击(3.9)的数字水印算法(3.10)。

4　缩略语

下列缩略语适用于本文件。

SaaS:软件即服务(Software as a Service)

SDK:软件开发工具包(Software Development Kit)

5　实现框架

数字水印技术实现涉及水印载体、数字水印算法、技术实现流程、水印服务封装等内容。本文件中数字水印技术所适用的水印载体包括文档、图像、音频、视频、网页、数据库等。数字水印算法主要有水印嵌入/提取算法、水印编码/解码算法等,常见数字水印算法见附录 A。技术实现流程主要有水印嵌入阶段、水印载体分发阶段、水印提取阶段。水印服务封装形式主要有 SDK、SaaS、产品等。数字水印技术主要应用在数据版权保护、数据泄露追踪溯源、生成式人工智能生成内容的水印标识、网络数据分类分级标识及管理、数据完整性保护等场景,典型安全场景见附录 B。数字水印技术实现框架如图 1 所示。

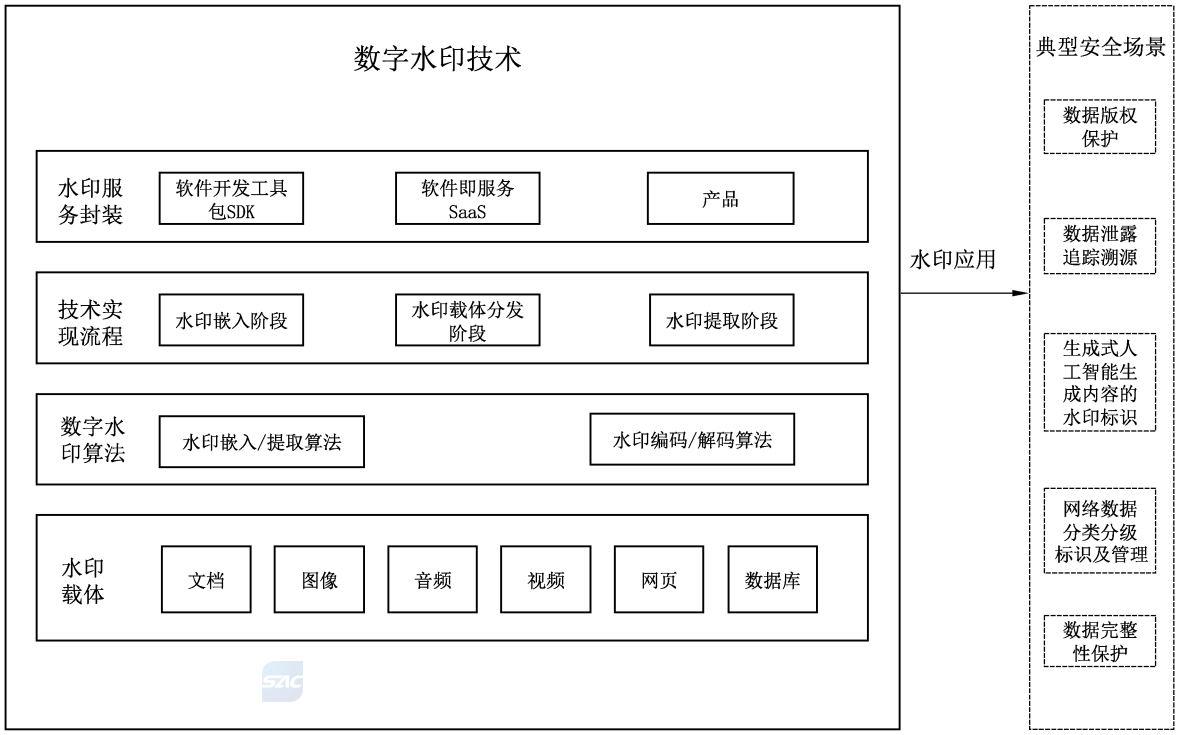

图 1　数字水印技术实现框架

6　功能

数字水印技术实现的功能分为：基本功能、增强功能和特定功能。水印技术功能实现情况判定方式见附录 C。

a）　基本功能指数字水印技术基本可用，能够达到预期目的：

1）　保证水印信息隐蔽：确保水印的存在难以被载体内容的使用者察觉，且水印信息无法通过视觉、听觉等直观感受识别。该功能是隐式水印与显式标识的本质区别；

2）　确保载体正常使用：确保嵌入水印的载体能够正常使用，并且完成预期功能和目的；

3）　支持水印信息提取：确保携带水印信息的载体在未受到任何失真干扰与水印攻击的情况下，水印信息能通过提取算法被完整提取。

b）　增强功能指水印载体在遭受失真干扰、水印攻击等情形下，数字水印技术仍然能够达到预期效果：

1）　防御水印攻击：通过构建数字水印安全模型的方式来保障水印信息的机密性、完整性和可用性，防范水印信息被监听、篡改和破坏，数字水印安全模型参考见附录 D；

2）　抵抗失真干扰：携带水印信息的水印载体在使用过程中，遭受格式转换、信道噪声、压缩等有损处理后，仍能通过对应的水印提取算法和水印解码算法准确地恢复出水印信息。

c）　特定功能指数字水印技术为满足特定应用场景下的需求所具备的功能：

1）　满足大容量需求：在对水印容量有较大需求的应用场景中，如版权保护、信息标注等，需考虑水印算法在目标载体上的信息嵌入量可满足对应的大容量需求，如为实现版权保护水印载体需要完整地携带对应的版权信息；

2）　满足实时性需求：在对水印嵌入或提取有较强实时性要求的应用场景中，水印算法的嵌入

或提取的效率需满足对应的实时性要求，例如在某些直播场景中，水印嵌入算法的时效性宜与直播流的帧率相匹配。

7 流程

7.1 概述

数字水印技术实现流程通常分为水印嵌入阶段、水印载体分发阶段和水印提取阶段，如图 2 所示。其中，水印嵌入阶段是将水印信息进行编码并通过合适的策略和算法嵌入到目标水印载体中的过程，包括嵌入方案设计及预处理、水印编码、水印嵌入等主要环节；水印载体分发阶段是将含水印载体分发至对应的目标受众或渠道的过程。在此过程中，水印载体易遭受失真干扰、水印攻击；水印提取阶段包括提取方案设计及预处理、水印提取、水印解码等主要环节。

注：水印提取阶段可能包含以下几种结果，一是水印提取完成并解码出正确的信息内容；二是水印提取完成但无法解码出有意义的信息内容，通常是乱码或是错误内容；三是水印无法提取或提取失败。仅第一种情况被认为是水印提取成功。

