孪生数字人的形象与语言授权框架研究

韩家伟,朱 妍

(长春大学 计算机科学技术学院,吉林 长春 130022)

摘 要: 由于AIGC(人工智能生成的内容)发展迅速,网络上涌现出一大批生成视频,但生成式AI可能会产生许多虚假信息,会对公众造成严重误导,不法之徒可以利用低成本高效率伪造文本、图片甚至视频进行诈骗、恐吓、诽谤等行为。据此,提出一个可以对孪生数字人的语言和行为进行授权的框架,该框架通过人脸识别和区块链加密生成数字签名,最后生成数字证书对信息进行保存授权。该方法有效地对生成的孪生数字人视频进行了真人核对、信息验证和物理信息保存授权。经过实验验证,该框架完全可以通过对视频内容的检测,达到对具体时空切片内所发布的言论和行为进行授权和鉴别的要求。

关键词: 孪生数字人;授权框架;言论加密;数字证书;生成式人工智能

DOI: 10.11907/rjdk.231515 **开放科学(资源服务)标识码(OSID):**

中图分类号: TP391 **文献标识码:** A **文章编号:** 1672-7800(2024)007-0045-06

A Study on the Image and Language Empowerment Framework of Twin Digital People

HAN Jiawei, ZHU Yan

(*School of Computer Science and Technology, Changchun University, Changchun* 130022, *China*)

Abstract: Due to the rapid development of AIGC (artificial intelligence generated content), a large number of generated videos have emerged on the web, but generative AI may generate a lot of false information, which could be seriously misleading to the public, and unscrupulous people could use the low cost and efficiency to fake texts, images, or even videos to commit fraud, intimidation, defamation, etc. A framework for authorising the language and behaviour of twin digital humans is proposed. The framework generates digital signatures by combining face recognition and encryption in the blockchain, and finally generates digital certificates to store the information for authorisation.The method effectively generates a video of the twin digital person for real person verification, message validation and physical information retention authorisation. It has been experimentally verified that the framework is fully capable of achieving authorisation and identification of the statements and actions posted within specific slices of time and space through content detection of the videos.

Key Words: twin digital people; authorization framework; speech encryption; digital certificates; generative artificial intelligence

0 引言

AI的兴起是时代的进步,其带来了许多新的发展方向。计算机识别、自然语言生成等技术的崛起,极大地简化了许多相关工作。目前,与数字人相关的工作最受瞩目,它有3种发展方向:虚拟化、智能化、外脑化[1]。数字人是基于真人在元宇宙中的分身,也被称为孪生数字人,其能够替代人类在元宇宙中执行特定任务,但缺乏情感和自主权,一切由真人控制。在不远的未来甚至现阶段,数字人代替人类完成许多工作将成为现实。

关于生成数字人的研究热度较高,Yi等[2]利用输入声音和固定300帧说话的视频即可输出说话的视频,主要通过语音驱动控制人脸表情和动作。Wan等[3]引入额外的表情标签以及对应的表情幅度标签,通过条件生成网络生成带有表情的说话人图像。Ji等[4]基于特定的音频数据显式地分离音频中的表情信息,该方法通过交叉重建引入重建损失、分类损失、特征损失,将音频特征解耦到内容空间和表情空间,然后预测人脸关键点并进行单目三维人脸重建,得到姿态、表情、纹理参数,组合后投影得到人脸边缘

收稿日期: 2023-07-28

作者简介: 韩家伟(1978-),男,博士,长春大学网络安全学院副教授、硕士生导师,研究方向为网络安全、量子保密通信;朱妍(1998-),女,长春大学计算机科学与技术学院硕士研究生,研究方向为中国文化网络传播、网络安全。

