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[17]. 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.

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[17]。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求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而在计算上效率较低。

According to the technology used for encryption, many categories are homomorphic-based[18-26].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 [24], a homomorphic encryption-based face feature ciphertext authentication approach is put forth. //这个不想要了

[20] suggests a successful homomorphic encryption-based face template protection solution. To improve the privacy of a cloud-based facial recognition system, [19] apply homomorphic encryption.[21] 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.[22] 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 [18,23] to encrypt the normalised facial feature vectors.

根据用于加密的技术，很多类别都是基于同态的[18-26].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，也就是说，解密前的计算与解密前的计算可以完全相同。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）。在[24]中，提出了一种基于同态加密的人脸特征密码文本认证方法。[20]提出了一个成功的基于同态加密的人脸模板保护方案。为了提高基于云的面部识别系统的隐私性，[19]应用同态加密。[21]建议在面部识别系统中使用同态加密（HE）和Kyber及Saber公钥加密（PKE）算法。完全同态加密算法也得到了应用，与其他算法相比，完全同态人脸为加密模板和被查询的人脸提供了更高的隐私认证。[22]提供了一种成功的、保护隐私的、基于损坏电路和完全同态加密的人脸验证方法。最近的同态加密突破，CKKS完全同态加密技术，被[18,23]用来加密归一化的面部特征向量。

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. [28] 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 [29], 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 [30] 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, [31] presents a novel method for implementing ring learning with errors (ring-LWE) cryptography. [32] 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 [33,34] to jumble the detected faces. Additionally, [35] 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 [36] and combines the properties of tent chaos and Henon chaos. [37] 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, [38] suggests a method based on Generative Adversarial Networks (GAN) to encrypt facial features. [39] introduces a encryption algorithm based on quantum image Hilbert permutation to produce cancelable face templates. The cancelable face system in [40] uses the Graph First Decomposition Mask (GFH) encoding algorithm.

由于使用同态加密面孔的计算效率低，有许多其他方法被应用于加密面孔。在[k]中建议使用一种独特的可取消的FaceHashing技术，基于不可逆转的变换，使用加密和解密模板。[28]提出了一种基于被称为NewHope密码学的后量子密码系统的革命性方法，以完全保护从电影中拍摄的面部照片。所提出的方法通过组织输入数据大大减少了加密和解密所需的时间。在[29]中，提出了一个简单但令人难以置信的有效的基于斑点的光学密码系统，并付诸实践。一个经过适当训练的解密神经网络随后可用于从随机斑点中解密人脸图像。[30]提出了一个用于矢量生物识别的新型生物识别密码系统，被称为对称钥匙圈加密（SKE），它从Rivest的钥匙圈模型中获得了灵感。对于在图形处理单元上基于视频的人脸加密和解密，[31]提出了一种新的方法来实现带错误的环形学习（ring-LWE）密码学。[32]提出了一种高效的正弦模块化算术混沌模型。首先使用人脸识别算法提取图像中的人脸部分，然后使用前向扩散和随机循环加扰技术的组合对人脸部分的信息进行加密。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]提供了一种基于DNA编码加密的人脸模板保护算法。为了解决基于多尺度块局部二进制模式（MB-LBP）特征改进的人脸散列算法和经典散列技术的问题，[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。[39]介绍了一种基于量子图像Hilbert permutation的加密算法，以产生可取消的人脸模板。[40]中的可取消人脸系统使用图先分解掩码（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。

