计算机系统应用 ISSN 1003-3254, CODEN CSAOBN
2025,34(4):64−75 [doi: 10.15888/j.cnki.csa.009808] [CSTR: 32024.14.csa.009808]

E-mail: csa@iscas.ac.cn
http://www.c-s-a.org.cn
Tel: +86-10-62661041

基于区块链的跨平台网络视频版权保护方案①

姚家鹏, 訾玲玲, 谢义莎

(重庆师范大学 计算机与信息科学学院, 重庆 401331)
通信作者: 姚家鹏, E-mail: yaojiapeng0120@163.com

摘　要: 随着网络视频平台 (network video platform, NVP) 应用, 网络视频在不同视频平台分享时常面临被侵权和跨平台版权检测问题, 所以本文提出了一种基于区块链跨平台网络视频版权保护方案 (blockchain-based cross-platform network video copyright protection scheme, BCVCP) 旨在通过区块链和利用生成的所有权序列 (ownership sequence, *OS*), 进行所有权序列检测, 来实现跨视频平台的网络视频版权保护. 本方案包括身份认证、提取关键帧、所有权序列的生成和检测、网络视频控制管理等部分. 具体来说, 在对网络视频上传或访问等操作之前, 需要进行身份认证, 确保身份信息的安全. 其次, 上传网络视频过程中会生成所有权序列, 存储在分布式节点中. 然后, 提取视频关键帧, 把生成的所有权序列嵌入到视频关键帧中. 最后, 调用智能合约进行跨平台所有权序列检测和对网络视频的传播控制管理, 避免侵权行为. 在实验中, 验证了跨视频平台传输网络视频时所有权编码质量和所有权识别的鲁棒性, 保护了网络视频的版权.

关键词: 区块链; 网络视频; 所有权序列; 版权保护; 跨视频平台

引用格式: 姚家鹏,訾玲玲,谢义莎.基于区块链的跨平台网络视频版权保护方案.计算机系统应用,2025,34(4):64–75. http://www.c-s-a.org.cn/1003-3254/9808.html

Blockchain-based Cross-platform Network Video Copyright Protection Scheme

YAO Jia-Peng, ZI Ling-Ling, XIE Yi-Sha

(College of Computer and Information Science, Chongqing Normal University, Chongqing 401331, China)

Abstract: With the application of network video platform (NVP), network videos often face copyright infringement and cross-platform copyright detection issues when shared across different video platforms. Therefore, this study proposes a blockchain-based cross-platform network video copyright protection scheme (BCVCP), which aims to protect network video copyrights across platforms by means of blockchain and through ownership sequence (*OS*) generation and detection. This study includes identity authentication, keyframe extraction, ownership sequence generation and detection, and network video control management. Specifically, before operations such as video uploading or access, identity authentication needs to be carried out to ensure identity information security. Secondly, during the process of uploading network videos, an ownership sequence is generated and stored in distributed nodes. Then, the keyframes of the video are extracted and the generated ownership sequence is embedded into these keyframes. Finally, smart contracts are invoked for cross-platform ownership sequence detection and network video dissemination management to avoid infringement behaviors. In the experiments, the robustness of ownership encoding quality and ownership recognition during cross-platform network video transmission is verified, thereby protecting the copyright of network videos.

Key words: blockchain; network video; ownership sequence (*OS*); copyright protection; cross-video platform

① 基金项目: 重庆市教育科学规划重点课题 (K22YE205098); 重庆师范大学博士启动基金 (21XLB030, 21XLB029)
收稿时间: 2024-09-20; 修改时间: 2024-10-21; 采用时间: 2024-11-01; csa 在线出版时间: 2025-02-18
CNKI 网络首发时间: 2025-02-19

随着国内互联网环境的不断优化以及 5G 技术的广泛应用, 视频用户的数量迅速增长, 网络视频平台 (network video platform, NVP) 规模也随之扩大. 然而, 伴随这一快速发展而来的, 是日益严重的视频侵权、盗窃等现象. 诸如盗用其他平台视频并在另外一个视频平台上上传和发表、肆意拼接他人视频[1]以及网络视频在这些平台之间的传播过程中出现了侵权的情况. 各平台之间的版权保护机制不兼容, 导致网络上盗版网络视频泛滥, 真实性难辨[2]. 在“抖音”“快手”“哔哩哔哩” 等网络视频平台检索“抄袭”“侵权”等关键词, 检索结果中不乏视频博主对自身视频被侵权现象的揭露, 数量之多, 方式之多样, 较监测数据更为严重, 所以未经授权的跨平台搬运现象屡见不鲜, 同时二次剪辑原创短视频、剽窃短视频创意等侵权行为也日益增多. 由于视频所有者多数活跃于一个或若干个平台, 无法进行全平台覆盖, 因此跨平台网络视频侵权行为更难被防止, 视频所有者常常经跨平台用户提醒后才发现自己的作品在其他平台被侵权[3]. 因此, 网络视频版权保护面临着巨大挑战. 传统方案中, 会利用区块链的不可篡改、可追溯特性, 采用多通道架构构建了视频版权保护系统, 升版权保护的透明性与安全性[4,5]. 或者通过相似视频检索算法验证视频的相似性、水印技术[6,7]和安全加密方法以及访问控制系统组成的组合方案, 实施版权授权管理, 确保版权的合法性[8]. 然而, 传统方案仅支持单一平台网络视频版权保护, 无法兼容跨平台版权保护.

本文提出一种基于区块链的跨平台网络视频版权保护方案 (blockchain-based cross-platform network video copyright protection scheme, BCVCP), 该方案的核心是它生成的所有权序列 (ownership sequence, *OS*), 是唯一的数字信息或标识, 这会嵌入到网络视频关键帧中, 保存在区块链中, 对视频版权进行检测. 每个视频在首次上传时, 都会生成一个独特的传播树, 与所有权序列一同创建. 传播树的根节点地址, 即由所有权序列指定, 代表视频的版权信息. 通过准确提取视频的所有权序列, 可以在对应传播树中精确定位到该视频, 防止侵权事件的发生. 使用智能合约在跨平台分享视频时进行控制. 为了应对跨视频平台传输过程中不可预测的噪声, 通过两阶段可分离的编码和解码 (two-stage separable encoding and decoding, TSED) 的噪声训练, 来增强所有权识别的鲁棒性. 本文的主要贡献可以概括如下.

(1) 本文提出 BCVCP, 通过区块链技术完成跨视频平台的网络视频版权检测, 主要分为身份认证、关键帧提取、所有权序列生成、所有权序列检测和网络视频分发控制管道.

(2) 在版权检测方案中, 提出了所有权序列检测方法. 视频所有者在上传网络视频时, 经过身份验证后生成所有者序列, 嵌入视频关键帧中, 实现所有权序列检测和网络视频版权保护.

(3) 在本方案的网络视频传播控制中, 使用了一系列智能合约来检测跨平台网络视频的所有权序列, 并对网络视频的传播控制进行管理.

(4) 通过在 TSED 中引入噪声, 测试版权检测过程中所有权编码的质量和所有权识别的鲁棒性, 验证 BCVCP 对不可预知操作的鲁棒性, 增强跨视频平台传输过程中对不可预知修改的抵御能力.

