B部分

生物

现有的PPFR解决方案可以分为两类基于图像处理的PPFR和基于密码学的PPFR。

基于密码学的根据加密技术又分为两类：基于同态的PPFR和基于随机性的PPFR。

图像加密的方法分为对称算法和非对称算法

如[8]中报道，Boult提出通过使用和调整加密技术并将其与智能视频处理方法相结合来保护隐私。主要贡献显示为仅对拥有解密密钥的授权用户进行密码学上的可逆遮蔽。为了满足视频监控的安全需求，图像加密方法已被越来越多地应用。传统的加密算法主要包括对称加密算法和非对称加密算法。数据加密标准（DES）、三重数据加密标准（TDEA）、Rivest Cipher5（RC5）和国际数据加密算法（IDEA）是典型的对称加密算法，而RSA（由Ron Rivest、Adi Shamir和Leonard Adleman于1977年提出）、ELGAMAL、RABIN、Diffe-Hellman和椭圆曲线密码学（ECC）是非对称密码算法。视频处理需要满足其需求，如快速和高水平的效率。因此，这些传统的加密算法可能不是对大尺寸视频帧进行加密的最理想的算法。通过分析最近的报告和出版物，图像应用的加密方案可以分为三类，包括像素位置置换法、值置换法和混合扰乱法

下标【】见整理文档

在人们的日常生活中摄像头已经无处不在，基于摄像头的机器视觉应用和个人隐私保护很难兼顾。除了完善相关法律法规，规范视频的收集、存储、使用外，有必要采取相应的技术措施来保护数据和信息，从而避免恶意侵犯和泄露个人隐私【2】。现有的人脸隐私保护解决方案主要基于图像处理或基于密码学。【1】基于图像处理的方法只保护人脸的视觉内容，仍然无法防止面部信息泄露。基于密码学的方法对显示身份的视频部分进行选择性加密以保护隐私，并在未来进行调查活动等合法需求时，授权恢复原始视频。【x】使用加密技术与智能视频处理方法结合来隐藏人脸，对拥有加密密钥的授权用户提供可逆性遮蔽，保护了受监视人的隐私。相较于基于图像处理的方法，基于密码学的方案因为沉重的加密技术计算效率较低。

Cameras have become ubiquitous in people's daily lives, and it is difficult to balance camera-based machine vision applications and personal privacy protection. In addition to improving relevant laws and regulations to regulate the collection, storage and use of video, it is necessary to adopt corresponding technical measures to protect data and information, so as to avoid malicious infringement and leakage of personal privacy [2]. Existing face privacy protection solutions are mainly based on image processing or based on cryptography. [1] Image processing-based approaches only protect the visual content of the face and still cannot prevent facial information leakage. Cryptography-based approaches selectively encrypt the portion of the video that shows identity to protect privacy and authorise recovery of the original video in the event of legitimate needs such as future investigative activity. [x] uses a combination of encryption techniques and intelligent video processing methods to hide faces, providing reversible masking to authorised users who have the encryption key, protecting the privacy of the person under surveillance. Compared to image processing-based methods, cryptography-based schemes are less computationally efficient due to heavy cryptography.

根据加密技术主要分为基于同态和基于随机性。同态加密是一类具有特殊自然属性的加密方法，与一般加密算法相比，同态加密除了能实现基本的加密操作之外，还能实现密文间的多种计算功能，即先计算后解密可等价于先解密后计算。这个特性对于保护信息的安全具有重要意义，利用同态加密技术可以先对多个密文进行计算之后再解密，不必对每一个密文解密而花费高昂的计算代价；利用同态加密技术可以实现无密钥方对密文的计算，密文计算无须经过密钥方，既可以减少通信代价，又可以转移计算任务，由此可平衡各方的计算代价；利用同态加密技术可以实现让解密方只能获知最后的结果，而无法获得每一个密文的消息，可以提高信息的安全性。目前存在三种同态加密方案类型：(1) partially homomorphic encryption systems that support only a single arithmetic operation i.e., either addition [30] or multiplication [10] in the encrypted domain, (2)somewhat homomorphic encryption systems that support a limited number of both additions and multiplications, and (3) fully homomorphic encryption (FHE) systems that support unlimited additions and multiplications directly in the encrypted domain.Jin et al. [27] proposed a PPFR scheme based on sparse representation using homomorphic encryption and oblivious transfer. In the proposed scheme, The SP identifies whether a user is authorized through face recognition without revealing any information of the two parties**.[1]** Inspired by computation outsourcing, Xiang et al. [24] presented a PPFR scheme which outsources a face recognition to the SP. The hybrid encryption based fully homomorphic encryption is utilized to protect the privacy of faces. The proposed protocol reduces the computation cost between users and the face owner.

【1】Jin等人在[x]当中使用同态加密和遗忘传输，通过人脸识别来识别用户是否被授权，而不透露双方的任何信息。完全同态加密算法也有应用，与其他相比，完全同态的人脸对加密的模板和被查询的人脸都提供了更高的私有验证。

According to the technology used for encryption, the two primary categories are homomorphic-based and Randomness -based.

A group of encryption techniques with unique natural characteristics is called homomorphic encryption(HE). In contrast to standard encryption methods, homomorphic encryption is capable of performing a number of computation functions between ciphertexts, meaning that computation before decryption can be identical to decryption before computation. There are three different types of homomorphic encryption schemes: (1) partially homomorphic encryption, which allow for only one arithmetic operation—either addition or multiplication in the encrypted domain; (2) somewhat homomorphic encryption, which allow for a limited number of additions and multiplications; and (3) fully homomorphic encryption (FHE), which allow for unlimited additions and multiplications. Jin et al. use homomorphic encryption and oblivious transfer among [x] to identify whether a user is authorised by face recognition without revealing any information about both parties. Fully homomorphic encryption algorithms have also been applied, and fully homomorphic faces provide a higher level of private authentication for both the encrypted template and the queried face compared to others.

由于使用同态加密人脸计算效率低，在[23]中随机性技术被用来保护参与方的参数的隐私。由于使用了随机性工具，其计算和通信效率得到了大幅提高。但是仍有许多限制，人脸特征对服务供应商是不保密的，隐私保护效果仍然不能令人满意。

Due to the low computational efficiency of using homomorphic encryption faces, randomness techniques were used in [23] to protect the privacy of the parameters of the participating parties. Due to the use of randomness tools, their computational and communication efficiency has been significantly improved. However there are still many limitations, the face features are not confidential to the service provider and the privacy protection is still unsatisfactory.

现有加密算法在计算通信效率和隐私保护效果方面仍有不足，目前很少有人尝试使用类人认知机制进行人脸加密处理，本文在此方向上进行初步探索。

Existing encryption algorithms are still inadequate in terms of computational communication efficiency and privacy-preserving effects, and few attempts have been made to use human-like cognitive mechanisms for face encryption processing, and our paper is a preliminary exploration in this direction.

[x]Boult, T.: PICO: privacy through invertible cryptographic obscuration. In: Proceedings of

the Computer Vision for Interactive and Intelligent Environment, pp. 27–38, October, 2005