图，放入生成器得到带有表情信息的重演图像。Fried 等[5]提出通过文字编辑视频的重演方法。在原有视频的基础上，用户对说话内容进行添加、替换、删除操作，该方法能生成逼真的对应视频。由于用户只能对说话内容进行有限修改，因此模型输入被极大地简化。同时，模型在已有视频基础上进行检索，挑选最适配于用户修改的片段，极大简化了模型的学习过程。该方法首先利用视频提供的语音素材对齐驱动文本信息，包括添加、删除、重排单词，随后对视频中的每一帧进行三维人脸重建，提取每一帧的身份和姿态参数，并根据语料的排序信息重排表情参数，最后使用渲染模块结合视频背景信息完成重演。Yao 等[6]进一步扩展了上述方法，引入参考人物音素及视频，通过建立音素索引、减少搜索空间的方式提升音频音素查找速度；通过引入参考任务表情参数到目标人物表情参数的转化模块，在搜索音素时仅搜索参考人物即可，摆脱了原有重演模型的身份限制。这类通过文字编辑视频的重演方法，通过简化模型的学习目标，得到了不错的重演结果。但也由于输入的文字只能进行有限的修改且需要用到大量的源人脸数据，这类模型在使用上存在很大限制。Li 等[7]所采用的方法则降低了对于源人脸数据的依赖，输入与时间对齐好的文本数据并将其作为驱动信息，分别预测头部姿态、面部表情、嘴部形状等信息，随后重建人脸三维模型并使用视频生成器生成面部重演视频。

2022 年，美国人工智能公司 OpenAI 发布了大型语言模型 ChatGPT，该模型一经发布，便在全国范围内受到了广大用户的追捧。随着数字人的快速发展，GPT+数字人生成视频，仅仅需要文本内容和数字人即可快速生成视频，告别复杂的拍摄过程，内容修改便捷，人物表达质量稳定，而且可以随时随地快速更新内容，在自媒体领域批量输出视频，极大提高了短视频内容生产效率。目前，在新闻播报、广告营销、时事热点、产品介绍等领域，都能通过 AI 内容生成+虚拟数字人讲解的方式，快速生成视频并传播。

生成数字人视频的方法多种多样，这也导致一些其他问题的出现。例如：Korshunova 等[8]通过风格迁移可以改变一个人的脸部形象，那么数字人在元宇宙中的形象是否与真人对应值得怀疑；其次，对于所需上传的文件内容与生成的所听到的内容是否相同也是需要注意的问题；最后，对于成功生成视频的一些授权问题也待解决。随着人工智能技术快速发展，世界数字化进程速度加快，孪生数字人已逐步成为信息传播的一个重要渠道，并广泛应用于网络直播、新闻传媒、即时通讯、短视频媒体、视频会议等多个方面。然而，孪生数字人发布的言论及行为是其权属人真实意愿的表达还是伪造或者黑客攻击，目前仍处于混乱状态。基于以上问题，本文提出了一个孪生数字人的语言和行为授权框架，该框架利用人脸识别方法和区块链中的哈希加密以确保信息的准确比对及生成，以及数字证书对视频的授权。

1 相关工作

1.1 数字人发展

孪生数字人从最早的手工绘制到现在的 CG、人工智能合成，孪生数字人大致经历了萌芽、探索、初级和成长 4 个阶段。最初，在开始尝试将数字人引入现实世界阶段，实现数字人主要靠手绘，效率极低，随后经过不断探索，可以利用 CG、动作捕捉等计算机技术实现，但是制作周期也较长。当深度学习大面积普及之后，数字人的制作得到了极大简化。目前，数字人已逐渐走进人们的日常生活，在文旅场景、文化传媒、影视动画、企业服务等方面发挥着独特作用[9]。同时，数字人在教育行业也发挥着极大作用，可以创建用户与虚拟世界连接的场景[10]。

1.2 数字人安全

人脸表情迁移技术、说话脸生成技术、3D 人脸重建技术等其他主流技术的发展，使得人们不得不更加深层次地考虑数字人的安全问题。孪生数字人作为真人在元宇宙中的分身，当它被“恶搞”时，虽然可以给大众提供娱乐，但也会因为滥用和缺少监管，造成信息安全隐患和传播侵权乱象[11]。面对此种状况，对孪生数字人的真人信息及应用场景信息进行有效的安全防护显得必要而迫切。