本文第 2 节回顾相关工作. 第 3 节详细介绍 BCVCP 的主要组成部分. 第 4 节给出实验. 第 5 节给出结论.

1 相关工作

1.1 区块链的版权保护

近年来, 国内外学者对基于区块链的版权保护进行了广泛研究. 研究者们鉴于区块链的透明性、不可篡改性和可靠性的特性, 提出基于区块链的版权保护. Guo 等[9]结合公有和私有区块链, 建立了一个在线教育多媒体资源数字版权管理系统, 侧重于安全存储和非中介验证. Garba 等[10]提出一个基于数字水印和可扩展区块链的分布式数字版权管理媒体交易框架, 仅允许授权用户使用在线内容. Chen 等[11]提出一种结合区块链分片技术的高安全、便捷的数字版权保护方案, 优化版权登记速度和系统性能. Cai 等[12]提出将区块链技术融入数字音乐版权保护和管理中, 在所有权、使用权和权利保护方面取得了令人满意的效果. Yang 等[13]提出了一种基于父子链的视频版权交易可追溯方法, 在私有区块链 (子链) 上记录可以唯一标识视频的视频可追溯源代码. Wang 等[14]提出了一种基于智能合约和感知哈希的版权保护数据交易方案, 防止非法转售, 确保公平交易. Zhao 等[15]通过以太坊应用程序 BMCProtector 来设计和构建, 是一个基于区块链的应用, 旨在保护音乐版权并确保创作者收益. 但是, 从上述的研究现状来

看, 大多都是通过区块链对版权的管理, 不能控制网络视频传播. 本文的方案中在实现网络视频版权保护的同时, 还能够通过智能合约管理网络视频以及对网络视频的传播控制.

1.2 网络视频版权保护

目前针对网络视频的版权检测主要方法有: 内容识别技术[16,17]、指纹识别技术[18]和数字水印技术[4]等. 首先是内容识别技术方面, Yang 等[19]和 Chen 等[20]利用内容识别技术, 提出基于视觉优先级规则的卷积神经网络算法和一种轻量级视频片段快速匹配算法, 能够精确定位原始视频内容. 但内容识别技术高度依赖于算法的准确性, 对于非常独特或少见的内容可能识别不准确. 其次是指纹识别技术, 这种技术通过提取视频内容的特定特征 (如图像帧的哈希值等) 来创建一个独特的“指纹”来识别版权. Agyekum 等[21]提出以数字指纹技术、星际文件系统 (IPFS) 和区块链技术为核心, 设计反映数字媒体文件特征的数字指纹. 但是对视频质量高度敏感, 视频压缩或格式转换可能导致指纹变化, 从而降低匹配精度. 最后是数字水印技术, 包括前文的介绍中也提到过. Sridhar 等[22]提出一种视频水印技术, 通过将水印图像重新整形并分为奇偶行, 对折叠后的图像进行单级分解后, 版权标记在中等级别的子频带上进行. Priya 等[23]提出了一种将细胞自动机变换和奇异值分解 (SVD) 相结合的数字视频水印版权保护方案. Resen 等[24]提出一种结合快速 Walsh-Hadamard 变换 (FWHT)、离散小波变换 (DWT) 和 Arnold 映射的视频水印技术, 实现安全的版权保护和盲提取. Liu 等[25]提出了一种保护视频版权的新型零水印方案, 利用对偶树复小波变换和离散余弦变换提高对转换和噪声的鲁棒性. 但是, 水印技术会降低视频内容的质量, 鲁棒性还不够, 视频处理技术可能会移除或损坏水印, 影响其可追踪性.

本文利用生成视频的所有权[26–28]序列, 用于网络视频的所有权识别检测版权. 在之前的序列研究中, de Jesus Vega-Hernandez 等[29]设计了一个视频序列空间和时间冗余的框架, 确保数字视频的所有权识别. Mandelli 等[30]提出从稳定视频序列中提取设备特征指纹, 然后将这些指纹与视频序列匹配, 解决视频稳定化技术带来的设备归属问题. 由此提出通过所有全序列来检测网络视频的版权, 它生成的原理基于 3 个核心: (1) 视频关键帧提取: 从视频中提取能够代表其内容的特征; (2) 唯一性保证: 结合视频特征和所有者信息, 生成一个独一无二的所有权序列; (3) 所有权明确化: 将所有者的标识信息整合到序列中, 确保任何时候都能追溯到视频的原始所有者.

2 方案

BCVCP 分为 5 个模块: 身份认证、关键帧提取、所有权序列生成、所有权序列检测和网络视频控制管理. 方案架构如图 1 所示.

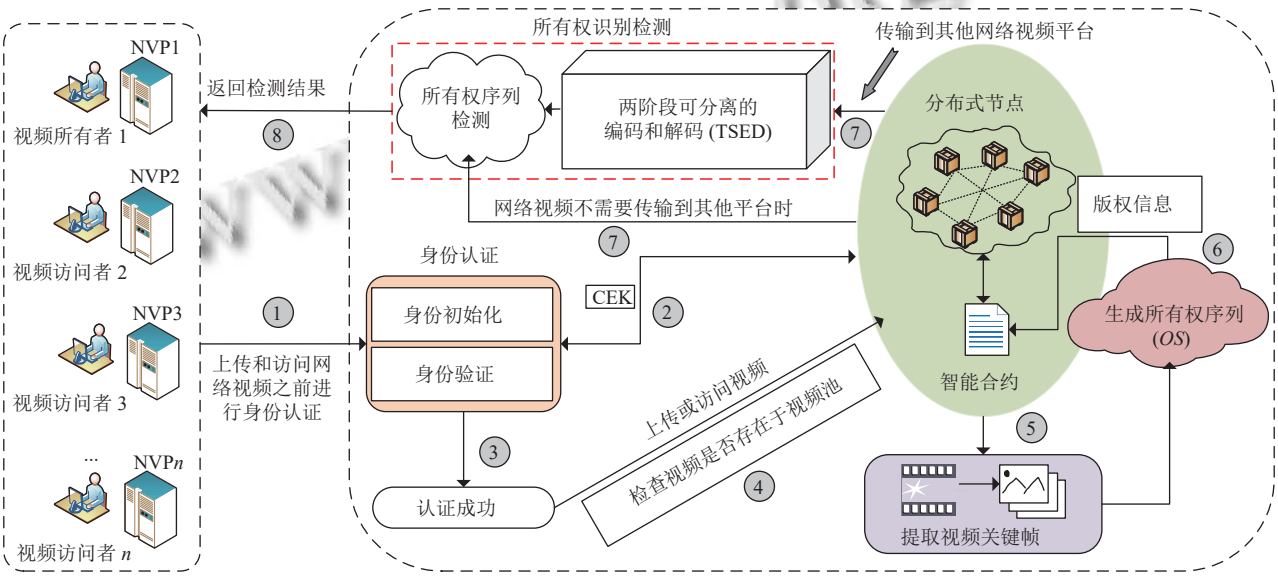

图 1 网络视频版权保护的 BCVCP 架构

在图 1 的 BCVCP 中有 4 个重要的组件: 视频所有者、视频访问者、网络视频平台和分布式节点.

视频所有者: 视频所有者将网络视频上传到视频平台时, 会生成唯一的所有权序列, 存储在分布式节点上, 验证版权归属. 视频所有者需要确保视频原创性, 并回应视频访问者的要求.

