Cameras have become ubiquitous in people's daily lives, and it is difficult to balance between camera-based machine vision applications and personal privacy protection. In addition to improving relevant laws and regulations to regulate the acquisition, storage and use of videos, corresponding technical measures are needed to protect personal privacy. The cryptography-based face privacy protection scheme selectively encrypts the face region in the video that shows the identity and can be decrypted to recover the original video in case of future legitimate demand.

Most of the existing face encryption schemes are are homomorphic-based[18-26]. There are three different types of homomorphic encryption schemes: (1) partially homomorphic encryption, (2) somewhat homomorphic encryption and (3) fully homomorphic encryption (FHE).Tamiya et al. proposed a successful homomorphic encryption-based face template protection scheme by computing the squared Euclidean distance between facial features with a single homomorphic multiplication method[20]. Román et al. suggested using the Kyber and Saber public key encryption (PKE) algorithms along with homomorphic encryption (HE) in facial recognition systems to achieve smaller protected template and key sizes and faster execution times than other HE schemes that use lattices[21]. The use of fully homomorphic encryption algorithms provides a higher level of privacy authentication for the queried face.[22] offered a successful, privacy-preserving face verification method based on a corrupted circuit and fully homomorphic encryption. [18,23] used CKKS fully homomorphic encryption to encrypt the normalised facial feature vector.

摄像头在人们的日常生活中已经无处不在，基于摄像头的机器视觉应用与个人隐私保护之间难以平衡。除了完善相关法律法规规范视频的采集、存储和使用外，还需要采取相应的技术措施保护个人隐私。基于密码学的人脸隐私保护方案对视频中显示身份的人脸区域进行选择性加密，并能在未来合法需求的情况下进行解密，恢复原始视频。

现有的人脸加密方案大部分都是基于同态的。【20】通过单一的同态乘法计算面部特征之间的平方欧几里得距离，提出了一个成功的基于同态加密的人脸模板保护方案。[21] proposed to use Kyber and Saber public key encryption (PKE) algorithms together with homomorphic encryption (HE) in face recognition systems，achieving smaller sizes of protected templates and keys, and shorter execution times than other HE schemes reported in literature that employ lattices.除此之外，完全同态加密也得到了应用。

[18,23]采用CKKS完全同态加密技术来加密归一化的面部特征向量。

Due to the low computational efficiency of using homomorphic encryption, there have been many studies that have attempted to use other methods to encrypt faces. Tan et al. proposed a novel approach to implement video-based ring-learning (ring-LWE) cryptography for face encryption and decryption on a graphics processing unit (GPU)[31].Duong-Ngoc et al. proposed a novel method to comprehensively protect facial images extracted from videos based on NewHope cryptography for post-quantum cryptosystems, greatly reducing the time for encryption and decryption [28]. zhao et al. proposed and implemented a simple and efficient speckle-based optical cryptosystem to encrypt face images by seemingly random optical speckles at the speed of light, by training an cryptographic neural network to decrypt face images from random speckles [29]. A fast block scrambling method was used in [33,34] to scramble the detected faces. In addition, an encryption technique using face biometrics to generate random phase masks was first proposed in [35]. A THM (tent-Henon map) chaotic encryption of faces based on the Ridgelet-DCT transform was proposed in [36] and combined the properties of tent chaos and Henon chaos. [37] introduced deoxyribonucleic acid (DNA) coding theory into biological template protection, and proposed a face protection algorithm based on DNA coding encryption. [38] proposed a Generative Adversarial Network (GAN)-based method to encrypt facial features using Wasserstein Generative Adversarial Network Encryption (WGAN-E). [40] used a graph theory-based graph first decomposition mask (GFH) coding algorithm.

由于使用同态加密的计算效率较低，有许多研究尝试使用其他方法来加密人脸。

Duong-Ngoc et al.基于后量子密码系统的NewHope密码学，提出一种新颖的方法全面保护从视频中提取的面部图像，大大减少了加密解密的时间[28]。Zhao et al.提出并实现了一个简单而高效的基于斑点的光学密码系统，通过看似随机的光学斑点以光速对人脸图像进行加密，通过训练一个加密神经网络从随机斑点中解密人脸图像[29]。Tan et al.提出了一种新颖的方法，在图形处理单元（GPU）上实现基于视频的人脸加密和解密的环形学习（ring-LWE）密码学。

在[33,34]中使用了快速块扰乱方法来扰乱检测到的人脸。此外，[35]首次提出了一种使用人脸生物特征生成随机相位掩码的加密技术。[36]中提出了一种基于Ridgelet-DCT变换的THM（tent-Henon map）混沌加密人脸技术，并结合了tent混沌和Henon混沌的特性。[37]将脱氧核糖核酸（DNA）编码理论引入生物模板保护，提出了一种基于DNA编码加密的人脸保护算法。[38]提出了一种基于生成对抗网络（GAN）的方法来加密人脸特征，使用Wasserstein生成式对抗网络加密法（WGAN-E）来加密面部特征。[40]使用了基于图论的图先分解掩码（GFH）编码算法。

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.

现有的加密算法在计算通信效率和隐私保护效果方面仍有不足，很少有人尝试使用类似人类的认知机制进行人脸加密处理，我们的论文是在这个方向上的初步探索。