当前，对生成的孪生数字人视频尚无一个整体的安全检测结构框架，相关研究主要有对换脸视频检测算法。例如：文献[12]采用多路卷积特征提取网络分别提取空域颜色通道特征、频域离散傅里叶变换特征以及时域光流特征引入通道注意力机制对视频进行检测。文献[13]在 EfficientNetV2 的网络架构基础上优化了注意力机制，引入 ECA（Efficient Channelattention）高效通道注意力模块，并在保证模型拥有较高准确度的前提下重新定义了网络各阶段的重复次数，降低了网络模型复杂度。除通过换脸对视频进行检测外，还可以对视频中的孪生人脸进行识别，并且与本体人脸进行对比以判断是否对其有恶意操作。在人脸识别部分，常用算法主要有基于几何特征的人脸识别、基于特征脸的人脸识别、基于模板匹配的人脸识别、基于神经网络的人脸识别。除对孪生数字人进行安全防护外，主要采用加密隐私保护技术确保视频中其他信息的安全性[14]。常见的加密技术主要有对称加密技术、非对称加密技术、同台加密技术和失真隐私保护技术。对称加密技术在对明文进行加密解密时使用相同的密钥，数据加密标准（Data Encryption Standard，DES）、高级加密标准（Advanced Encryption Standard，AES）等都是常见的对称加密技术[15]。非对称加密方法在加解密时使用不同的公私钥，私钥自己保留，用于解密；公钥可以公开，用于加密明文。李维斯特—萨莫尔—阿德曼算法（Rivest-Shamir-Adleman，RSA）是目前最为流行的非对称加密技术，其密钥有不同的长度可供选择。同态加密技术是由 Rivest 等[16]于

1978年提出的一种特殊加密方式，可保证用户对明文进行加密后计算得出的结果经过解密后与加密前所计算的结果相同。

以上两种技术在各自领域都已发展得较为成熟，且应用颇为广泛。本文将它们有效地结合起来，并加入其他技术对框架进行完善，实现孪生数字人应用安全上的有效保护，防止中间篡改，同时引入第三方机构进行认证。

2　孪生数字人形象与语言框架结构

本文主要目的是提供一个框架，对孪生数字人的语言和行为进行授权，整体框架如图 1 所示。首先需要 3 项输入内容，分别是生成的数字人视频、用于生成视频的文本和真人照片；随后需要对视频授权的一些其他信息，包括但不限于播放平台、播放时间期限等，主要分 3 个部分进行操作：①对真人与孪生数字人进行识别对应，以证明“我是我”；②对文本进行判断，将文本与识别出的字幕进行比对，防止出现文本内容和动作不对应的情况；③对视频的物理信息进行加密生成数字签名，在后续查验时可以有准确的信息。在完成以上 3 部分后，生成具有效应的数字证书。

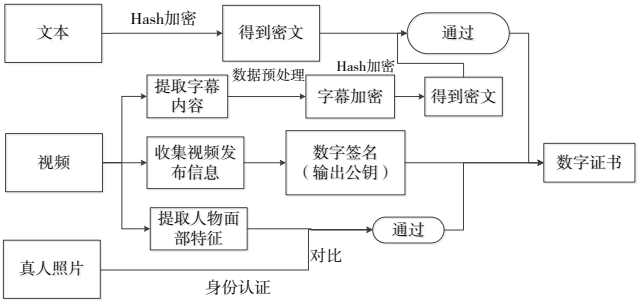


Fig. 1　Image and language framework structure

图 1　形象与语言框架结构

2.1　人脸识别

人脸识别主要包括图像获取、模型训练和人脸识别对比。本文采用 1∶1 的方式筛选其身份验证，前面的 1 代表从设备中采集的照片，后面的 1 代表身份证中的照片，通过将现场采集的照片和身份证中存放的照片进行比对，判别持证人是否为本人。

在进行图像预处理时，一些物理因素影响会导致结果偏差，这就需要对图像进行预处理操作。在人脸识别中，不同的图片大小会对识别结果产生很大影响，因此需要对不同大小的图片作尺寸归一化处理。本文先将图片缩放到固定大小到 256×256；然后将人脸对齐，采用 landMark 的方法选取关键点个数进行人脸对齐和裁剪，将人脸图像调至标准角度，使不同角度的人脸图像具有一致的朝向和比例；最后，通过数据增强提高识别准确率。

人脸识别流程如图 2 所示，通过使用 OpenCV 获取视频数据流，捕获视频或者摄像头传来的图像，每隔若干帧取一帧进行人脸识别，调用 Dlib 中的人脸检测器以检测人脸，并通过 Dlib 的人脸关键点预测器获得人脸关键点。然后，使用 Dlib 的面部识别模型将获得的 68 个关键点转换成 128 D 面部描述符，通过计算人脸的 128 D 面部描述符与本地人脸库（需要自己建立人脸库）中人脸 128 D 面部描述符的欧氏距离，计算公式如式（1）所示。

$$\rho = \sqrt{\left(x_2 - x_1\right)^2 + \left(y_2 - y_1\right)^2 + \left(z_1 - z_2\right)^2} \tag{1}$$