视频访问者: 其他视频平台 (如 NVP2 和 NVP3) 上的访问者想访问视频平台 (如 NVP) 上的网络视频, 访问节点需要发出请求.

网络视频平台: 由现有的第三方 NVP 组成. 访问者和所有者都会从视频平台发出请求, 实现跨平台网络视频的所有权序列检测以及传播.

分布式节点: 由分布式区块链组成, 利用智能合约统一处理来自不同网络视频平台的请求, 控制传播. 每个请求视为一个独立事务, 记录在区块链上, 并通过广播机制同步到联邦中的所有对等节点. 存储在区块链上的所有权序列进行所有权检测, 判断版权状态.

在 BCVCP 架构中进行的步骤: 第 1 步视频访问者或视频所有者进行身份认证; 第 2 步通过区块链进行身份初始化和验证, 第 3 步确保认证成功之后进行第 4 步上传或者访问视频, 检查视频是否存在于视频池中; 第 5 步进行视频关键帧提取; 第 6 步生成所有权序列嵌入在视频关键帧中, 存储在分布式节点中; 第 7 步调用智能合约进行所有权序列检测和传播控制管理, 如果是跨平台间的访问传输就需要经过 TSED, 关键帧上的所有权序列编码和传输视频, 提取视频的所有权序列进行检测, 确保在传播树中准确定位视频和所有权序列的正确识别; 最后一步返回所有权序列检测结果.

2.1 身份认证

在区块链网络上, 它必须经过验证节点 (主要用于验证视频所有者、视频访问者的身份和请求) 的处理后, 然后在进行视频版权检测和视频传播控制. 身份初始化和验证过程如图 2 所示.

身份初始化与验证过程在区块链技术的支持下, 提供了一个安全与去中心化的身份认证框架. 在初始化阶段 (图 2 中第 1–4 步), 用户首先提交包含基本身份认证信息及登录凭证的注册请求给验证节点, 并在本地生成一对公私钥. 身份信息通过使用验证节点的公钥加密后, 连同公钥一起发送至节点. 验证节点利用私钥解密信息, 并通过哈希算法转换身份信息生成唯一的用户身份 ID 存储于区块链, 最后返回数字证书给用户. 在身份验证过程中 (图 2 中第 a–d 步), 用户以私钥签名的请求发送至节点, 节点验证签名真实性并确认用户身份 ID 与区块链记录的公钥匹配, 完成用户认证, 确保身份信息的安全.

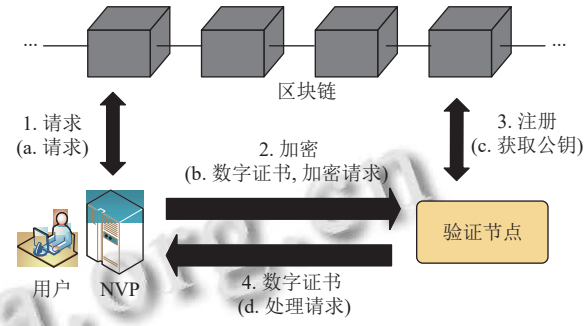

图 2 身份初始化和验证

2.2 网络视频的所有权序列检测

关键帧中嵌入的所有权序列用于检测, 以确定网络视频版权. 该所有权序列为每个关键帧分配一个唯一标识, 并根据所有权序列进行 TSED 和传输, 确保在传输过程中准确识别所有权. 为了便于说明, 本文中使用的符号、所有权序列中包含的信息以及伪代码中函数的作用均详见表 1、表 2 和表 3.

表 1 解释符号

符号	解释
O	视频所有者
V	共享视频
$V_1, V_2, \cdots, V_n$	视频访问者
A	视频属性
T	时间戳
V_{pool}	上传的视频池
OS	所有权序列
$OS(V)$	视频的所有权序列
L	视频的时长
R	视频的分辨率
Operation	操作类型
Vid	一个可选变量, 用于将相应的记录与新创建的传播节点的ID链接起来
keyFrames	关键帧
FrameHash	关键帧哈希

表 2 所有权序列中包含的信息

符号	解释
UID	视频的唯一标识符
I_o	所有者的身份信息

2.2.1 生成所有权序列

根据第 1.2 节中提到的所有权序列生成的原理, 有如下 3 个步骤. 所有权序列的生成过程如图 3 所示.

表 3 伪代码中函数的作用

函数	解释
ConvertVideoAttributesToSequence()	将视频属性转换为序列
CombineOnwerInfoAndUID()	结合所有者信息和UID
checkNotExistence()	检查视频池中是否有已上传的视频
checkAccessRecord()	检查访问记录
getStatus()	获取视频状态
createAccessRecord()	创建访问记录
checkOwnership()	检查所有权
addTreeNode()	添加节点
updateVMCContract()	更新视频管理合约
updateDMCContract()	更新传播管理合约

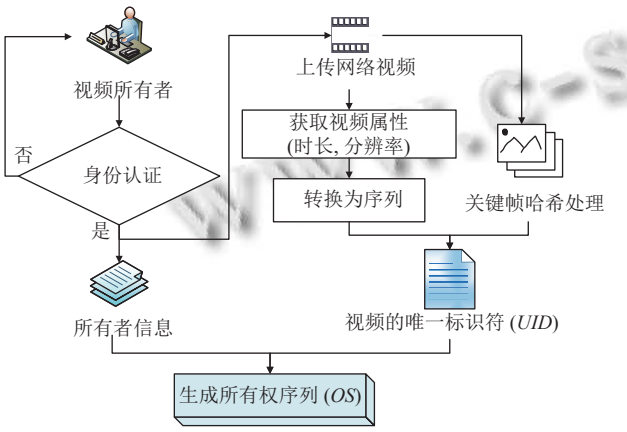

图 3 所有权序列生成过程

步骤 1: 首先需要确定视频的关键帧, 形成一个关键帧集合 $K=\{K_1,K_2,\cdots,K_n\}$, 这是生成视频的唯一的所有权序列提供基础.

步骤 2: 完成关键帧提取后, 接下来是构建视频的唯一标识. 主要涉及两个主要活动: 一是对每个关键帧进行哈希处理 $F(K_n)$=$H(K_n)$, 二是汇总视频属性 A (视频的时长、分辨率), 将这些属性转换为一种可处理的序列形式. 视频的唯一标识 (UID) 由公式: UID=$H(A||F(K_1)||F(K_2)||\cdots||F(K_n))$ 生成. 这个 UID 是基于视频的物理属性和内容特征的一个综合体现, 确保了每个视频的 UID 都是独一无二的, 从而为视频的唯一性提供了坚实的保障.

步骤 3: 所有权序列的生成是整个方案中最为关键的部分, 它不仅包含了视频内容的唯一标识 (UID), 还结合了视频所有者的信息 I_o (通过身份认证). 通过公式使用哈希函数生成所有权序列: OS=$H(UID||I_o)$.

算法 1 展示了所有权序列生成的伪代码.

算法 1. 所有权序列的生成

输入: V, I_o.
输出: OS.