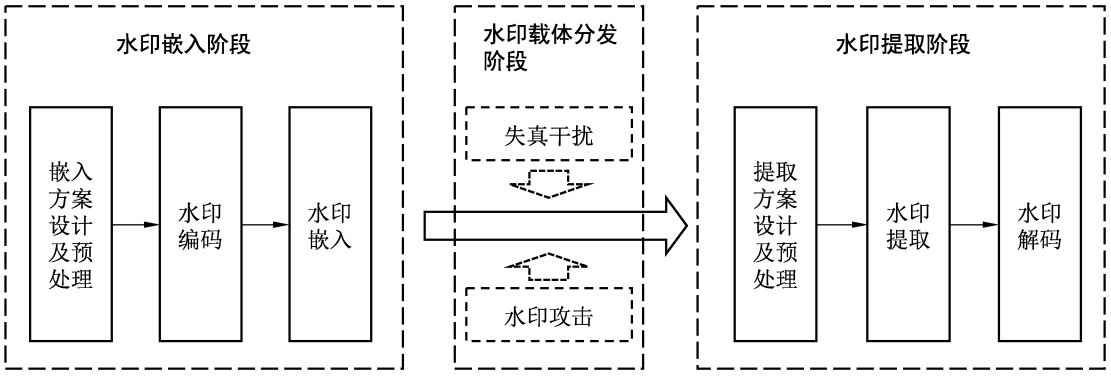

图 2 数字水印技术实现流程

7.2 水印嵌入阶段

7.2.1 嵌入方案设计及预处理

在此环节，首先明确数字水印的使用场景、待嵌入的水印信息及水印载体的基本特性，以确定拟实现的基本功能及特定功能。其次评估使用场景下潜在的失真干扰和水印攻击，确定拟实现的增强功能。最后根据上述评估结果对水印嵌入算法、水印编码算法等进行设计，并对水印载体和水印信息进行必要的初步处理。

a) 对水印嵌入方案进行设计时，需要考虑的因素包括但不限于：
   1) 载体的基本信息：包括但不限于载体类型、载体结构（如是否含有元数据等）、内容编码算法、封装格式、空域尺度信息（如图像的分辨率、位深等）、时序尺度信息（如视频的时长、帧率等）；
   2) 水印信息的类型及容量需求：水印信息的类型理论上可涵盖所有类型的数字内容，但常见的类型主要包括文本信息（如某公司版权所有、仅供某组织使用）、图像（如企业图标）等；水印的容量需求指在特定环境下能够完整携带水印信息的二进制流的长度，通常以“比特”为单位来衡量；
   3) 水印嵌入强度限制：即水印载体在水印嵌入过程中所允许的内容调整区域和调整幅度，该项因素通常与水印载体的类型及后续的使用场景有关，例如高清影视作品中允许的水印

嵌入强度通常会远小于在线直播视频的嵌入强度；

4） 防御水印攻击功能、抵抗失真干扰功能：即评估水印载体在后续的使用场景中可能会引入的失真干扰或水印攻击带来的破坏程度，如水印载体后续要通过社交网络进行传输，那么水印技术需抵抗此类传输所导致的失真干扰；

5） 实时性需求：即此应用场景对水印在嵌入和提取阶段所消耗时间的限制，通常对实时性有需求的场景包括高并发应用场景、流媒体场景等；

6） 提取准确率需求：水印的提取准确率宜尽可能接近100%；

注：在特殊情况下水印提取时，在不影响最终语义读取的前提下可能存在一定比率的错误，如企业图标图像水印。

7） 嵌入位置评估：一些内容或场景中，水印仅允许被嵌入在载体的指定或特定位置，或载体的部分区域不适合嵌入水印信息，如数据库载体中的个人身份证号码、银行卡余额等高敏感信息不宜用来嵌入水印。

b） 对水印载体和水印信息预处理时，需要考虑的因素包括但不限于：

1） 载体内容解析：将原始载体文件解析到水印嵌入算法可操作的层面，如在视频帧中嵌入水印，在预处理阶段对视频载体进行解帧；

2） 载体嵌入容量评估：即根据载体内容计算其在所设计的嵌入方案下的容量；

3） 水印信息数字化：将具有现实意义的水印信息构造为数字化表达的过程；

4） 水印信息映射：通过映射函数或映射表将水印信息进行合适变换的过程，例如，泄露溯源水印中通常并不会直接嵌入分发渠道的名称，而是将各个渠道映射成具有唯一性的ID信息；

5） 水印信息去冗余：对水印信息中的冗长部分进行精简的行为。

7.2.2 水印编码

在水印编码环节，根据水印的容量需求、实现功能等因素进行编码方案的选择。

a） 水印编码时，需要考虑的因素包括但不限于：

1） 水印信息机密性保护：主要以加密、扰动等方式实现；

2） 水印信息完整性验证：主要通过为水印信息添加校验码等方式实现；

3） 抗失真干扰：通过纠错编码、扩频编码、图形化编码、同步编码等方式实现，该因素的实现可能会损失部分水印容量；

4） 提升水印容量：通过压缩编码或保持二进制明文编码等方式实现，以最大化水印的有效载荷。

b） 文档、图像、音频、视频、网页、数据库等载体的水印编码算法选择见第8章。

7.2.3 水印嵌入

在水印嵌入环节，根据7.2.1的水印嵌入方案设计进行，选择合适的水印嵌入策略、水印嵌入算法，对编码后的水印信息进行嵌入。

a） 根据增强功能和特定功能等需求，进行嵌入策略的综合设计，常用的嵌入策略包括：

1） 全局嵌入：在原始载体的所有内容中嵌入水印信息；

2） 局部嵌入：仅选择在原始载体的一部分区域嵌入水印信息；

3） 周期嵌入：以空间或时间为周期，在原始载体中轮番、多次嵌入水印信息；

4） 定点嵌入：仅在原始载体中满足预设条件的位置嵌入水印信息；

5） 自适应嵌入：根据原始载体中各部分内容的不同，动态选择是否嵌入水印信息或动态调整水印的嵌入容量等。

b） 文档、图像、音频、视频、网页、数据库等载体的水印嵌入算法选择见第8章。

7.3 水印载体分发阶段

常见的含水印载体分发方式主要包括：

a） 统一分发：对于同一原始载体，向所有渠道和目标受众分发相同的含水印内容；

注 1：常用于版权水印、标签水印等场景。

b） 渠道分发：根据分发渠道或内容受众等的不同，在原始载体中嵌入不同的水印信息，再将对应的含水印载体分发至对应的渠道或投放给对应的内容受众。

注 2：失真干扰和水印攻击，都可能对水印载体及水印信息带来不同程度的损坏，导致水印提取阶段所获取的载体与之前分发阶段的载体存在差异。当此类差异过大时，即使存在抵抗失真干扰的设计，仍可能导致水印失效或无法提取。因此，数字水印技术有其局限性，水印载体也需尽量设计、分发至合适的场景才能起到理想的作用。

7.4 水印提取阶段

7.4.1 提取方案设计及预处理

在提取方案设计及预处理环节，首先根据水印嵌入算法来决定提取阶段的策略、参数等内容，其次评估含水印内容在分发及后续的使用中因失真干扰和水印攻击所引入的噪声对水印信息的影响，最后根据上述评估对水印提取算法、水印信息解码算法等进行设计，并对待提取的水印载体进行初步处理。

a） 对水印提取方案进行设计时，考虑的因素包括但不限于：

1） 水印嵌入算法：通常情况下，水印提取算法和水印嵌入算法存在互逆特性，因此设计水印提取算法时，水印嵌入算法是第一参考要素；

2） 载体的基本信息：由于失真干扰和水印攻击的存在，水印载体的基本信息可能已经改变，在水印提取算法设计时，需要重新考虑载体类型、载体结构、内容编码算法、封装格式、空域尺度信息、时序尺度信息等基本信息；

3） 水印嵌入的策略：水印的嵌入策略影响水印提取的区域和策略，如采用周期嵌入策略的载体，仅定位并提取出一个完整周期内的水印信息即可，不必提取整个载体中的水印；

4） 潜在的失真干扰和水印攻击类型：载体可能遭受的失真干扰或水印攻击类型多样，主要包括裁剪、压缩、缩放、旋转、拼接、遮挡、格式转换、涂抹、滤波、社交传输、截图、翻拍、翻录、水印擦除以及水印替换等操作。

b） 对含水印载体进行预处理时，考虑的因素包括但不限于：

1） 载体内容解析：将原始载体文件解析到水印嵌入算法可操作的层面，如在视频帧中嵌入的水印，在预处理阶段对视频载体进行解帧；

2） 含水印载体失真分析及矫正：即通过对载体的初步处理来评估载体是否经历裁剪、压缩、缩放等有损操作及预测对应操作的参数范围，并在必要时通过技术手段对已失真内容进行矫正，如对于扫描文档，需要去除文档无关背景，并将其矫正为原始尺寸。