通过结果判断是否为同一人，当距离小于特定阈值时，认定识别成功，打上人物姓名标签，否则打上 unKnown 标签。最后，将打上标签的图像和视频输出到本地。

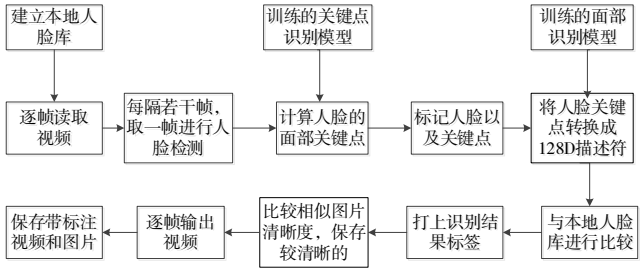


Fig. 2　Face recognition process

图 2　人脸识别流程

首先需要建立一个本地人脸图像，流程如图 3 所示。经过人脸检测获取关键点，经过深度残差网络（见图 4）取得人脸特征向量，以便后续对视频中的人像进行判断时有所对比；然后，在视频中利用获取的人脸向量，与本地已经标注的人脸进行匹配；最后，获得分类结果，判断是否为同一个人。具体流程如图 5 所示。

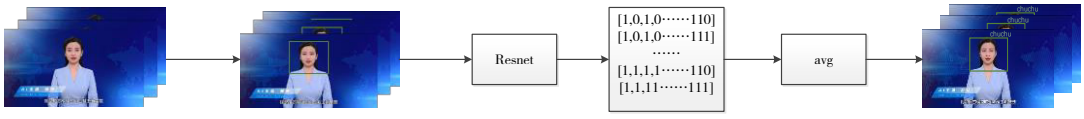


Fig. 3　Local image library establishment process

图 3　本地图像库建立流程

2.2　文本加密解密

为了更好地对信息保密，减小其在传输过程中被修改的可能性，利用对称加密技术对文本信息进行加密。AES 加密技术是目前最流行的机密算法之一，密钥长度可以是 128 位、192 位或 256 位。设 E 为 AES 的加密函数，加密算法流程如图 6 所示，则密文 C 可以使用明文 P 和密钥 K 表

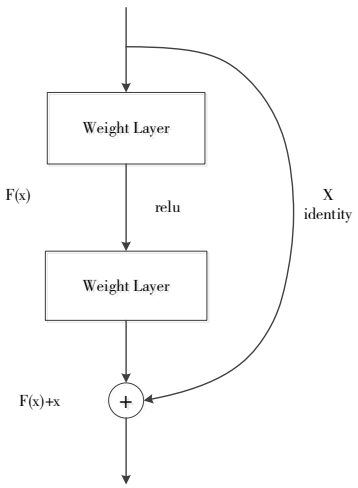


Fig. 4 Residual blocks

图4 残差块

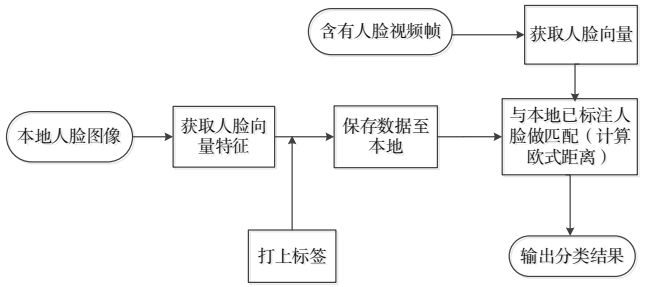


Fig. 5 Video portrait comparison flow

图5 视频人像对比流程

示为E(K,P)。换言之,若将P和K作为参数输入加密函数E,会得到密文C。需要注意的是,密钥K是接收方与发送方一起协商产生,但为了防止密钥泄漏,不能直接在网络上进行传输。原因在于,加密和解密时使用的密钥一致,一旦泄露会使得攻击者直接对明文进行还原,造成隐私泄露。解密时,设D(K,C)为AES的解密函数,也即将K和C输入解密函数,会得到P。