1. $L \leftarrow V$.duration;
2. $R \leftarrow V$.resolution;
3. *keyFrames* ← ExtractKeyFrames(V);
4. *FrameHash* ← HashFunction(*keyFrames*);
5. A ← ConvertVideoAttributesToSequence (L, R);
6. *UID* ← HashFunction(*FrameHash*, A);
7. *combinedInfo* ← CombineOnwerInfoAndUID(I_o, *UID*);
8. *OS* ← HashFunction(*combinedInfo*);
9. **return** *OS*;

生成的所有权序列为每个视频创建了一个独特的身份证明, 这个身份证明是可验证、不可篡改的, 增强了视频内容的版权保护.

2.2.2 嵌入所有权序列

本文为了让所有权序列嵌入到视频关键帧上, 采用基于帧间差分[31]的方法进行关键帧提取, 这种方法有效地保留了视频中重要的动作和信息. 所有权序列嵌入到视频帧中的模型可以表示为:

$$x(m,n_1,n_2)=x_0(m,n_1,n_2)+OS(m,n_1,n_2) \quad (1)$$

其中, $x(m, n_1, n_2)$ 表示经过所有权序列嵌入后的视频帧信息. 其中 m 代表帧编号, n_1 和 n_2 代表视频帧中的像素坐标. $x_0(m, n_1, n_2)$ 表示原始视频帧信息, 未经修改之前的视频数据. $OS(m, n_1, n_2)$ 代表根据生成的所有权序列, 被添加到原始视频帧中, 用以嵌入所有权序列. 所有权序列的组成部分嵌入在相位中, 随着正弦波变化:

$$OS(m,n_1,n_2)=B\cdot\sin(\theta m+\phi(n_1+n_2)) \quad (2)$$

其中, B 表示所有权序列的振幅. θ 表示参考频率, 用于生成所有权序列的正弦波形. $\phi(n_1+n_2)$表示每个像素位置的相位信息.

2.2.3 所有权序列的编码和解码

本文根据文献[32]中提出的两阶段可分离深度学习 (TSDL) 框架, 提出了两阶段可分离的编码和解码 (TSED) 方法来进行传输. 这意味着编码器和解码器的训练分为两个独立的阶段, 编码器在前一阶段的性能不受后续解码器训练的影响, 从而提升所有权编码质量和所有权识别的鲁棒性. 在编码阶段, 这可以通过修改关键帧的特定分量来实现, 编码过程可以表示为:

$$C'_a=Q^{-1}(Q(C_a+OS_a)) \quad (3)$$

其中, C'_a 有权序列嵌入并可能经过量化调整后的第

a 个系数的值, $Q^{-1}(\cdot)$代表反量化函数, 它是量化函数的逆过程, 用于将量化后的离散级别恢复为连续值或原始精度值. C_a表示第 a 个原始系数, 是视频关键帧在进行变换后得到的系数中的一个, 未进行所有权序列嵌入前的值. OS_a是对应于第 a 个系数的所有权序列, 用于嵌入到视频关键帧中以编码所有权序列. $Q(\cdot)$表示量化函数, 它将输入的连续值转换为有限数量的离散级别.

在解码阶段, 如果方法设计得当, 即使在视频压缩和传输过程中受到一定程度的失真, 仍然可以准确提取出所有权序列:

$$OS'_a = Q(C'_a) - Q(C_a) \tag{4}$$

在这个过程中, 通过比较原始系数的量化值和嵌入所有权序列后系数的量化值之差, 可以估计出嵌入的所有权序列OS'_a.

2.2.4 所有权序列提取

利用线性移不变 (linear shift-invariant, LSI) 系统和其复值冲激响应 (impulse response, IR) 来从嵌入后的视频帧中提取所有权序列. 假设 LSI 系统的冲激响应为:

$$h(m) = \alpha^m \mathrm{e}^{i\cdot\theta\cdot m} \tag{5}$$

通过 LSI 系统处理输入 $x(m, n_1, n_2)$ 到输出:

$$\begin{aligned} y(m,n_1,n_2) &= h(m)\cdot x(m,n_1,n_2) \\ &= y_c(m,n_1,n_2) + i\cdot y_s(m,n_1,n_2) \end{aligned} \tag{6}$$

其中, $h(m)$ 表示线性移不变系统的复值冲激响应, 用于处理嵌入了所有权序列的视频. α 表示 LSI 系统的衰减参数, 用于调整冲激响应的衰减速率. $y_c(m,n_1,n_2)$表示通过 LSI 系统处理后的输出, 是一个复数值, 包含了实部 y_c 和虚部 y_s. $y_c(m,n_1,n_2)$和$y_s(m,n_1,n_2)$分别代表输出的实部和虚部, 它们分别通过与 LSI 系统的实部和虚部冲激响应卷积得到.

从文献[2]中提到的相位信息, 结合到本文的所有权序列的提取和嵌入中, 它在数字信号处理、通信和数字版权管理中起着关键作用, 在版权保护中, 会利用相位来携带嵌入到内容中的所有权序列. 这种方法可以在不明显影响内容质量的情况下, 提供一种隐蔽而具有鲁棒性的版权保护方法. 从$y_c(m,n_1,n_2)$和$y_s(m,n_1,n_2)$中提取相位信息, 该相位信息包含了原始所有权序列:

$$\phi = \tan^{-1}\left(\frac{y_s(m,n_1,n_2)}{y_c(m,n_1,n_2)}\right) \tag{7}$$

其中, $\tan^{-1}$表示反正切函数, 用于从 y_c 和 y_s 计算相位信息ϕ, 它代表了在视频帧 m 的像素位置 (n_1, n_2) 入的所有权序列, 以提取嵌入的所有权序列信息, 进行所有权序列检测, 验证版权.

2.2.5 网络视频版权检测

从网络视频关键帧提取所有权序列之后, 进行所有权序列检测的时候调用智能合约, 最后返回检测的结果. 如图 4 所示, 展示通过智能合约进行所有权序列检测来识别版权的流程.

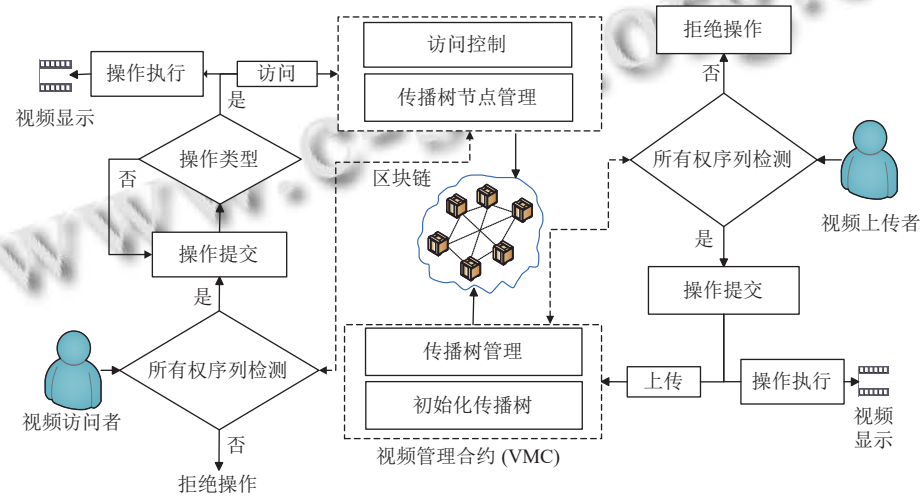

图 4 版权检测的过程

所有权序列提取之后, 进行所有权序列检测过程中, 会调用智能合约实现, 包括网络视频的控制, 详见第 3.3.1 节和第 3.3.2 节. 智能合约公开透明, 所有交易公开可见, 进行版权检测判断的过程可被监控, 结果真实可信. 算法 2 是一段详细的伪代码, 展示了通过所有权序列检测判断网络视频的版权.

