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. Existing face privacy protection solutions are mainly based on image processing or based on cryptography[9]. 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. Compared to image processing-based methods, cryptography-based schemes are less computationally efficient due to heavy cryptography.

According to the technology used for encryption, many categories are homomorphic-based[A-J].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, (2) somewhat homomorphic encryption and (3) fully homomorphic encryption (FHE). In [G], a homomorphic encryption-based face feature ciphertext authentication approach is put forth. [C] suggests a successful homomorphic encryption-based face template protection solution. To improve the privacy of a cloud-based facial recognition system, [B] apply homomorphic encryption.[D] suggests using the homomorphic encryption (HE) and Kyber and Saber public key encryption (PKE) algorithms in a facial recognition system. 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.[E] offer a successful, privacy-preserving face verification method based on a corrupted circuit and completely homomorphic encryption.The most recent homomorphic encryption breakthrough, the CKKS fully homomorphic encryption technique, is used by [A,F,I] to encrypt the normalised facial feature vectors. In addition, to balance security and operational efficiency, [I] also employs the symmetric encryption properties of the state secret SM4 algorithm, while the SM9 asymmetric encryption algorithm is used to manage the symmetric key of the SM4 algorithm. This increases the resistance of the facial feature ciphertext to malicious attacks.

Due to the low computational efficiency of using homomorphic encryption faces, there are many other methods that have been applied to encrypt faces. It has been suggested in [k] to use a unique cancelable FaceHashing technique based on non-invertible transformation using encryption and decryption templates. [L] suggests a revolutionary method based on the post-quantum cryptosystem known as NewHope cryptography to completely safeguard facial photos taken from movies. The proposed method considerably decreases the time required for encryption and decryption by organising the input data. In [M], a simple but incredibly effective speckle-based optical cryptosystem is suggested and put into practise. A properly trained decryption neural network can subsequently be used to decrypt face images from random specks.A novel biometric cryptosystem for vectorial biometrics is proposed by [N] and is known as symmetric keyring encryption (SKE), which draws inspiration from Rivest's keyring model. For video-based face encryption and decryption on a graphics processing unit, [O] presents a novel method for implementing ring learning with errors (ring-LWE) cryptography. [p] proposes an efficient sine modular arithmetic chaotic model. The face portion of the image is first extracted using a face recognition algorithm, and the information of the face portion is then encrypted using a combination of forward diffusion and random cyclic scrambling techniques. The quick block scrambling method is used in [q,R] to jumble the detected faces. Additionally, [s] suggests an encryption technique for the first time using the face biometric to generate the random phase mask. A THM (tentHenon map) chaotic encrypted face technique based on Ridgelet-DCT transform is proposed in [t] and combines the properties of tent chaos and Henon chaos. [u] offers a face template protection algorithm based on DNA coding encryption.In order to solve the issues with the Multiscale Block Local Binary Pattern (MB-LBP) feature improvement-based face hashing algorithm and the classical hash technique, [v] suggests a method based on Generative Adversarial Networks (GAN) to encrypt facial features. [w] introduces a encryption algorithm based on quantum image Hilbert permutation to produce cancelable face templates. The cancelable face system in [x] uses the Graph First Decomposition Mask (GFH) encoding algorithm.

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.

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来规范视频的采集、存储和使用外，还需要采取相应的技术措施来保护数据和信息，以避免个人隐私被恶意侵犯和泄露。现有的人脸隐私保护方案主要是基于图像处理或基于密码学。基于图像处理的方法只能保护人脸的视觉内容，仍然不能防止人脸信息的泄露。基于密码学的方法对视频中显示身份的部分进行选择性加密，以保护隐私，并授权在未来调查活动等合法需要的情况下恢复原始视频。与基于图像处理的方法相比，基于密码学的方案由于沉重的密码学，计算效率较低。

根据用于加密的技术，其中很多使用同态加密。一组具有独特自然特征的加密技术被称为同态加密（HE）。与标准的加密方法相比，同态加密能够在密码文本之间进行一些计算功能，这意味着解密前的计算可以与计算前的解密相同。有三种不同类型的同态加密方案：（1）部分同态加密，（2）有点同态加密和（3）完全同态加密（FHE）。[10] uses the CKKS algorithm in the SEAL library, latest homomorphic encryption achievement, to encrypt the normalized face feature vectors.

[E] present an efficient privacy-preserving face verification scheme based on fully homomorphic encryption and garbled circuit.

由于使用同态加密人脸的计算效率低，在[12]中使用了随机性技术来保护参与方的参数隐私。由于使用了随机性工具，其计算和通信效率得到了显著提高。但是仍然有很多局限性，人脸特征对服务提供者来说是不保密的，隐私保护仍然不尽人意。

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。

## [A] Design on Face Recognition System with Privacy Preservation Based on Homomorphic Encryption

[B] Privacy Enhanced Cloud-Based Facial Recognition

[c] Improved Post-quantum-secure Face Template Protection System Based on Packed Homomorphic Encryption

[D] A Quantum-Resistant Face Template Protection Scheme using Kyber and Saber Public Key Encryption Algorithms

[E] Efficient privacy-preserving face verification scheme

[F] Outsourced Secure Face Recognition Based on CKKS Homomorphic Encryption in Cloud Computing

[G] Face Security Authentication System Based on Deep Learning and Homomorphic Encryption

## [H] On the Application of Homomorphic Encryption to Face Identification

## [I] FaceEncAuth:Face Recognition Privacy Security Scheme Based on FaceNet and SM Algorithms

## [J] Face Detection for Privacy Protected Images

[K] A Novel Cancelable FaceHashing Technique Based on Non-Invertible Transformation With Encryption and Decryption Template

[L] Efficient NewHope Cryptography Based Facial Security System on a GPU

[M] Speckle-Based Optical Cryptosystem and its Application for Human Face Recognition via Deep Learning

[N] Symmetric keyring encryption scheme for biometric cryptosystem

[o] Ring-LWE Based Face Encryption and Decryption System on a GPU

[P] A selective image encryption algorithm based on a chaotic model using modular sine arithmetic

[q]A Study of Privacy Protection of Photos Taken by a Wide-angle Surveillance Camera

[r] Privacy Protection in Surveillance Videos Using Block Scrambling-Based Encryption and DCNN-Based Face Detection

[s] Optical selective encryption based on the FRFCM algorithm and face biometric for the medical image

[t] Encrypted face recognition algorithm based on Ridgelet-DCT transform and THM chaos

[u] Face Template Protection Algorithm Based on DNA Encoding Encryption

[v] WGAN-E: A Generative Adversarial Networks for Facial Feature Security

[w] Efficient Generation of Cancelable Face Templates Based on Quantum Image Hilbert Permutation

[x] Presented cancelable face recognition system using graph theory