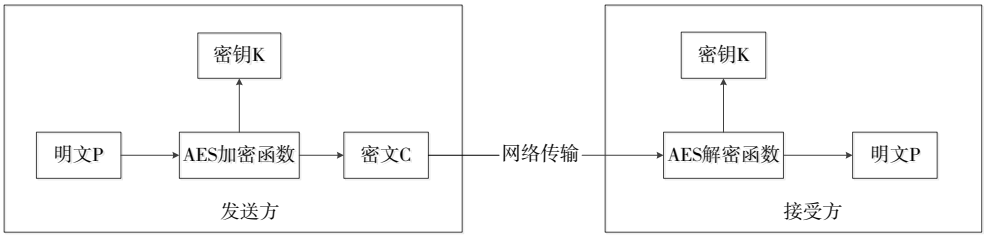


Fig. 6 AES encryption algorithm flow

图6 AES加密算法流程

2.3 数字证书生成

电子签名应用了数字认证技术,以保障电子素质证书的可靠性、完整性、合法性。区块链使得各节点均可写入数据库,同时采用分布式系统,建立一个不依靠信任的电子系统。

在电子签名这一环节,数字认证技术的主要作用体现如下:①身份识别,证明各实体在互联网上身份的真实性;②电子签名及文件内容防篡改,接入第三方权威CA认证的数字证书产品和数字认证技术,在实现素质证书电子签名的同时,保证签名的有效性和安全性。可靠的电子签名由签署主体身份和签名防篡改两方面的内容构成,对于已附上电子签名的文件而言,任何文件内容和签名主体身份改动都能够被发现。

CA证书的认证流程是:①申请证书,该环节只需填写一个在线申请表格,该表格将要求提供必要的个人和公司信息,在申请过程中,需要提供公司或组织的注册证明和合法性证明,这些信息将有助于CA证书认证中心核实身份;②CA证书认证中心对提交的身份信息进行验证,当身份通过验证后,CA证书认证中心开始生成密钥对,密钥对由私钥和公钥组成,私钥将保存在其使用数字证书的服务器上,这样数据将受到保护;③5进行证书签名,即CA证书认证中心将使用私钥对密钥进行数字签名,所有使用CA证书认证中心的公钥都可以验证数字证书的真实性和有效性,这样可以确保数字证书不会被篡改;④发送证书,CA证书认证中心将发送数字证书,该证书包括公钥、数字签名和与组织相关的其他信息,需要将数字证书安装在服务器上,并确保它与私钥配对;⑤进行验证和加密。

3 实验与对比分析

3.1 人脸识别

首先建立本地人脸库,再对视频进行处理,通过OpenCV提供的VideoCapture()函数对视频进行加载,并计算视频的fps,以方便人脸标记之后的视频输出。将已经训练好的模型加载进来,并将人脸关键点标记模型和面部识别模型加载进来,以便后续使用。

下一步,读取视频帧,进行人脸检测,先将取得的照片进行灰度处理,然后进行人脸检测,绘制人脸标记框并进行展示,再通过加载的人脸关键点标记模型识别图像中的人脸关键点,并作好标记。最后进行人脸识别,将获取的人脸关键点转换成128 D人脸描述符,将其与人脸库中的128 D面部描述符进行欧氏距离计算,当距离值小于某个阈值时,认为人物匹配,识别成功,打上标签。当无一小于该阈值,打上Unknown标签。视频中人物识别结果如图7所示。

Fig. 7　People identification results in the video

图7　视频中人物识别结果

3.2　文本提取

在对文本进行比对之前，先对数据作预处理操作，该环节主要分为两部分，分别是对从视频中提取出的字幕和所提供的文本进行操作。对于所提供的文本，需要对其非文字的其他字符进行清洗，由于提取的字幕不包含标点符号等信息，为防止在加密过程中受其他字符影响，只留下文本字符。

对字幕提取出的文本，处理过程将会比处理前面的文本字幕稍复杂，需先作去重处理。这里，每 30 帧提取一张图片进行字幕提取，但是对于一些单句较长的部分，还是会出现语句重复现象，图 8 是对视频中的文字进行提取。处理完这部分之后，同前面一样，将非文本字符进行删除操作，变成纯文字文本。在对视频中字幕提取时，利用飞浆 Paddle 中所提供的 OCR 方法，可以快速准确地得到字幕内容，再利用 Pandas 将数据清洗干净，由此数据处理完毕。