传播管理合约的访问记录包括访问用户 ID、所有权序列、操作类型、结果、时间戳和 *Vid*, 用户 ID 用于绑定访问者的身份信息. 所有权检测通过确定用户是否拥有视频的合法版权, 并确保相应的传播节点处于活动状态 (如果视频被删除则标记为非活动状态). 当视频访问者通过 NVP1 上的传播节点 *O* 发起对视频 *V* 的访问时, 算法 2 会首先检查视频 *V* 是否存在于视频池中, 并通过嵌入的所有权序列来验证用户是否拥有该视频的合法版权, 以避免不诚实或伪造的访问请求. 算法 2 还会进一步检查传播节点 NVP1.*O* 在传播树中的记录, 确保传播节点的合法性和活动状态, 确保网络视频的版权得到有效保护. 通过这一系列检查, 算法 2 的所有权序列检测保证了用户 *O* 对视频 *V* 的所有权, 并确保其在网络视频平台 NVP1 上的访问行为符合版权保护要求, 从而有效防止跨平台的版权侵权行为, 保护视频的合法传播.

算法 2. 所有权序列检测

输入: *V*, *O*, *OS*(*V*), V_{pool}, *VMC*.
输出: Ownership legitimacy of *O* to *V*.

1. **if** checkNotExistence(*OS*(*V*), V_{pool}) **then**
2. 没有视频∈V_{pool} 匹配 *V*;
3. **return** False;
//调用函数, 检查所有权序列 *OS*(*V*) 是否存在于视频池中
4. **else**
5. *DMC* ← getTree(*OS*(*V*));
6. **if** checkAccessRecord(*O*, NVP1, *DMC*) 不是成功的 **then**
7. NVP1.*O* 是非法的视频所有者;
8. **return** False;
//检查 *O* 是否在网络视频平台 NVP1 上有合法的访问记录
9. **end if**
10. *Vid* ← getVid(*O*, NVP1, *DMC*);
11. **if** *Vid* == 0 **then**
12. NVP1.*O* 不是一个合法的传播树节点;
13. **return** False;
14. **end if**
15. **if** getStatus(*Vid*) != Active **then**
16. NVP1.*O* 的传播状态为非活动;
17. **return** False;
//检查传播节点当前是否为活跃 (Active) 状态, 才能保证是否传播
18. **end if**
19. **end if**
20. **return** *Vid*, *DMC*;

2.3 网络视频的控制管理

在通过身份认证之后, 用户需要访问或者上传视频的时候, 所有传播过程中对网络视频的控制都由智能合约完成: 视频管理合约 (*VMC*) 和传播管理合约 (*DMC*). 将传播空间从单一的视频平台扩展到多个视频平台. 这两种智能合约结构之间的关系如图 5 所示.

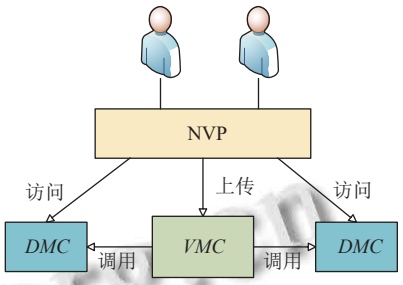

图 5 智能合约的关系结构

2.3.1 视频管理合约 (*VMC*)

VMC 只负责上传视频, 它拥有一个由所有传播树根组成的视频池, 记录视频及其原始所有者的信息. 在 *VMC* 中, 每个视频在第 1 次上传时只注册 1 次. 算法 3 展示了网络视频上传的伪代码.

算法 3. 上传网络视频

输入: *V*, *O*, *T*, *OS*, NVP1, *OS*(*V*), V_{pool}, *VMC*.
输出: ResultNVP1.

1. **if** checkNotExistence(*OS*(*V*), V_{pool}) **then**
2. *V* 之前已经上传过了;
3. **goto** 算法 2;
4. **if** checkNotExistence(*OS*(*V*), V_{pool})!=True **then**
5. **goto** 算法 1;
6. **else**
7. *Operation* ← upload;
8. *Id* ← *DMC*.createAccessRecord(*O*, NVP1, *Operation*);
9. *Vid* ← *VMC*.createTreeRoot(*OS*(*V*));
10. *VMC*.setVid(*Id*, *Vid*);
11. *V* ← {*OS*(*V*), *O*, NVP1, *T*, *DMC*, *VMC*};
12. V_{pool} ← V_{pool} ∪ *V*;
13. updateVMCContract(*VMC*, V_{pool});
14. updateDMCContract(*DMC*, *Id*);
15. *DMC*.setStatus(*Vid*, Active);
16. **return** ResultNVP1 {*DMC*.Status, *VMC*, *T*};
17. **end if**

在上传时, 首先检查视频是否已存在于视频池中. 若已存在, 则转向算法 2 进行所有权检测, 通过所有权序列验证. 对于新视频, 记录上传操作, 创建访问记录和树根节点, 然后转到算法 1 生成所有权序列, 并更新视频和 *DMC* 的状态, 将新视频改为活动状态. 若此次访问更新传播树并创建新的传播节点, 则 *Vid* 是一个可选变量, 用于将相应的记录与新创建的传播节点的

ID 链接起来.

2.3.2 传播管理合约 (*DMC*)

与 *VMC* 不同, *DMC* 侧重于管理第 1 次上传后的后续访问等. *DMC* 列出的访问记录包括访问上传者 ID、所有权序列、操作类型以及时间戳等. 算法 4 的伪代码展示了通过在上传视频之后通过 *DMC* 来进行访问.

算法 4. 访问网络视频

输入: V, V_2, O, T, OS, NVP2, O, $OS(V)$, V_{pool}, *VMC*, *DMC*.
输出: ResultNVP2.