1. S. Guo, T. Xiang, and X. J. S. P. Li, "Towards efficient privacy-preserving face recognition in the cloud," vol. 164, pp. 320-328, 2019.
2. Y. Yang, Q. Zhang, W. Gao, C. Fan, Q. Shu, and H. J. W. P. C. Yun, "Design on Face Recognition System with Privacy Preservation Based on Homomorphic Encryption," vol. 123, no. 4, pp. 3737-3754, 2022.
3. T. Yang, Y. Zhang, J. Sun, and X. J. N. P. L. Wang, "Privacy enhanced cloud-based facial recognition," vol. 54, no. 4, pp. 2717-2725, 2022.
4. H. Tamiya, T. Isshiki, K. Mori, S. Obana, and T. Ohki, "Improved Post-quantum-secure Face Template Protection System Based on Packed Homomorphic Encryption," in *2021 International Conference of the Biometrics Special Interest Group (BIOSIG)*, 2021, pp. 1-5: IEEE.
5. R. Román, R. Arjona, P. López-González, and I. Baturone, "A Quantum-Resistant Face Template Protection Scheme using Kyber and Saber Public Key Encryption Algorithms," in *2022 International Conference of the Biometrics Special Interest Group (BIOSIG)*, 2022, pp. 1-5: IEEE.
6. H. Huang, L. J. J. o. I. S. Wang, and Applications, "Efficient privacy-preserving face verification scheme," vol. 63, p. 103055, 2021.
7. L. Jiasen, W. X. An, C. Bowei, T. Zheng, Z. J. I. J. o. M. C. Kaiyang, and M. Communications, "Outsourced Secure Face Recognition Based on CKKS Homomorphic Encryption in Cloud Computing," vol. 12, no. 3, pp. 27-43, 2021.
8. D. Sun *et al.*, "Face Security Authentication System Based on Deep Learning and Homomorphic Encryption," vol. 2022, 2022.
9. P. Drozdowski, N. Buchmann, C. Rathgeb, M. Margraf, and C. Busch, "On the application of homomorphic encryption to face identification," in *2019 international conference of the biometrics special interest group (biosig)*, 2019, pp. 1-5: IEEE.
10. Q. Wang, L. Gao, H. Wang, and X. J. I. A. Wei, "Face detection for privacy protected images," vol. 7, pp. 3918-3927, 2019.
11. A. Sardar, S. Umer, C. Pero, and M. J. I. A. Nappi, "A novel cancelable FaceHashing technique based on non-invertible transformation with encryption and decryption template," vol. 8, pp. 105263-105277, 2020.
12. P. Duong-Ngoc, T. N. Tan, and H. J. I. A. Lee, "Efficient NewHope cryptography based facial security system on a GPU," vol. 8, pp. 108158-108168, 2020.
13. Q. Zhao et al., "Speckle-based optical cryptosystem and its application for human face recognition via deep learning," 2022.
14. Y.-L. Lai, J. Y. Hwang, Z. Jin, S. Kim, S. Cho, and A. B. J. J. I. s. Teoh, "Symmetric keyring encryption scheme for biometric cryptosystem," vol. 502, pp. 492-509, 2019.
15. T. N. Tan, Y. Hyun, J. Kim, D. Choi, and H. Lee, "Ring-LWE based face encryption and decryption system on a GPU," in 2019 International SoC Design Conference (ISOCC), 2019, pp. 15-16: IEEE.
16. X. Wang, N. Guan, and P. J. O. Liu, "A selective image encryption algorithm based on a chaotic model using modular sine arithmetic," vol. 258, p. 168955, 2022.
17. K. Nakai, M. Kuribayashi, and N. Funabiki, "A Study of Privacy Protection of Photos Taken by a Wide-angle Surveillance Camera," in 2021 Asia-Pacific Signal and Information Processing Association Annual Summit and Conference (APSIPA ASC), 2021, pp. 1865-1871: IEEE.
18. K. M. Hosny, M. A. Zaki, H. M. Hamza, M. M. Fouda, and N. A. J. I. A. Lashin, "Privacy Protection in Surveillance Videos Using Block Scrambling-Based Encryption and DCNN-Based Face Detection," vol. 10, pp. 106750-106769, 2022.
19. Y. Shen, C. Tang, M. Xu, Z. J. O. Lei, and L. Technology, "Optical selective encryption based on the FRFCM algorithm and face biometric for the medical image," vol. 138, p. 106911, 2021.
20. Z. Liu, J. Li, and J. J. M. B. E. Liu, "Encrypted face recognition algorithm based on Ridgelet-DCT transform and THM chaos," vol. 19, pp. 1373-1387, 2022.
21. F. He and J. Zhen, "Face Template Protection Algorithm Based on DNA Encoding Encryption," in International Conference in Communications, Signal Processing, and Systems, 2018, pp. 387-393: Springer.
22. C. Wu, B. Ju, Y. Wu, N. N. Xiong, and S. J. E. Zhang, "WGAN-E: A generative adversarial networks for facial feature security," vol. 9, no. 3, p. 486, 2020.
23. H. Alhumyani, G. M. El-Banby, H. S. El-Sayed, F. E. Abd El-Samie, and O. S. J. E. Faragallah, "Efficient Generation of Cancelable Face Templates Based on Quantum Image Hilbert Permutation," vol. 11, no. 7, p. 1040, 2022.
24. H. J. M. T. Ashiba and Applications, "Presented cancelable face recognition system using graph theory," pp. 1-22, 2022.