7.4.2 水印提取

在水印提取环节，首先根据 7.4.1 的水印提取方案进行，选择合适的水印提取策略与水印提取算法，对水印载体进行解析及提取。

a） 水印提取策略与水印提取算法紧密相关，常见的水印提取策略包括：

1） 盲提取：不依赖原始载体内容，直接从含水印载体中提取水印信息；

2） 非盲提取：以全部或部分原始载体内容为参考才能进行水印信息的提取；

3） 全局提取：依次提取出载体内容中所有嵌入的水印信息；

4） 局部提取：定位到载体中含水印的部分并提取其中的水印信息，局部提取适用于局部嵌入

和定点嵌入的水印；

5） 单周期提取：在空间或时间等尺度上定位到水印的一个完整嵌入周期，并提取出该周期内的水印信息；

6） 多周期提取：定位到水印的多个嵌入周期，提取出其中的所有水印并综合获得最终的水印信息；

7） 自适应提取：根据载体中各部分内容的不同，动态选择是否提取水印信息或动态调整水印的提取参数等。

b） 文档、图像、音频、视频、网页、数据库等载体的水印提取算法选择见第 8 章。

7.4.3 水印解码

在水印解码环节，首先根据提取出的水印信息进行解密、分离校验码等各种解码，随后根据所提取的水印信息去验证水印信息的真伪与完整性。

a） 水印解码时考虑的因素包括但不限于：

1） 水印信息是否加密：若为加密信息，则进行解密操作；

2） 水印信息是否存在校验位：若存在，则分离出校验位，并判断校验信息是否正确；

3） 水印信息是否包含纠错编码：若包含，则对提取出的水印信息进行纠错；

4） 水印信息是否含有同步码：若含有，则定位同步码，并以同步码为起点定位出完整的水印信息周期；

5） 水印信息的其他编码方式：采用相应的解码方式进行还原；

6） 恢复出有实质意义的水印信息：对提取出的水印信息进行解码等相关操作。

b） 文档、图像、音频、视频、网页、数据库等载体的水印解码算法选择见第 8 章。

水印解码完成后，可通过提取出来的水印信息进行数据版权保护、数据泄露溯源等应用处理。

8 水印算法选择

8.1 概述

不同水印载体类型在结构和内容上存在共性和差异，载体中可利用的冗余空间及适用的水印嵌入/提取算法也因此存在较大异同。即使是在相同载体类型上，根据功能的差异，水印嵌入/提取算法的选择也存在明显差异。此外，根据载体类型和功能的差异，水印编码/解码算法的选择也存在较明显差异性。

8.2～8.7 根据水印载体的特性，针对不同类型的功能给出水印嵌入/提取算法和水印信息编码/解码算法的选择建议。当所设计的水印嵌入/提取算法和水印编码/解码算法同时满足多种类型的功能时，宜优先选择推荐算法的交集。常见水印嵌入/提取算法见 A.1，常见水印编码/解码算法见 A.2，常见水印编码/解码算法与主要类型水印载体的适配情况见 A.3。

注：通常情况下，水印的嵌入算法和提取算法对载体的操作存在较为明显的对称性和互逆性，且同属一类算法，故在本章中，将水印嵌入算法和提取算法归并为“水印嵌入/提取算法”进行阐述。同理，将水印信息编码算法和水印信息解码算法归并为“水印信息编码/解码算法”进行阐述。

8.2 文档

文档中的冗余空间与载体本身的特性有密切的联系，选择水印算法时宜结合水印的功能需求，以及载体的类型、结构、布局等情况进行综合判断。

a） 针对基本功能：

1） 水印嵌入/提取算法宜选择内容水印算法、深度学习水印算法，在文本载体拥有文件结构

和页面布局的情况下可选择元数据水印、不可感知元素水印等算法；

2） 水印编码/解码算法宜选择二进制明文编解码、扰动/加密编解码等算法，部分情况下可选择 A.2 中所述的其他所有编码/解码算法。

b） 在上述 a)的基础上，针对增强功能：

1） 水印嵌入/提取算法宜选择内容水印、深度学习水印和不可感知元素水印等算法；

2） 水印编码/解码算法宜选择扰动/加密编解码、纠错编解码、同步码、校验编解码、图形化编码、扩频编解码等算法。

c） 针对特定功能中的大容量需求：

1） 水印嵌入/提取算法宜选择不可感知元素水印算法等，或者在可行的情况下选择元数据水印、内容水印、不可感知元素水印算法进行组合使用；

2） 水印编码/解码算法宜选择二进制明文编解码、扰动/加密编解码、压缩编解码等算法等。

通常上述文档类水印技术涉及的水印嵌入/提取算法、水印编码/解码算法均能满足特定功能中的实时性需求。

8.3 图像

对于图像载体，元数据、像素空间域、变换域等都是较为常见且理想的水印嵌入位置。运用现代信息处理和编码等技术，能够找到这些矩阵中的视觉非敏感部分，从而用水印信息去替代这些部分内容，或者通过深度信号处理去发掘矩阵中的冗余空间来携带额外的水印信息。

a） 针对基本功能：

1） 水印嵌入/提取算法宜选择元数据水印、模板水印、变换域水印、直方图水印、最低有效位水印、分块调制水印、深度学习水印等算法，在图像拥有透明层等情况下可选用不可感知元素水印算法；

2） 水印编码/解码算法宜选择 A.2 所述所有编码/解码算法等。

b） 在 a)的基础上，针对增强功能：

1） 水印嵌入/提取算法宜选择模板水印、变换域水印、分块调制水印、深度学习水印和不可感知元素水印等；

2） 水印编码/解码算法宜选择扰动/加密编解码、纠错编解码、同步码、图形化编解码、扩频编解码和校验编解码等。

c） 针对特定功能中的大容量需求：

1） 水印嵌入/提取算法宜选择变换域水印、直方图水印、最低有效位水印或不可感知元素水印，或者在可行的情况下选择元数据水印、不可感知元素水印与模板水印、变换域水印、直方图水印、最低有效位水印中的一种或多种进行组合使用；

2） 水印编码/解码算法宜选择二进制明文编解码、扰动/加密编解码、压缩编码等算法等。

d） 针对特定功能中的实时性需求：

1） 水印嵌入/提取算法宜选择元数据水印、模板水印、不可感知元素水印、分块调制水印、最低有效位水印等；

2） 水印编码/解码算法宜选择二进制明文编码、扰动/加密编解码、纠错编解码和校验编解码等。

8.4 音频

对于音频载体，元数据、时序信号、变换域等都能够携带水印信息。

a） 针对基本功能：

1） 水印嵌入/提取算法宜选择元数据水印、时序水印、变换域水印、直方图水印、分块调制水

印、深度学习水印和最低有效位水印等算法；

2） 水印编码/解码算法宜选择 A.2 所述所有编码/解码算法等。

b） 在 a)的基础上，针对增强功能：

1） 水印嵌入/提取算法宜选择时序水印、变换域水印、分块调制水印、深度学习水印等；

2） 水印编码/解码算法宜选择扰动/加密编解码、纠错编解码、扩频编解码、图形化编解码、同步码和校验编解码等。

c） 针对特定功能中的大容量需求：

1） 水印嵌入/提取算法宜选择变换域水印、直方图水印、深度学习水印或最低有效位水印，或者在可行的情况下选择元数据水印与变换域水印、直方图水印或最低有效位水印中的一种或多种进行组合使用；