1. **if** 算法 2 ($OS(V)$, O, V_{pool})!=True **then**
2. O 不是一个合法的传播树节点;
3. **return** False;
//通过调用算法 2, 验证 O 是否是合法的传播树节点. 如果算法 2 检测到 O 不具备所有权, 则拒绝访问请求
4. **else**
5. *Vid*, *DMC* ← 算法 3($OS(V)$, O, V_{pool});
//*DMC* 记录了视频的所有者相关信息, 是视频传播过程中的核心合约, 确保传播节点合法性
6. **end if**
7. *Operation* ← visit;
8. *IsValidOwner* = *DMC*.checkOwnership(V_2, $OS(V)$);
//设置当前的操作类型为“访问”, 并调用函数, 检查视频的所有权是否合法. 这个函数会验证 O 是否有权访问视频, 确保其行为符合视频版权的要求.
9. **if** *IsValidOwner* then
10. *Id* ← *DMC*.createAccessRecord(V_2, $OS(V)$, *Operation*, T);
11. *Vid* ← *DMC*.addTreeNode($OS(V)$);
12. updateDMCContract(*DMC*, *Id*);
13. **return** ResultNVP2 {V_2, *DMC*, T, *Operation*};
//如果所有权验证通过, *DMC* 会创建一个访问记录, 记录视频的访问信息, 并为 O 创建一个新的传播树节点. 随后, *DMC* 会更新合约, 将新的访问记录写入区块链中, 确保每一次访问行为都被记录和追踪.
14. **end if**

算法 4 通过验证 O 对视频 V 的所有权, 确保其在网络视频平台 NVP2 上的访问行为符合版权保护要求. 首先, 调用算法 2 进行所有权序列检测, 若未通过验检, 则拒绝访问; 若通过, 则调用算法 3. 随后, *DMC* 会创建访问记录, 并为用户添加新的传播节点, 更新传播管理合约中的信息. 整个过程确保了视频的所有权检测和传播路径的合法性, 防止未经授权的访问或伪造请求, 进而有效保护视频的跨平台版权. *DMC* 负责管理视频在平台上的每次传播和访问, 记录每个传播节点的合法性, 并创建相关的访问记录. 最终, 算法将访问结果返回给 NVP2, 确保视频的版权得到保护, 并完整记录每次访问行为, 防止侵权.

3 实验与分析

本实验需在 Ubuntu 20.04.6 系统中进行, 使用 HyperLedger Fabric 2.5 用于构建区块链, 以便验证所提出方案的可行性, 其余配置的版本描述: Go 版本 1.18.5, Docker 版本 24.0.5, Node 版本 14.21.3, Docker-compose 版本 1.26.0, Caliper 版本 0.5.0.

通过实验, 来验证和评估所有权序列检测在 5 个网络视频平台 (NVP1, NVP2, NVP3, NVP4, NVP5) 上的性能, 展示 BCVCP 在不同网络视频平台传输时的性能和鲁棒性. 实验从 Kaggle 官网 (https://www.kaggle.com/) 下载 50 个视频均为 MP4 格式的片段, 涵盖 10 s–1 min、1–3 min、3–5 min 的不同时长和不同分辨率 (480p、720p、1 080p、4k) 的视频, 将 50 个视频平均分为训练集和验证集两组, 每组各 25 个视频, 视频的时长和分辨率应在两组中均匀分布, 确保每组都有足够的多样性和代表性, 以测试 BCVCP 对各种视频的适应性.

3.1 方案评估

3.1.1 区块链性能

使用 HyperLedger Caliper 测试区块链网络的性能, 确保高效稳定地处理和检测视频版权. 测试性能指标包括事务成功率、每秒事务数、事务延迟和资源使用情况. 通过测试能验证 BCVCP 在不同网络视频平台的适应性. 通过 Caliper 配置测试脚本和网络参数, 然后进行测试, 测试成功后, 会在当前目录生成测试结果报告. 区块链性能测试的指标和资源占用情况报告如表 4 和表 5 所示.

表 4 中, 测试的事务成功率为 100%, 平均事务延迟为 0.02 s (最大事务延迟为 0.22 s, 最小事务延迟为 0.01 s), 吞吐量为 1 962.9 Tb/s, 满足网络视频上传或者访问以及检测等操作需求.

表 4 性能指标

名称	成功	失败	发送速率 (Tb/s)	最大延迟 (s)	最小延迟 (s)	普通延迟 (s)	吞吐量 (Tb/s)
invoke	50 000	0	1 963.7	0.22	0.01	0.02	1 962.9

表 5 中, 返回的资源占用结果包括内存使用情况、CPU 使用情况、I/O traffic 等, 资源占用情况直接反映了运行效率, 在资源消耗较低的同时, 也能处理数据和请求, 展示了区块链稳定的性能. 此外, 所有节点都会占用一定的内存量, 因为它们处于活动状态.

表 5 资源利用情况

标识符	CPU (最大) (%)	CPU (平均) (%)	内存 (最大) (MB)	内存 (平均) (MB)	流量输入 (MB)	流量输出 (MB)
dev-peer1.org5.example.com-asn_1	0.00	0.00	15.7	15.7	0.00	0.00
dev-peer3.org5.example.com-asn_1	0.00	0.00	17.8	17.8	0.00	0.00
dev-peer0.org5.example.com-asn_1	0.00	0.00	15.7	15.7	0.00	0.00
cil	0.00	0.00	2.22	2.22	0.00	0.00
orderer.example.com	2.75	1.02	84.3	81.9	182	242
peer1.org5.example.com	2.90	2.14	120	117	198	271
peer2.org5.example.com	1.50	1.43	60.0	59.9	0.00	0.00
peer3.org5.example.com	2.98	2.31	130	128	199	272
peer0.org5.example.com	2.85	2.23	155	151	237	927

3.1.2 性能分析

为了展现本文提出 BCVCP 的性能, 进行了测试, 在实验条件下, 通过评估视频上传和访问时的吞吐量, 展示在处理不同视频平台上传和访问请求时的效率和响应速度, 同时也反映了跨视频平台网络视频上传和访问时的所有权序列检测的性能, 如图 6 所示.

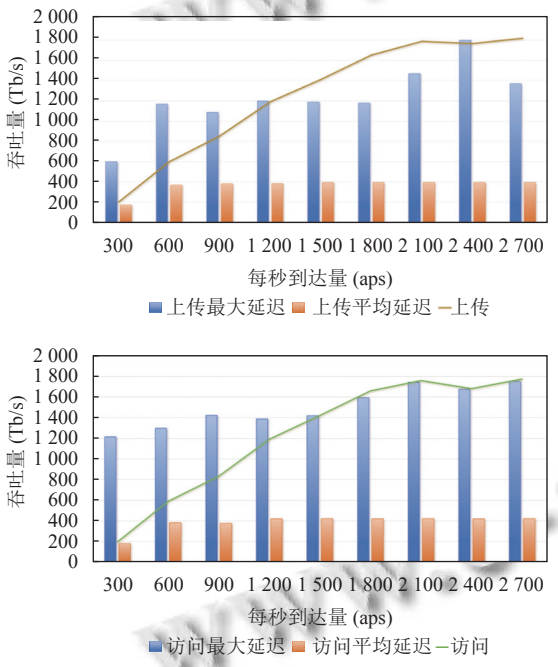

图 6 性能评估

随着事务到达率的增加, 通过所有权合法性检测来判断版权时的上传和访问视频的吞吐量线性增加, 直到达到饱和点, 分别为 1 820 Tb/s 和 1 772 Tb/s. 平均延迟稳定在 1 s 内, 不随每秒到达量 (arrival per second, aps) 的增长而波动. 相比之下, 最大延迟对每秒到达量很敏感, 很早就达到峰值. 该方案能够在保持较高吞吐量的同时, 实现可靠的所有权合法性检测, 上传过程平均耗时和访问响应时间均在可接受的范围内.