Fig. 8　Text extraction

图8　文字提取

在将数据处理完毕后，分别将双方数据用相同方法进行加密和传送，防止在此过程中对文件进行更改，下一步，通过公钥对其解密，并进行对比。加密解密结果如图 9 所示。

3.3　生成数字证书

该环节主要是生成一个数字证书，以对视频进行确定

（a）　Successful file encryption　　（b）　Successful file decryption

（a）　文件加密成功　　（b）　文件解密成功

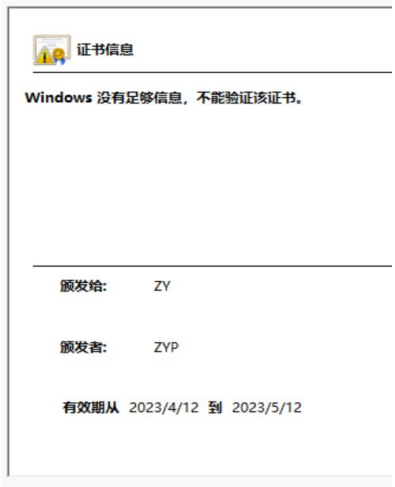
Fig. 9　File encryption and decryption

图9　文件加密解密

授权。使用 AES-CBC 模式对文件进行加密，AES 的本质是分组加密算法。数字证书通过可信任的证书颁发机构，保证了通信双方的身份认证，也解决了公钥分发问题。数字证书包括颁发者信息、被颁发者公钥信息、身份信息、证书序列号、证书签名算法以及该数字证书有效期等。在本文实验中，通过自己给自己颁发数字证书的模式研究数字证书，以确定该框架的实用性。

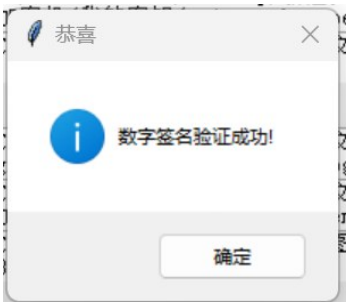
利用 Cryptography 库中的 x509 实现数字证书颁发，首先读取用户公钥信息并生成自己的公私钥，然后利用 x509 模块，实现数字证书的颁发和保存，结果如图 10(a)所示。在签名的时候，是对文件的哈希值进行签名，所以在验签阶段，只需要选择原文件和已签名的文件，对原文件进行哈希，对已签名的文件进行解密得到哈希，比较两者的哈希值是否相等即可。

当对之前的签名文件进行签名验证，页面将显示验证成功，如图 10(b)所示。如果选择的文件是不正确的文件，则页面会显示签名验证失败。



（a）　The digital certificate information

（a）　数字证书信息



（b）　The verification result of the digital signature

（b）　数字签名验证结果

Fig. 10　Generating digital certificates and signatures

图10　生成数字证书、数字签名

3.4　对比实验

数字人形象语言视频相关的授权内容主要包括：分别对数字人身份进行授权、对视频内容进行保护以及对视频

中的文本进行保护。下文将本文研究框架与其他保护方法进行比较，并列出各自优缺点，如表1所示。

Table 1 Comparison between the proposed framework and other protection methods

表1 本文框架与其他保护方法比较

类型	典型方法	优点	缺点
身份信息保护	区块链	分布式存储 去中心化控制 不可篡改的记录 可控的透明性	性能限制 安全性风险法律和合规要求
	差分隐私	个体可控性 数据实用性 法律合规性	数据质量问题 隐私与效用的权衡 差分隐私机制设计复杂性
视频、文本内容保护	基于深度学习	高效的特征提取 多样的保护技术 自适应学习能力 可扩展性	数据需求量大 训练和部署复杂性 隐私和安全问题 模型解释性
形象与语言授权	本文框架	真人、视频信息同时得到保护 可扩展性 法律合规性 安全性	需要第三方体系认证

综上得出，在对数字人身份进行识别保护的同时，视频内容安全也得到了保障，通过基于深度学习的身份识别、文本信息加密处理和第三方授权认证的多模态处理，得到了完整的授权框架，对孪生数字人的形象和语言具有授权和鉴别作用。

4 结语

随着AI的快速发展，孪生数字人的信息安全问题逐渐凸显。由此，本文设计了基于深度学习的身份识别、文本信息加密处理和第三方授权认证的框架，利用三方技术构建一个较完整的授权框架，对生成的孪生数字人视频进行授权保护。经过实验证明，框架可有效实现对孪生数字人视频的内容检测，达到对具体时空切片内所发布的言论和行为进行授权和鉴别的要求。