2） 水印编码/解码算法宜选择二进制明文编解码、扰动/加密编解码、压缩编解码等算法等。

d） 针对特定功能中的实时性需求：

1） 水印嵌入/提取算法宜选择元数据水印、分块调制水印、最低有效位水印等；

2） 水印编码/解码算法宜选择二进制明文编码、扰动/加密编解码、纠错编解码和校验编解码等。

8.5 视频

在选择视频水印算法时，主要考虑三个维度，首先，视频与图像在处理上有共性，视频的关键帧可视为独立图像，其元数据和视觉内容提供了潜在的水印空间。其次，视频的时间连续性和内部冗余为水印信息的嵌入提供了机会。最后，视频编码中的关键元素，如运动矢量和残差，也是嵌入水印的有效载体。

注：由于无损存储视频开销大，几乎所有常见的视频载体都是经过压缩编码的，例如 MPEG 和 H.26X 系列编码。因此，在考虑时序冗余空间时，视频编码的结构、时序的误差传递等特性需要考虑。

a） 针对基本功能：

1） 水印嵌入/提取算法宜选择元数据水印、模板水印、时序水印、变换域水印、直方图水印、分块调制水印、深度学习水印和最低有效位水印等；

2） 水印编码/解码算法宜选择 A.2 所述所有编码/解码算法等。

b） 在 a)的基础上，针对增强功能：

1） 水印嵌入/提取算法宜选择模板水印、变换域水印、分块调制水印、深度学习水印和时序水印等；

2） 水印编码/解码算法宜选择扰动/加密编解码、纠错编解码、图形化编解码、扩频编解码、同步码和校验编解码等。

c） 针对特定功能中的大容量需求：

1） 水印嵌入/提取算法宜选择变换域水印、直方图水印、深度学习水印或最低有效位水印，或者在可行的情况下选择元数据水印与模板水印、变换域水印、直方图水印、最低有效位水印中的一种或多种进行组合使用；

2） 水印编码/解码算法宜选择二进制明文编解码、扰动/加密编解码等算法等。

d） 针对特定功能中实时性需求：

1） 水印嵌入/提取算法宜选择元数据水印、模板水印、最低有效位水印、分块调制水印、深度学习水印等；

2） 水印编码/解码算法宜选择二进制明文编码、扰动/加密编解码、纠错编解码和校验编解码等。

8.6 网页

对于网页内容的各个组成部分来说，可依据其内容形式、结构、动态变换等特性进行水印的添加。

注：由于网页内容可能包含视频、音频、图像等几乎所有模态的多媒体内容，为避免描述的重复和冗余，本章节所推荐的适用于网页的相关算法仅指代整体网页渲染页面或网页源码，不包含网页中视频、音频、图像等多媒体内容本身所适用的算法。

a) 针对基本功能：
   1) 水印嵌入/提取算法宜选择模板水印、深度学习水印和内容水印等算法，存在时序内容的动态网页，且支持时序记录的情况下，宜选择时序水印算法，在以网页源码或页面文本为提取对象时，宜选择不可感知元素水印算法；
   2) 水印编码/解码算法宜选择 A.2 所述所有编码/解码算法等。
b) 在 a)的基础上，针对增强功能：
   1) 水印嵌入/提取算法宜选择模板水印、内容水印、时序水印、深度学习水印和不可感知元素水印等；
   2) 水印编码/解码算法宜选择扰动/加密编解码、纠错编解码、同步码、扩频编解码、图形化编解码和校验编解码等。
c) 针对特定功能中的大容量需求：
   1) 水印嵌入/提取算法宜选择内容水印或不可感知元素水印，或者在可行的情况下选择内容水印或不可感知元素水印相互组合使用；
   2) 水印编码/解码算法宜选择二进制明文编解码、压缩编码、扰动/加密编解码等算法等。
d) 针对特定功能中的实时性需求：
   1) 水印嵌入/提取算法宜选择模板水印和不可感知元素水印等；
   2) 水印编码/解码算法宜选择二进制明文编码、扰动/加密编解码、纠错编解码和校验编解码等。

8.7 数据库

数据库的主要形式是结构化数据库。数据库型水印设计宜考虑新增数据表的行/列、修改数据内容或附加不可见数据内容等策略。这些策略不可避免地会修改数据库中的数据，修改的幅度要根据实际情况选用。

注：数据库水印在开发设计时，宜避免对原始数据造成任何形式的更改或损害，若直接修改数据库中数据表的内容，可能会产生风险，如用户余额表中的数据不宜做任何改动，否则会造成直接经济纠纷。

a) 针对基本功能：
   1) 水印嵌入/提取算法宜选择内容水印、分块调制水印和不可感知元素水印等算法，在数据库含有元数据的情况下宜选择元数据水印算法，部分场景下宜选择最低有效位水印算法；
   2) 水印编码/解码算法宜选择 A.2 所述所有编码/解码算法等。
b) 在 a)的基础上，针对增强功能：
   1) 水印嵌入/提取算法宜选择内容水印、分块调制水印、不可感知元素水印等；
   2) 水印编码/解码算法宜选择扰动/加密编解码、纠错编解码、同步码、扩频编解码、图形化编解码和校验编解码等。
c) 针对特定功能中的大容量需求：
   1) 水印嵌入/提取算法宜选择内容水印、不可感知元素水印、最低有效位水印，或者在可行的情况下选择内容水印、不可感知元素水印、最低有效位水印进行组合使用；
   2) 水印编码/解码算法宜选择二进制明文编解码、压缩编码、扰动/加密编解码等算法等。
d) 针对特定功能中的实时性需求：
   1) 水印嵌入/提取算法宜选择元数据水印、内容水印、不可感知元素水印、分块调制水印、最低有效位水印等；

2） 水印编码/解码算法宜选择二进制明文编码、扰动/加密编解码、纠错编解码和校验编解码等。

9 水印服务封装形式选择

9.1 SDK 封装

在本地化或私有化部署的情况下，数字水印技术宜封装为 SDK 形式。采用单个 SDK 或多个独立 SDK 的方式宜侧重考虑整体性或灵活性。

如果侧重于整体性，宜封装为一个 SDK，通过 SDK 提供的多个不同接口提供水印嵌入、水印提取等服务；如果侧重于灵活性，宜封装为水印嵌入、水印提取等多个独立的 SDK，各 SDK 仅提供单一服务。

注 1：SDK 水印嵌入服务的输入接口包括水印载体、水印信息及各功能的控制参数等，输出接口包括嵌入水印信息的载体内容、服务状态等参数；SDK 水印提取服务的输入接口包括携带水印信息的载体、水印提取辅助信息等，输出接口包括水印信息等，部分水印算法（例如可逆水印）也会输出提取水印后的载体内容。若为单个 SDK 模式，输入接口除兼容上述的两类输入以外，接口数据还需包含算法的类型，即指定当前服务是嵌入还是提取。

注 2：SDK 具有较强的私密性，数字水印技术的使用者和服务方之间以技术模块交付为主要交流方式，无需进行数字载体及水印信息的传输和交互。

9.2 SaaS 封装

在远程部署或共享服务的情况下，数字水印技术宜封装为 SaaS 的形式。该服务模式下，水印的嵌入和提取等技术将封装成不同的服务接口。

注 1：SaaS 水印嵌入服务的输入接口包括水印载体、水印信息及各功能的控制参数等，输出接口包括嵌入水印信息的载体内容、服务状态等参数；SaaS 水印提取服务的输入接口包括携带水印信息的载体、水印提取辅助信息等，输出接口包括水印信息等，部分水印算法（例如可逆水印）也会输出提取水印后的载体内容。