3.2 所有权编码质量

在 BCVCP 中, 视频关键帧被编码其所有权序列, 按照其所有权序列进行编码, 这有助于在传输过程中进行正确的所有权识别. 为了评估编码质量, 本文采用峰值信噪比 (*PSNR*) 来衡量. *PSNR* 的高值表示编码质量高, 视觉失真低. 计算 *PSNR* 前需计算均方误差, 嵌入所有权序列视频关键帧图像与原始视频关键帧图像之间的差值可用均方误差 (*MSE*) 评价, *MSE* 与 *PSNR* 成反比关系, 公式如下:

$$MSE = \frac{1}{w \times h}\sum_{x=1}^{w}\sum_{y=1}^{h} \times (I(x,y) - I'(x,y))^2 \quad (8)$$

计算 *PSNR*:

$$PSNR = 10\log 10\frac{255^2}{MSE} \quad (9)$$

其中, $I(x,y)$表示原始视频关键帧在位置(x,y)的像素值. $I'(x,y)$嵌入了所有权序列后的视频关键帧在位置(x,y)的像素值. (x,y)代表原始和嵌入所有权序列后的视频关键帧中像素的位置; 以及$w \times h$表示原始视频帧的宽度和高度.

为了确保在传输过程中不丢失和损坏所有权序列, 采用了 TSED. 传输过程可能受到多种噪声的影响, 通过噪声训练, 可以更好地模拟实际场景, 提高在实际应用中的可靠性. 不同噪声攻击下的 *PSNR* 值验证了在传输过程中视频关键帧图像质量的能力. 表 6 展示了本文提出的 TSED 与文献[22–24]中提出的独立编码和联合编码, 在不同噪声共攻击 (无噪声: No noise; 高斯噪声: Gaussian; 裁剪: Crop; 缩放: Resize; 亮度与对比度调整: Brightness & Contrast; 填充: Padding; 帧丢失: Frame dropping; 帧平均: Frame averaging; 帧交换: Frame swapping) 下进行比较, 显示了在不同噪声攻击下的 *PSNR* 值.

从表 6 中结果可以看出, 本文所提出的 BCVCP,

使 *PSNR* 可以平均达到 65.09 dB, 与最低相比提升了许多, 性能表现最好, 解码的所有权序列将与其对应的传播树根的地址相匹配. 因此, 只要正确提取关键帧所有权序列, 就能够在跨视频平台上传的分布式节点的传播树中定位上传的视频. 而文献[22–24]中使用编码器和解码器都在一起训练, 会导致编码器图像质量不可避免地下降.

表 6 不同噪声攻击下的 *PSNR* (dB)

噪声类型	文献[22]	文献[23]	文献[24]	BCVCP
No noise	63.43	64.53	62.97	73.58
Gaussian	53.51	54.23	56.16	69.35
Crop	55.22	50.10	57.34	65.99
Resize	43.92	42.32	46.77	59.47
Brightness & Contrast	54.55	57.12	59.19	61.51
Padding	56.47	58.67	60.11	63.78
Frame dropping	60.76	62.97	58.98	66.84
Frame averaging	59.91	62.32	60.45	66.34
Frame swapping	61.38	63.77	62.78	67.91

3.3 BCVCP 的鲁棒性

以上评估证明了本文的方案在保持关键帧图像质量方面的优势. 由于实际视频传输过程中存在的噪声是不可预测的, 为了确保不被侵权, 还需验证所有权序列进行的所有权识别在跨平台分享视频时, 所有权识别的鲁棒性, 将本文的方案与文献[22–25]的方案进行比较. 比特精度高意味着能够更好地保留细节和颜色信息, 减少传输过程中的质量损失. 通过验证编码视频关键帧及其所有权序列进行传输过程中遇到不可预测的噪声时, 所有权序列嵌入在关键帧中仍然能准确识别和验证视频所有权的能力, 确保在传输过程中受到不可预测的噪声时的鲁棒性.

比特精度与比特错误率 (*BER*) 有关, 两个是互补的关系, 比特错误率的公式:

$$BER=\left(\frac{1}{W\times L}\sum_{p=1}^{W}\sum_{q=1}^{L}\left|OS(p,q)-OS'(p,q)\right|\right)\times 100\% \tag{10}$$

其中, OS 和 OS' 表原始和提取的所有权序列, W 所有权序列的行数和列数, $|OS(p,q)-OS'(p,q)|$ 是原始所有权序列和提取所有权序列之间在位置 (p,q) 的差异. 所以比特精度的公式如下:

$$(1-BER)\times 100\% \tag{11}$$

如表 7 所示进行了比较. 从结果中可以看出, 本文所提出的 BCVCP 表现最好. 对于无噪声以 91.73% 的比特精度位居榜首. 事实证明, 当比特精度低于 80.00% 时, 解码的所有权序列将无法与其对应的传播树根的地址相匹配. 总体而言, 平均比特精度达到 89.90%. 通过测试解码器在噪声环境下的比特精度, 展示了所有权识别技术在跨视频平台传输时的鲁棒性. 其主要作用是确保即使在数据传输过程中遭受干扰的情况下, 所有权序列仍能被准确保护和识别, 从而防止因视频质量变化导致的侵权问题.

表 7 噪声攻击的鲁棒性指标 (%)

噪声类型	文献[22]	文献[24]	文献[25]	BCVCP
No noise	83.56	82.11	81.56	91.73
Gaussian	78.67	81.39	80.76	89.82
Crop	79.72	78.79	77.11	88.82
Resize	78.61	81.23	7672	89.95
Brightness & Contrast	84.35	79.98	84.38	91.03
Padding	82.78	83.64	79.43	90.43
Frame dropping	78.99	79.34	82.78	89.76
Frame averaging	79.12	80.88	78.99	88.93
Frame swapping	81.44	77.90	79.67	88.63

4 结论

本文提出的 BCVCP 提供了一种有效的版权保护方案. 该方案保护了网络视频版权信息, 为每次上传和访问建立了唯一且可验证的所有权序列. 实验验证了 BCVCP 在跨平台传输网络视频时所有权编码质量和所有权识别的鲁棒性, 满足了网络视频版权保护的需求. 未来工作将集中在提高基于区块链的所有权序列跨平台网络视频版权保护的性能、安全性和用户友好性方面. 同时, 也将关注提升用户体验、确保合法性和合规性, 并探索在其他数字内容版权管理中的应用.

参考文献

1 王露莹, 张峻玮, 赵禹恩, 等. 基于区块链的短视频版权保护与交易研究. 数字出版研究, 2023, 2(1): 89–98.

2 Shapiro D, Sergeyev V, Fedoseev V. Improved ECC-based phase watermarking method for video copyright protection. Proceedings of the 11th International Symposium on Digital Forensics and Security (ISDFS). Chattanooga: IEEE, 2023. 1–6.

3 周雯荻. 基于区块链的短视频版权保护机制的研究 [硕士学位论文]. 北京: 北京邮电大学, 2023.