当然，该框架也存在一些不足，在文本信息加密对比部分，由于加密生成的哈希码对比十分精确，当对比的两个原文本存在无关误差时，也会对结果造成影响。此外，生成的数字证书要利用第三方机构，在达到安全性的同时，外部影响因素也较大。因此，希望后续能够设计出不经由第三方插入便可得到授权的框架。同时，对视频中孪生数字人的动作进行保护授权，并且在多场景下都可以进行判断和应用。

参考文献：

[1] CHEN H. Ten risks of virtual digital people[J]. Money, 2022(9): 8-9.
陈辉. 虚拟数字人的十大风险[J]. 理财, 2022(9): 8-9.

[2] YI R, YE Z, ZHANG J, et al. Audio-driven talking face video generation with learning-based personalized head pose[DB/OL]. https://arxiv.org/abs/2002.10137v2, 2020.

[3] WANG K, WU Q, SONG L, et al. MEAD: a large-scale audio-visual dataset for emotional talking-face generation[C]//Proceedings of European Conference on Computer Vision, 2020: 700-717.

[4] JI X, ZHOU H, WANG K, et al. Audio-driven emotional video portraits[C]//2021 IEEE/CVF Conference on Computer Vision and Pattern Recognition (CVPR), 2021: 14075-14084.

[5] FRIED O, TEWARI A, ZOLLHFER M, et al. Text-based editing of talking-head video[J]. ACM Transactions on Graphics (TOG), 2019, 38(4): 1-14.

[6] YAO X, FRIED O, FATAHALIAN K, et al. Iterative text-based editing of talking-heads using neural retargeting[J]. ACM Transactions on Graphics (TOG), 2021, 40(3): 1-14.

[7] CHENG L, WANG S, ZHANG Z, et al. Write-a-speaker: text-based emotional and rhythmic talking-head generation[DB/OL]. https://arxiv.org/abs/2104.07995v1, 2021.

[8] KORSHUNOVA I, SHI W Z, DAMBRE J, et al. Fast face-swap using convolutional neural networks[C]//Venice: 2017 IEEE International Conference on Computer Vision (ICCV), 2017.

[9] LI X Q. Virtual digital people come into daily life[N]. People's Daily Overseas Edition, 2023-05-10(008).
李雪钦. 虚拟数字人走进日常生活[N]. 人民日报海外版, 2023-05-10(008).

[10] LIN H. "Virtual digital human" empowering microlesson production[J]. Information Technology Education in Primary and Secondary Schools, 2023(4): 78-81.
林华. “虚拟数字人”赋能微课制作[J]. 中小学信息技术教育, 2023(4): 78-81.

[11] WU L H. How to guide "technology for good" in the black and gray industry chain of "AI face replacement"[N]. Jiefang Daily, 2023-04-20(5).
邬林桦. “AI换脸”暗藏黑灰产业链，如何引导“技术向善”[N]. 解放日报, 2023-04-20(5).

[12] HU Y J, YAO Q S, LIN Y Y, et al. Multi-domain feature fusion for face replacement video detection algorithm[J]. Journal of Hefei University of Technology (Natural Science Edition), 2022, 45(12): 1615-1622.
胡永健, 姚其森, 林育仪, 等. 多域特征融合的换脸视频检测算法[J]. 合肥工业大学学报(自然科学版), 2022, 45(12): 1615-1622.

[13] LI A. A lightweight EfficientNetV2 method for face replacement detection[J]. Information Recorded Materials, 2022, 23(10): 219-222.
李昂. 一种轻量化EfficientNetV2换脸检测的方法[J]. 信息记录材料, 2022, 23(10): 219-222.

[14] QIU C X, LI C. Application of data encryption technology in computer Networks[J]. China Management Informatization, 2018, 21(4): 131-132.

[15] WANG H L. Research on the risk management strategy of mobile company's capability open platform construction[D]. Nanjing: Nanjing University of Posts and Telecommunications, 2018.
王红亮. 移动公司能力开放平台建设风险管理策略研究[D]. 南京: 南京邮电大学, 2018.

[16] RIVEST R L, SHAMIR A, ADLERNAN L M. A method for obtaining digital signatures and public-key cryptosystems[J]. Communications of the ACM, 1978, 21(6): 120-126.

（责任编辑：孙 娟）