注 2：SaaS 具备高度的便捷性，数字水印技术的使用者无需进行数字水印技术模块部署和维护，使用者和服务方之间以数据流形式进行数字载体和水印信息的输入输出。

9.3 产品封装

在本地化或私有化部署且面向业务人员使用的情况下，数据水印技术宜封装为产品形式。该模式下，水印的嵌入和提取等技术将转化为产品界面上直观的操作。

注 1：水印产品根据不同的应用场景，适配多样的水印载体、水印信息，同时支持算法选择及参数配置的灵活性。

注 2：产品具备高度的通用性和用户友好性，使得数字水印技术的使用者能够轻松地进行操作和配置，而无需深入了解背后的算法细节。服务提供方主要通过数字水印产品与使用者进行交流，使用者直接在产品界面上完成水印的嵌入和提取。

附 录 A
（资料性）
常见数字水印算法

A.1 水印嵌入/提取算法

常见的水印嵌入/提取算法包括但不限于：

a) 基于元数据的水印算法：利用内容载体在文件层面元数据中的空白位置、保留位置或者可替换位置添加水印信息；

b) 基于最低有效位的水印算法：通过修改图像、视频、音频等数据基本单元（例如像素点）的最低有效位嵌入水印信息；

c) 模板水印：将水印信息单独设计成小于或等于内容载体大小的模板，再将上述模板按照一定规律或编码逻辑叠加在载体上；

d) 直方图水印：基于直方图统计结果，通过直方图偏移进行水印信息的嵌入；

e) 变换域水印：通过将载体内容进行离散余弦变换（DCT）、离散傅里叶变换（DFT）、离散小波变换（DWT）等一种或多种可逆变换转换成变换域信号，再对变换域中一些合适的位置进行调制以达到嵌入水印的目的。由于对变换域的操作带来的视觉效果会被整个载体均匀分摊，变换域水印在一些场景下会拥有更好的隐蔽性；

f) 内容水印：通过载体内容层面对相同内容的不同表达来达到嵌入水印的目的，多用于文本类、音频类载体，例如，文档、网页等可编辑文本载体中，“我把梨子吃了”和“梨子被我吃了”可用来携带不同的水印信息；

g) 不可感知元素水印：指利用实际存在但是视觉、听觉等层面上不可感知的元素来携带水印信息的方法，例如，在文档中插入不可见字符或者透明图形元素等来携带水印信息；

h) 时序水印：基于原载体内容的时序冗余信息来进行水印嵌入的方法，通常适用于音频、视频等具有时序尺度的内容；

i) 分块调制水印：通过将载体内容进行分块或分组，再对分块或分组后的内容进行幅度、频率、色彩等不同形式的调制，以达到嵌入水印的目的；

j) 深度学习水印：通过深度神经网络来进行各模态水印嵌入和提取的技术，通常是通过大规模数据训练来实现的，主要包括传统嵌入、深度提取和端到端的深度嵌入、深度提取两种模式。

注：上述所列水印嵌入/提取算法是业界和学术界较为常用的算法类型，各算法并没有明确的边界，也并不在同一个划分维度，故部分算法之间可能存在一定的交集，例如一种算法可属于变换域水印，同时也属于直方图水印。在数字水印实现过程中，根据所推荐算法类型查阅相关学术或技术文档并结合具体应用场景来确定相关细节。

A.2 水印编码/解码算法

水印编码算法是指将待嵌入的水印信息转化成合适的二进制流的算法，常用的编码算法包括但不限于：

a) 二进制明文编码：一些对水印安全性要求较低的场景下，可直接将水印信息转换成二进制码流后进行嵌入；

b) 纠错编码：纠错编码主要用来提高水印的抗失真干扰，加入了纠错编码的水印信息在提取时候即使出现了若干的错误比特也可完整恢复出原始内容，不过纠错编码通常会带来水印内容膨胀，例如 64 比特水印信息进行纠错编码以后可能会变成 256 比特；

c) 加密/扰动编码：在一些高安全性要求的场景下，通过映射、扰动或者加密等操作来增加水印信息的抗攻击能力，加密宜采用 SM2/3/4 等国产商业密码实现，一些通用的流加密技术、位置扰动、映射表加密技术等编码技术都适用于此；

d) 校验编码：以一定的规则，通常是较为成熟的校验码算法，为水印信息生成可检验内容真实性的信息流，并将校验码与水印信息相互融合；

e) 扩频编码：对信息进行扩频调制，增加原始水印信息中每一比特的出现频率和次数，该编码方法以成倍的水印信息膨胀为代价来增加水印的鲁棒性；

f) 同步码：在一些噪声场景下，水印信息可能会面临着被裁剪或者截断的危险，这种场景下加入同步码可有效帮助寻找水印信息周期的起始位置；

g) 图形化编码：以图形的形式携带原水印信息；

h) 压缩编码：改变(通常是减少)水印信息的长度的编码方式。

水印解码算法是指从提取的水印码流中恢复出有实质意义水印信息的算法，通常来说是上述编码算法的逆过程。

A.3 常见水印算法与主要类型水印载体的适配情况

常见水印算法与主要类型水印载体的适配情况见表 A.1。

表 A.1 常见水印算法与主要类型水印载体的适配情况

算法类型	算法名称	文档	图像	音频	视频	网页	数据库
水印嵌入/提取算法	元数据水印	√	√	√	√	×	√
	模板水印	×	√	√	√	√	×
	时序水印	×	×	√	√	√	×
	变换域水印	×	√	√	√	×	×
	直方图水印	×	√	√	√	×	×
	最低有效位水印	×	√	√	√	×	√
	内容水印	√	×	×	×	√	√
	不可感知元素水印	√	√	×	√	√	√
	分块调制水印	×	√	√	√	×	√
	深度学习水印	√	√	×	√	√	×
水印编码/解码算法	二进制明文编码	√	√	√	√	√	√
	纠错编码	√	√	√	√	√	√
	加密/扰动编码	√	√	√	√	√	√
	校验编码	√	√	√	√	√	√
	扩频编码	√	√	√	√	√	√
	同步码	√	√	√	√	√	√
	图形化编码	√	√	√	√	√	√
	压缩编码	√	√	√	√	√	√
注：√表示适配，×表示不适配。							

附 录 B
（资料性）
典型安全场景

B.1 数据版权保护

数据版权保护场景主要是利用数字水印来保护数字内容的版权，在发生相关侵权行为的时候可利用数字水印来进行鉴权，以维护数字内容拥有者的合法权益，其主要场景如图 B.1 所示。