4 Wang BW, Jiawei S, Wang WS, *et al*. Image copyright protection based on blockchain and zero-watermark. IEEE Transactions on Network Science and Engineering, 2022,

9(4): 2188–2199. [doi: 10.1109/tnse.2022.3157867]
5 Qi YF, Liu JB, Dong F, *et al*. Short video copyright protection based on blockchain technology. Proceedings of the 2nd Asia Conference on Computers and Communications (ACCC). Singapore: IEEE, 2021. 106–110.
6 Zhao WH, Lin X, Chen YX, *et al*. A blockchain-based copyright protection system for short videos. Proceedings of the 2022 IEEE International Conference on Parallel & Distributed Processing with Applications, Big Data & Cloud Computing, Sustainable Computing & Communications, Social Computing & Networking (ISPA/BDCloud/SocialCom/SustainCom). Melbourne: IEEE, 2022. 929–936.
7 Zheng JJ, Teng SH, Li PR, *et al*. A novel video copyright protection scheme based on blockchain and double watermarking. Security and Communication Networks, 2021, 2021(1): 6493306. [doi: 10.1155/2021/6493306]
8 Barua S, Talukder D. A blockchain based decentralized video streaming platform with content protection system. Proceedings of the 23rd International Conference on Computer and Information Technology (ICCIT). Dhaka: IEEE, 2020. 1–6.
9 Guo JQ, Li CY, Zhang GZ, *et al*. Blockchain-enabled digital rights management for multimedia resources of online education. Multimedia Tools and Applications, 2020, 79(15): 9735–9755. [doi: 10.1007/s11042-019-08059-1]
10 Garba A, Dwivedi AD, Kamal M, *et al*. A digital rights management system based on a scalable blockchain. Peer-to-peer Networking and Applications, 2021, 14(5): 2665–2680. [doi: 10.1007/s12083-020-01023-z]
11 Chen QY, Kong YH, Cheng LL. A digital copyright protection system based on blockchain and with sharding network. Proceedings of the 10th IEEE International Conference on Cyber Security and Cloud Computing (CSCloud)/the 9th IEEE International Conference on Edge Computing and Scalable Cloud (EdgeCom). Xiangtan: IEEE, 2023. 393–398.
12 Cai ZN. Usage of deep learning and blockchain in compilation and copyright protection of digital music. IEEE Access, 2020, 8: 164144–164154. [doi: 10.1109/ACCESS.2020.3021523]
13 Yang Y, Yu DG, Zhang RB, *et al*. A video copyright transaction traceability method based on mother-child blockchain. Proceedings of the 3rd International Conference on Blockchain Technology and Applications. Xi'an: ACM, 2020. 1–6.
14 Wang BW, Li B, Yuan Y, *et al*. CPDT: A copyright-preserving data trading scheme based on smart contracts and perceptual hashing. Proceedings of the 2022 IEEE International Conference on Trust, Security and Privacy in Computing and Communications (TrustCom). Wuhan: IEEE, 2022. 968–975.
15 Zhao SJ, O'Mahony D. BMCProtector: A blockchain and smart contract based application for music copyright protection. Proceedings of the 2018 International Conference on Blockchain Technology and Application. Xi'an: ACM, 2018. 1–5.
16 Jiang C, Huang KM, He SF, *et al*. Learning segment similarity and alignment in large-scale content based video retrieval. Proceedings of the 29th ACM International Conference on Multimedia. ACM, 2021. 1618–1626.
17 Khelifi F, Bouridane A. Perceptual video hashing for content identification and authentication. IEEE Transactions on Circuits and Systems for Video Technology, 2019, 29(1): 50–67. [doi: 10.1109/TCSVT.2017.2776159]
18 Zhao GJ, Li FY, Yao H, *et al*. TASTNet: An end-to-end deep fingerprinting net with two-dimensional attention mechanism and spatio-temporal weighted fusion for video content authentication. Journal of Visual Communication and Image Representation, 2023, 96: 103913. [doi: 10.1016/j.jvcir.2023.103913]
19 Yang Y, Yu DG. Short video copyright storage algorithm based on blockchain and expression recognition. International Journal of Digital Multimedia Broadcasting, 2022, 2022(1): 8827815. [doi: 10.1155/2022/8827815]
20 Chen Y, Yan ZL, Dong C, *et al*. A novel fast video fragment matching algorithm for copyright protection. Proceedings of the 2023 IEEE International Conference on Dependable, Autonomic and Secure Computing, International Conference on Pervasive Intelligence and Computing, International Conference on Cloud and Big Data Computing, International Conference on Cyber Science and Technology Congress (DASC/PiCom/CBDCom/CyberSciTech). Abu Dhabi: IEEE, 2023. 0220–0227.
21 Agyekum KOBO, Xia Q, Liu YS, *et al*. Digital media copyright and content protection using IPFS and blockchain. Proceedings of the 10th International Conference on Image and Graphics. Beijing: Springer, 2019. 266–277.
22 Sridhar B, Syambabu V. Security enhancement in video based on gatefold technique for copyright protection. Multimedia Tools and Applications, 2021, 80(6): 8241–8256. [doi: 10.1007/s11042-020-09909-z]
23 Priya C, Ramya C. Robust and secure video watermarking

based on cellular automata and singular value decomposition for copyright protection. Circuits, Systems, and Signal Processing, 2021, 40(5): 2464–2493. [doi: 10.1007/s00034-020-01585-6]

24 Resen MS, Laftah MM. A blind video copyright protection technique in maximum and minimum energy frames based on the fast walsh Hadamard transform (FWHT) and discrete wavelet transform (DWT) and Arnold map. International Journal of Interactive Mobile Technologies, 2022, 16(10): 163–175. [doi: 10.3991/ijim.v16i10.30039]

25 Liu XY, Zhang YY, Wang JY, *et al*. Multiple-feature-based zero-watermarking for robust and discriminative copyright protection of DIBR 3D videos. Information Sciences, 2022, 604: 97–114. [doi: 10.1016/j.ins.2022.05.010]

26 Palomar E, González-Manzano L, Alcaide A, *et al*. Implementing a privacy-enhanced attribute-based credential system for online social networks with co-ownership management. IET Information Security, 2016, 10(2): 60–68. [doi: 10.1049/iet-ifs.2014.0466]

27 Juarez-Sandoval OU, Cedillo-Hernandez M, Nakano-Miyatake M, *et al*. Digital image ownership authentication via camouflaged unseen-visible watermarking. Multimedia Tools and Applications, 2018, 77(20): 26601–26634. [doi: 10.1007/s11042-018-5881-0]

28 Mohit M, Kaur S, Singh M. Design and implementation of transaction privacy by virtue of ownership and traceability in blockchain based supply chain. Cluster Computing, 2022, 25(3): 2223–2240. [doi: 10.1007/s10586-021-03425-x]

29 de Jesus Vega-Hernandez P, Cedillo-Hernandez M, Nakano M, *et al*. Ownership identification of digital video via unseen-visible watermarking. Proceedings of the 7th International Workshop on Biometrics and Forensics (IWBF). Cancun: IEEE, 2019. 1–6.

30 Mandelli S, Bestagini P, Verdoliva L, *et al*. Facing device attribution problem for stabilized video sequences. IEEE Transactions on Information Forensics and Security, 2020, 15: 14–27. [doi: 10.1109/TIFS.2019.2918644]

31 Hu LH. Lossless decoding method of compressed coded video based on inter-frame differential background model: Multi-algorithm joint lossless decoding. International Journal of Grid and High Performance Computing, 2023, 15(2): 1–13. [doi: 10.4018/ijghpc.318407]

32 Liu Y, Guo MX, Zhang J, *et al*. A novel two-stage separable deep learning framework for practical blind watermarking. Proceedings of the 27th ACM International Conference on Multimedia. Nice: ACM, 2019. 1509–1517.

(校对责编: 张重毅)