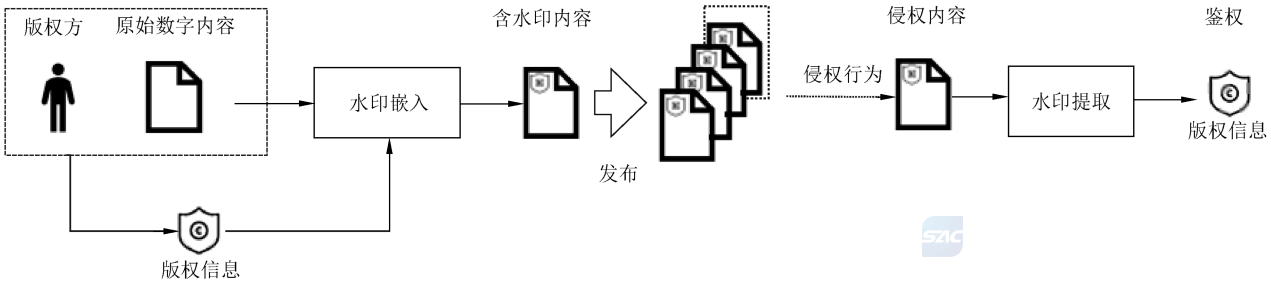

图 B.1 数字内容版权保护场景

在此场景中：

a) 版权方将版权信息以水印的形式嵌入到对应的原始数字内容中，获得含水印的数字内容后再进行发布和传播，其中，水印的嵌入可依赖第三方机构或者采用经认证的公开方法来完成；

b) 当含水印的数字内容在传播过程中遇到盗版、挪用等版权纠纷时，版权方可通过水印提取算法从对应的侵权内容中提取出版权信息，通过水印所表达的语义信息或通过第三方版权认证 & 管理机构判定版权归属，从而维护自身权益，达到版权保护的目的；

c) 数据版权保护场景中使用的版权信息可是经第三方机构认证的，该类版权信息通常是版权号、序列号等非自然语义信息，由第三方机构管理，该类版权信息通常适用于原始数字内容的水印容量较小的情况下，版权信息在提取出来以后，由第三方机构的参与来进行鉴权；

d) 在数据版权保护场景中，使用的版权信息可是明文水印内容，即直接嵌入具有明确版权声明的文本，如“×××有限公司版权所有”，这种明文水印适用于水印容量较大的情况，可嵌入完整的语言版权声明，在这种情况下，提取出的版权信息可直接用于验证和确认版权归属，无需复杂的解码过程。

B.2 数据泄露追踪溯源

数据泄露追踪溯源分为数据组织外泄露追踪溯源和数据组织内泄露追踪溯源。数据组织外泄露追踪溯源，指对数字内容分发过程中的泄露行为进行溯源，以求找到组织外部泄露的具体渠道方。数据组织内泄露追踪溯源，指对组织内数据处理过程中可能的外发、截屏、打印、复印、扫描、翻拍、翻录、录屏等泄露行为进行溯源，以求找到组织内部泄露的具体人员。其主要场景如图 B.2 所示。

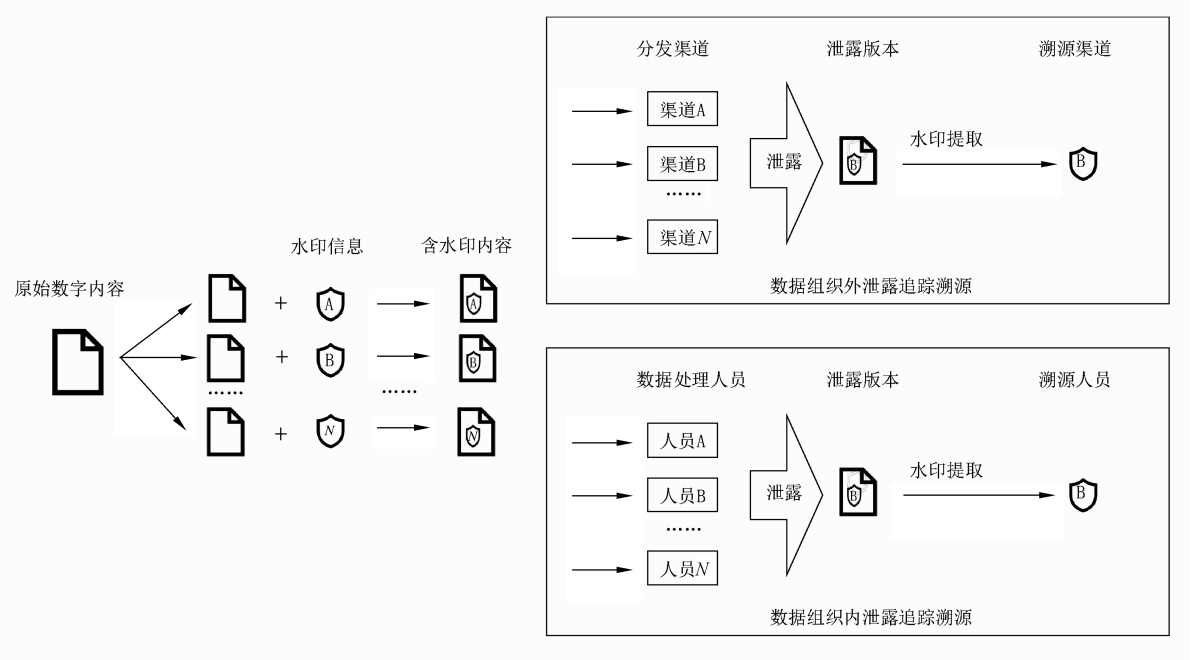

图 B.2　数据泄露追踪溯源场景

在此场景中：

a）　数字内容的拥有者会为所有溯源对象（分发渠道、数据处理人员等）设计各不相同的水印信息，并维护一个水印信息与溯源对象的映射关系，通常来说这样的映射关系是一一映射；

b）　在数据分发或数据处理前，原始数字内容会被拷贝成多份，并在每一份中嵌入各个溯源对象所对应的水印信息，从而获得携带不同水印的数字内容；

c）　在数据组织外泄露追踪溯源中，在数据分发后，水印信息不同的各版本数据将分别分发给各对应渠道以供其内部使用，如果某个渠道发生了数据泄露事件，在获取泄露版本后，内容拥有者可通过提取版本中对应的水印信息来定位到对应的泄露渠道，并根据需要来进行追责等处置；

d）　在数据组织内泄露追踪溯源中，在数据处理前，水印信息不同的各版本数据将分别提供给各数据处理人员以供其使用加工，一旦发生数据泄露事件，内容拥有者可通过分析泄露版本，提取出水印信息来定位到具体的内部人员，并据此采取相应的法律行动或内部管控措施。

B.3　生成式人工智能生成内容的水印标识

在生成式人工智能生成内容的水印标识场景中，数字水印被用以注明内容的生成源头等信息。该类应用场景中，数字水印以隐式水印标识方式标明该内容的服务提供者、内容 ID 等众多相关辅助信息。数字水印与生成式内容强绑定，具有携带水印信息容量大、不影响生成式内容二次加工等特点，给人工智能治理带来极大的便利。生成式人工智能生成内容的水印标识目前主要应用于图像、音频、视频等载体，其主要场景如图 B.3 所示。

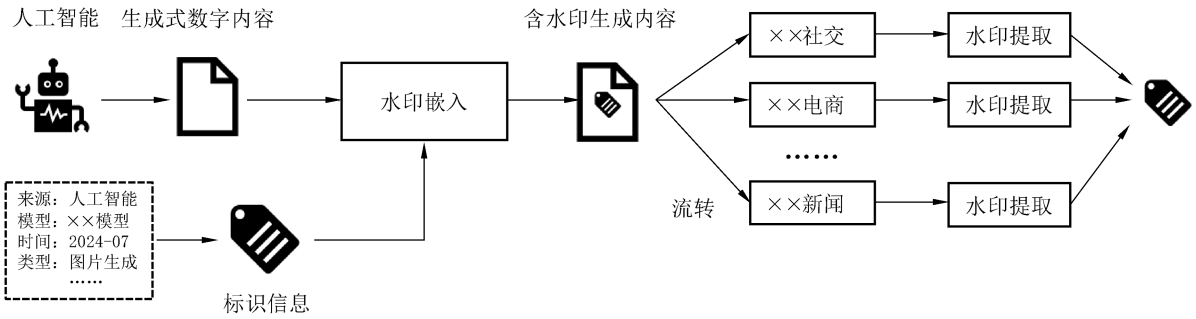

图 B.3 生成式人工智能生成内容的数字水印标识场景

在此场景中：

a) 生成式人工智能通过算法生成数字内容，包括但不限于图像、音频、视频等类型，随着人工智能技术的发展，此类内容已经达到以假乱真的程度；

b) 人工智能生成内容过程中涉及的相关信息将会被制作成标识信息，标识信息主要包括服务提供者名称，也可包括内容 ID 等其他内容；

c) 上述步骤 b)中所述标识信息以水印的形式被嵌入到上述步骤 a)中对应的生成式内容中，获得含水印的生成式内容，通常来说，该场景下所采用的水印技术宜选择常见的水印算法，以保证其通用可提取性，此后，含水印的生成式数字内容会被正常分发和流转；

d) 含水印的生成式数字内容在流转过程中可能被传播至多种目标受众，各目标受众通过提取内容中的水印信息来判断对应的内容来源。

B.4 网络数据分类分级标识及管理

网络数据分类分级标识及管理场景主要是利用不同的数字水印信息作为数字内容的数据分类分级标识。数字水印形式的标识可与对应的内容始终绑定在一起，无需借助多余的数据库、映射表等数据管理系统，因此具有极大的应用便捷性，其主要场景如图 B.4 所示。

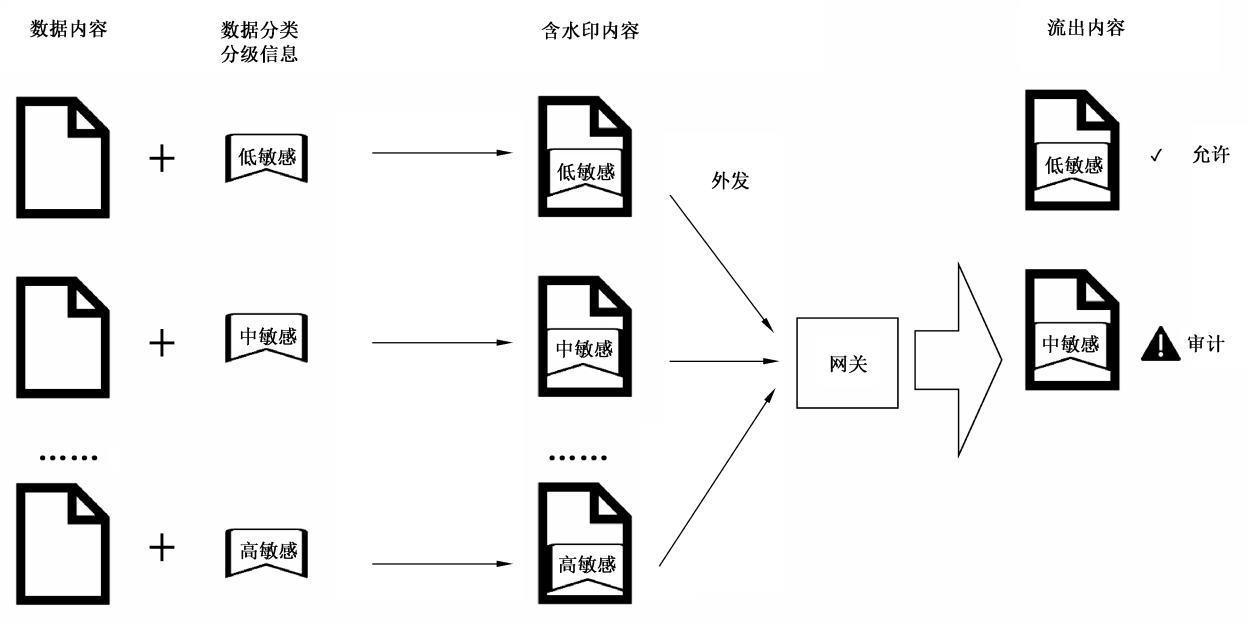

图 B.4 网络数据分类分级标识及管理场景

在此场景中：

a） 不同的数字内容经过数据分类分级系统获得对应的数据分类分级标识信息；

b） 上述数据分类分级标识信息以水印的形式被嵌入到对应的内容中，获得含有数据分类分级标识的数字内容；

c） 上述含水印内容在外发过程中，网关可通过提取水印获得该内容对应的数据分类分级信息，从而采取对应的安全措施，如拦截高敏感数据，仅发出中、低敏感数据，同时对中敏感数据进行安全审计。

B.5 数据完整性保护

数据完整性保护场景主要是利用易碎数字水印作为内容完整性的“鉴定器”。易碎数字水印又称脆弱数字水印，是一种特殊类型的数字水印技术，其特点是对载体内容的任何微小变化都极为敏感。这种水印的鲁棒性极低，但敏感性极高，意味着即使是最微小的修改，如格式转换、压缩或编辑，都可能导致水印的损坏，使其无法被提取或识别。其主要场景如图 B.5 所示。

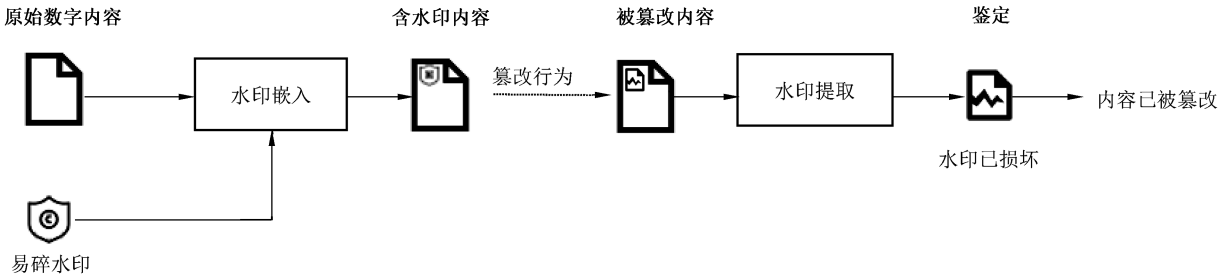

图 B.5 数据完整性保护场景

在此场景中：

a） 易碎水印被添加到受保护的原始数字内容中，获得含水印的数字内容；

b） 上述受完整性保护的含水印数字内容在传播过程中如果经历了删除、修改等攻击，其中嵌入的水印将会被破坏；

c） 内容接收者在获得内容后提取其中的易碎水印进行内容完整性鉴定，易碎水印被破坏的表现形式包括不限于提取失败、提取出的是乱码或空白信息等；

d） 若接收者发现上述水印被破坏的现象，则可鉴定出所接收数字内容的完整性已被破坏。

附 录 C
（资料性）
水印技术功能有效性评定方法

C.1 基本功能

基本功能有效性评定方法如下。

a） 保证水印信息隐蔽。根据算法适用的水印载体，选取典型样本进行水印的编码和嵌入，观察嵌入水印的样本，判断是否可察觉水印的存在。无法察觉则视为功能有效。

b） 确保载体正常使用。根据算法适用的水印载体，选取典型样本进行水印的编码和嵌入，使用正常方式打开嵌入水印的样本，判断是否影响正常使用。可正常打开且不影响正常使用则视为功能有效。

c） 支持水印信息提取。根据算法适用的水印载体，选取典型样本进行水印的编码和嵌入后，再进行水印的提取和解码，读取解码后的水印信息，判断是否可解读有实质意义的信息并与原始被编码信息一致。可解读有实质意义的信息，并且与原始被编码信息一致则视为功能有效。

C.2 增强功能

增强功能有效性评定方法如下。

a） 防御水印攻击。根据算法适用的水印载体，选取典型样本进行水印的编码和嵌入后，使用几何变换（如图像视频的缩放、裁剪、旋转、平移、仿射、透视；音频的频度缩放、裁剪、时长拉伸）、内容篡改（如拼接、替换、内容增删改）、信号处理（如图像视频亮度、对比度、滤波；音频均衡、滤波、降噪）和二次数字化（如打印、扫描、拍照、录屏、录音）等方法进行恶意攻击，再进行水印的提取和解码，读取解码后的水印信息，判断是否可解读有实质意义的信息并与原始被编码信息一致。可解读有实质意义的信息，并且与原始被编码信息一致的比例达到预期则视为功能有效。

b） 抵抗失真干扰。根据算法适用的水印载体，选取典型样本进行水印的编码和嵌入后，将水印载体选择常用压缩工具进行压缩后解压，使用常用社交工具进行传输后下载，再进行水印的提取和解码，读取解码后的水印信息，判断是否可解读有实质意义的信息并与原始被编码信息一致。可解读有实质意义的信息，并且与原始被编码信息一致的比例达到预期则视为功能有效。

C.3 特定功能

特定功能有效性评定方法如下。

a） 满足大容量需求。根据大容量水印信息场景需求，明确水印信息包含的具体容量长度，选取典型样本进行水印的编码和嵌入后，再进行水印的提取和解码，读取解码后的水印信息，判断是否可解读出需覆盖的水印内容。可完整解读出全部水印信息视为功能有效。

b） 满足实时性需求。根据场景需求，在实时业务过程中对样本进行水印的编码和嵌入后，再进行水印的提取和解码，读取解码后的水印信息，判断是否对实时业务产生不良影响。对实时业务不产生不良影响视为功能有效。

附 录 D
（资料性）
数字水印安全模型参考

D.1 概述

数字水印安全模型是一种安全框架，主要采用增强型数字水印算法，用于描述和分析数字水印技术在各种攻击和威胁下的安全性。数字水印安全模型旨在提高和评估数字水印技术中水印信息的机密性、完整性和可用性，防止水印信息被监听、篡改和破坏。

数字水印安全模型涵盖水印嵌入算法、水印编码算法、水印嵌入策略多个方面。通过选择合适的水印加密和校验等编码算法，提高水印信息的机密性和完整性；在设计水印嵌入策略时，采用周期嵌入、自适应嵌入等策略来提高水印的抗攻击能力，增强水印的完整性和可用性。另外，该模型避免采用元数据水印等安全性较弱的嵌入算法，以防止未经授权的访问和篡改。同时，通过攻击测试等方法，全面评估和改进数字水印技术的安全性。

数字水印安全模型主要涉及以下几个方面。

D.2 安全威胁

常见水印攻击主要针对水印载体进行裁剪、形变、压缩、滤波、去噪、涂抹、拼接、提取破译等操作，例如：裁剪攻击通过移除或修改包含水印信息的部分，导致水印信息不完整，影响其完整性和可用性；压缩攻击通过降低图像质量来损坏嵌入媒体中的水印信息，影响水印提取，损害其可用性；提取破译攻击通过分析嵌入算法来尝试解码水印信息，从而泄露原本应保密的数据，危及其机密性。这些攻击严重威胁着数字水印技术的安全性和可靠性。

D.3 安全目标

数字水印安全模型的安全目标如下：

a） 机密性：确保已嵌入载体中的水印信息不被未经授权的第三方获取或理解；

b） 完整性：确保已嵌入载体中的水印信息不被伪造、篡改，保持其内容的完整和真实；

c） 可用性：确保水印信息能够被合法的提取者准确提取和使用。

D.4 机密性保障

为了保障数字水印的机密性，数字水印安全模型需要采用水印编码算法和水印嵌入策略，在水印编码上，选择加密算法（如 SM4 或 SM2 等国产商用密码算法）对水印信息进行加密，即使水印被非法提取，也需要再通过解密才能获取原始内容；在水印嵌入策略上，宜采用随机化嵌入位置和强度的水印嵌入策略，显著增加了攻击者分析和破解水印信息的难度。如某视频网站在发布的视频中嵌入数字水印时，先使用 SM4 算法对水印信息进行加密，再使用伪随机序列来增加对每个视频帧中水印的嵌入位置和强度的扰动，这种方法不仅增加了水印的隐蔽性，也提高了破解难度，有效增强了数字水印的机密性。

D.5 完整性保障

为了保障数字水印的完整性，数字水印安全模型需要选择和设计合适的编码算法和嵌入策略。与数据安全常用技术类似，水印信息的完整性可依赖哈希校验、数字签名、数字证书来实现，并通过加密算法来进一步提高安全性。例如在编码阶段，以使用哈希函数（如 SM3 等国产商用密码算法）生成水印信息的摘要值，将其与水印一同嵌入到媒体内容中，当水印被提取出来时，能够通过重新计算水印信息的

摘要值并与嵌入时的摘要值对比，来验证水印是否被篡改。在嵌入策略上，可采用周期嵌入、自适应嵌入等，在一定程度上抵抗常见的物理攻击（如裁剪、压缩、滤波等），保证水印信息的稳定性和一致性。例如某音乐发行平台在发布音乐文件时，除了使用 SM3 算法生成并嵌入水印信息的摘要值外，还会在音乐文件的不同部分重复嵌入相同的水印信息（周期嵌入），即使部分水印信息受损，也能从其他部分恢复完整的水印信息，有效保护水印信息的完整性。

D.6 可用性保障

为了保障数字水印的可用性，数字水印技术在实现时宜充分考虑载体数字内容在生命周期内面对的失真干扰和水印攻击，尤其是在数字内容的传输和使用过程中。安全模型需要采用增强型数字水印算法和嵌入策略，确保水印信息在需要时能够被合法的提取者准确地提取和使用。在水印嵌入上，可使用抵御水印攻击和失真干扰的算法，避免使用元数据水印等易被篡改和破坏的算法。在嵌入策略上，可使用自适应嵌入等策略，根据媒体内容的特性（如纹理复杂度、边缘信息等）动态调整水印的嵌入强度和位置，确保水印在不影响媒体质量的同时保持较高的稳定性。例如某图片共享平台在用户上传的图片中嵌入数字水印时，在图像的多个频域层嵌入水印，并根据图像的纹理和颜色信息选择合适的嵌入位置和强度，即使图像经过压缩攻击，水印信息仍能被可靠提取，有效保障了数字水印的可用性。

D.7 测试与评估

为了评估数字水印安全模型的效果，宜从机密性保障、完整性保障和可用性保障三个方面进行详细测试。在机密性保障方面，通过提取破译等攻击测试，评估水印信息的加密强度，量化指标包括破解水印信息的成功率。在完整性保障方面，通过模拟常见的物理攻击（如裁剪、压缩、滤波等），使用哈希函数生成的摘要值进行比对，验证水印信息的完整性和一致性，量化指标包括水印信息的篡改检测率和哈希值匹配率。在可用性保障方面，通过模拟实际应用场景中的攻击（如压缩攻击、噪声干扰等），测试水印信息的提取效果，量化指标包括水印提取成功率。通过这些量化指标能够客观评估安全模型，并根据测试结果不断优化水印算法和嵌入策略，从而提高数字水印技术的整体安全性。